Hate Aid

Social commitment in danger?

A crisis plan for the committed.

Courses of action and protection strategies for dealing with digital violence at the municipal level. From sports club to refugee aid.

Contents

1 What is a crisis?

Are you taking part in a discussion on climate protection, organizing a discussion group for refugees or occasionally sharing pictures of your work online? The reactions can be fierce. You don't have to be frequently active on social media or hold a political office to be attacked via email, text message or messenger. Such attacks are part of everyday life for many politically active people and can trigger a crisis.

This is how a crisis can unfold, for example:

- First you are criticised.

We need a solution, not another event!

- Criticism develops into **hatred, insults and threats**.

You a**! You have no idea how people really feel.

- Suddenly, within days, you receive **loads of hate mail with violent fantasies or a person publishes your home address** on Facebook.

I know where you live! If you don't stop, we'll pay you a visit.

- **Untrue information about you or fake (nude) photos** are published on the internet and spread rapidly. The aim: to defame you and your work.

Have you seen the latest nude photo of the old hag? She'd be better off in the kitchen and not doing politics.

The consequences: you feel threatened and are afraid for your safety and that of your family. You are unable to assess the real danger of this threat of violence. You are overwhelmed and do not know how to continue your work and deal with the situation. You are facing a crisis or are already in the middle of one.

A crisis situation is an acute state of overwhelm, tension or threat of danger in which the requirements of the situation surpass one's own resources and capabilities.[1]

Crises can be triggered in both the **analogue** and **digital** worlds.

Digital hostility often spills over into the analogue world: for example, you are insulted online and then approached in the supermarket about the subject of the dispute and attacked again. Conflicts and arguments can also shift from analogue life to the internet.

For example, in Germany external perceptions show: 76 % of respondents perceive that politicians are most frequently affected by hate speech.[2] Latest study results show that digital hate is most frequently directed at the political views of those affected.[3]

13% of local politicians have already considered withdrawing from politics out of concern for their safety and that of their family.[4]

Prepare for crisis situations and hostility!

1.1 How can you deal with a crisis situation?

Even if such a scenario seems unlikely to you, it stems from a disagreement. This can escalate both digitally and in the analogue world. **Crises can hit anyone – suddenly, unexpectedly and without warning.**

A crisis plan allows you a minimum amount of control over the situation in an acute case and can help you to manage the crisis well.

Recommendations for action as "Keep calm!" or "Don't let yourself be provoked!" are often given when dealing with crisis situations. This is often easier said than done. What really helps: draw up a preventative crisis plan and use it to prepare yourself for a potential crisis situation. That way, you will be prepared for an emergency.

Answer the following questions to be prepared:

1. What do you consider to be risk scenarios and therefore potential crises?
2. Who is part of your crisis team?
3. What specific steps do you take to deal with a crisis?

1.2 What are potential crises? – Some risk scenarios

- False information about you that is damaging to your reputation is circulating on the internet.
- You receive threats by email.
- You receive hate comments or hate messages on social media or even a shitstorm.
- Sexualised deepfakes are created of you to discredit you.
- Your data is used to create fake social media profiles or email addresses. This is used to spread content and make false statements.
- A person stalks you.[5]
- Your email address was hacked and you can no longer log in with your password or you notice unusual activity on your account.
- You receive phishing emails, e.g. to harm you financially.
- Your sensitive personal data, such as your home address, private photos or information about family members, is published.
- …

The starting point of a crisis is very individual and depends on both your working environment and your own resources for dealing with hostility.

Crisis situations / danger scenarios:

Which scenarios would exceed your personal and professional resources and could therefore pose a threat to you? **Define your potential crisis scenarios.** Use the above-mentioned crisis scenarios as a guide and try to find other examples.

2 Who is your crisis team?

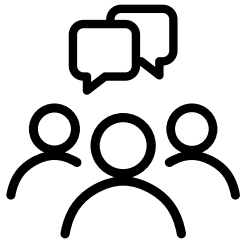
A crisis requires a lot of resources. In order to prepare preventively for a crisis situation, it makes sense to put together a crisis team. This team takes on certain tasks and roles during and after a crisis. Ideally, you should set up this crisis team before the crisis occurs and can then activate it immediately. This gives you the confidence to act and allows you to conserve your own resources in the acutely challenging crisis situation. If you do not yet have a crisis team at this point, organise one first of all. It is not yet too late.

For example, your crisis team could consist of you, your superiors and your colleagues. There may also be dedicated people in the team who can support you at short notice – such as volunteers, interns or people from your private and professional environment.

2.1 Roles of the crisis team

Crisis management:

- Crisis coordinator
- Observers of the attacks



Analogue and digital security:

- Security officer
- Privacy guardian
- IT security officer

Communication:

- Safeguard for netiquette
- Community management
- Press spokesperson

2.2 Crisis management

One or more people maintain an overview of the crisis situations and thus bring calm to the team. They are also responsible for allocating roles.
The following roles should be fulfilled:

Crisis coordinator

- Manages the crisis team.
- Convenes meetings, assigns roles for a crisis situation and informs the team about the next steps of the crisis plan.
- Preventive preparation: prepares a list of potential supporters, organisations and experts that are missing in the team and will be contacted in the event of a crisis. The crisis coordinator also creates a correspondence distribution list.
- In an acute situation: contacts the supporters on the distribution list, explains the situation and describes concrete steps. This person also informs those around them, e.g. office colleagues, about the attack and discusses support measures.
- Follow-up: reflects on the crisis situation together with the team and considers what went well and what can be done better next time.

Observers of the attacks

- Monitors the development of the crisis, which can develop very rapidly, especially on social media channels.
- Constantly evaluates the situation.
- Defines a communication channel through which everyone is regularly informed (email, chat, etc.).
- Informs the crisis coordinator and the team about the development of the crisis.
- Alerts the team if major changes and/or escalations occur (e.g. if defamatory information is spread on further social media platforms).

2.3 Analogue and digital security

One or more people deal with measures for the analogue security and digital protection of those affected. **The following roles and areas of responsibility exist:**

Security officer

- Logs and analyses attacks and assesses which threat scenarios have occurred.
- Contacts the law enforcement authorities, describes the situation and asks for support. Contacts a suitable counselling centre for a risk assessment and protective measures (e.g. HateAid or other counselling centres)
- Obtains legally compliant screenshots from the community manager and, in consultation with the person concerned, files a criminal complaint with a local police station, an online police station, or a reporting centre for digital violence.

Privacy guardian

- Uses search engines to check what sensitive personal data can be found online about the person under attack and their environment. This could be, for example, home address, workplace, telephone number, private photos, etc.
- If sensitive personal data is found: contacts the responsible parties, e.g. website operators[6] or search engine operators and, if necessary, supports them in deleting the data.[7]
- Checks the social media platforms to see what information about the person under attack is visible to third parties and tightens the privacy settings (e.g. temporarily set the account to private or switch off the comment function).

Anyone who has certain personal data about you may be able to find out your current home address very easily, especially if there is an obligation to register in your country. In Germany, for example, this can be done with the help of what is known as a simple registration register enquiry, which can be requested (online) from the registration office. To protect yourself against this, you can apply for an address protection measure, depending on the regulations in your country, e.g. in Germany the entry of a registration block.[8]

To do this, you must submit an application to the relevant registration authority. In this application, you must explain why disclosure of your private address to third parties would pose a risk to you. Proof of this, e.g. criminal charges you have filed, but also a letter from your employer, an association or a counselling centre can be helpful. **In the best case scenario, you can ideally obtain the entry of a so-called registration block preventively.**

IT security officer

- Informs the team about hacking[9] and phishing[10] attacks. If no one in your team or environment has expertise in this area, seek support, e.g. from an IT consultancy.
- Introduces a password manager and two-factor authentication for everyone in the team.
- Reminds the team regularly to use strong passwords.
- Reminds the team regularly to carry out updates on work devices and to back up data.
- If hacking is suspected: alerts the team, changes all passwords, keeps old devices (important for preserving evidence of the hacking attack). Institutions and companies commission a so-called cyber incident response company.[11]

2.4 Communication

Internal and external communication plays a particularly important role when dealing with digital hostility. **If you work alone or with a small team, consider who can support you in crisis situations as a preventative measure.** This could be volunteers, (former) co-workers, other organisations or people from your professional and private environment. These people are your solidarity network. Inform them in advance of an acute crisis and discuss who will take on which role. This will save you time and work in acute crisis situations. Assign the following tasks and roles in the area of communication.

Safeguard for netiquette

- Defines rules on how to communicate on your own social media channels and publishes these rules as netiquette.
- Regularly edits the netiquette and ensures that it is regularly updated.

Community manager

- Enforces the netiquette's rules, filters comments and answers, blocks, reports or deletes them.
- Creates legally compliant screenshots of violent content (see section on creating legally compliant screenshots).
- Reports violent content correctly. In the European Union, there are two options here: either reporting a violation of the rules of the platform itself ('Community Guidelines' or T&Cs) or reporting illegal content on the basis of the Digital Services Act. Only a report based on the Digital Services Act imposes certain legal obligations on the platform, such as checking whether the reported content is illegal and deleting it if necessary.

Press spokesperson

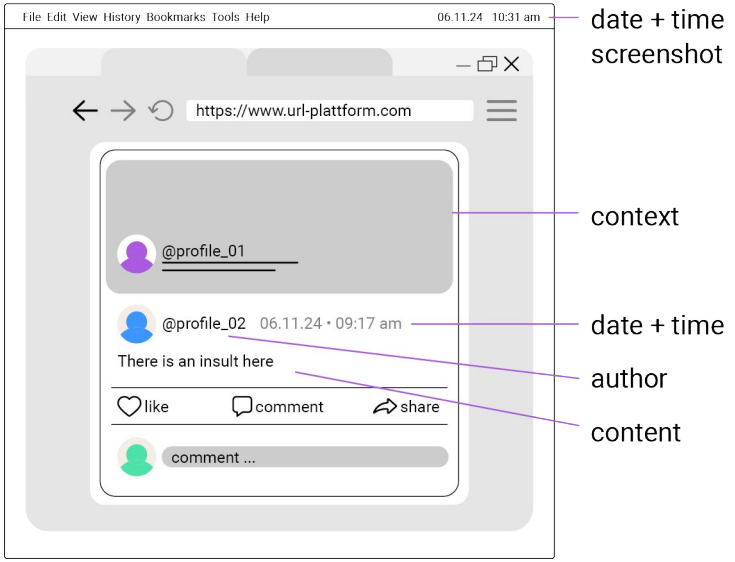
In a small team, you may not have a press spokesperson. However, this role must be filled in crisis situations. This person is responsible for external communication. The spokesperson should be able to write and communicate precisely.

- Creates a draft for a public statement in crisis situations.
- Prepares text modules that the team can use.
- Informs the team about the statement so that everyone follows a standardised line of communication.
- Is available for public enquiries.

2.5 Creating legally compliant screenshots

A legally compliant screenshot is a screen capture of a post or comment on social media, for example, on which certain important information can be seen. This information includes

- the URL of the associated link,
- date (DD.MM.YYYY) and time (hour:minute) of the hostile content,
- image of the offender's profile,
- as well as the context in which the hostility took place.



Example of a legally compliant screenshot

With these screenshots, incidents can be documented quickly and permanently. This is essential if you decide to take legal action against certain content.

2.6 Publishing a statement

Why should you publish a statement?

- It serves to correct false information about you or your organisation.
- It allows you to position yourself on an issue and take responsibility.
- You can reveal the strategies of the attackers.
- You communicate to the outside world how you are behaving in view of the acute crisis, for example whether you are withdrawing for the time being or cancelling an event.
- It helps to receive support and solidarity from other people and important partners.

Where do you publish your statement?

- Publish it on your website.
- Share it on your social media account.
- Share it in regionally relevant groups on social media platforms, e.g. in a local Facebook group.
- Send it directly to network partners, colleagues and elected representatives.
- Pass it on to the media as press releases.

When do you publish your statement?

- Take your time, observe the situation and assess what strategies the attackers are pursuing.
- Take a digital break and then announce that you are now back online when you feel ready.
- Express your gratitude for digital moral/civic courage and support from your community when you experience it.

How do you frame and spread a successful statement?

- To achieve an impact, the statement should be disseminated on the channel you use to reach your target group.
- Be brief, precise and emphasise your position.
- Give little room for the hostilities and defamations.
- Activate your digital community and promote solidarity and support.
- Be honest and transparent in your statement.
- Avoid statements that contradict your own values.
- If you regret something, apologise for it. Do not take a defensive stance, but an informative one.

3 Recognise the different phases of a crisis

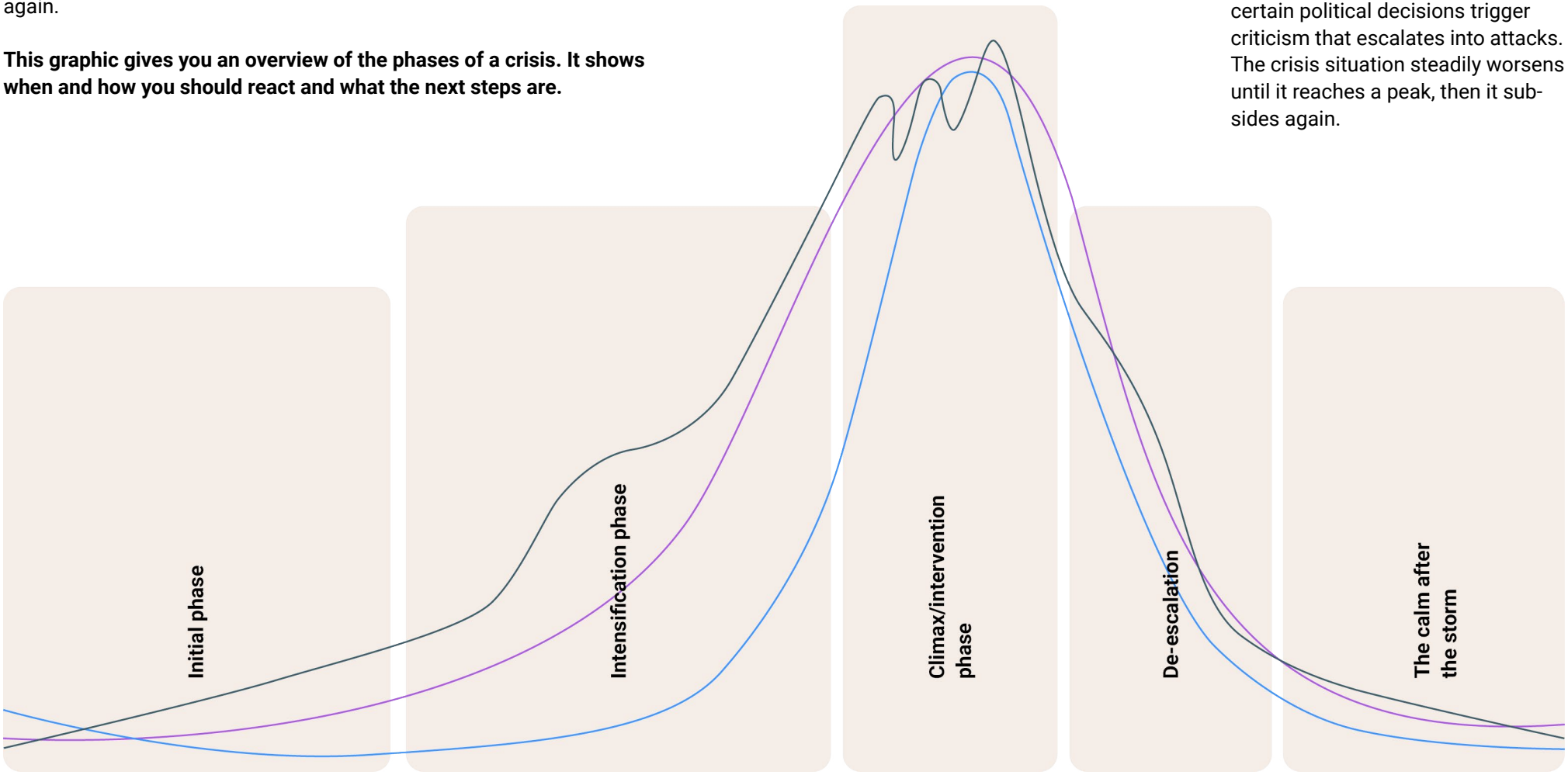
A crisis is caused by several targeted attacks and often occurs in waves. An event, such as a political decision, can initially trigger criticism, which quickly escalates into hostilities. These reach a peak and usually subside again before the issue comes back into focus and the attacks can flare up again.

This graphic gives you an overview of the phases of a crisis. It shows when and how you should react and what the next steps are.

A certain event triggers a crisis situation. The attacks happen suddenly and quickly, reach a peak and and after a short time the situation calms down again.

The crisis does not relate to just one situation, but several individual attacks. Peaks of such a crisis are reached several times as soon as the topic of the attack is present again. Hate waves are often similar to this graphic.

An event or, for example, certain political decisions trigger criticism that escalates into attacks. The crisis situation steadily worsens until it reaches a peak, then it subsides again.



Initial phase

- You are severely criticised and attacked. However, the criticism is not hostile or threatening towards you.
- **Implement preventive measures:** minimise personal information online, check privacy settings, protect your address (e.g. by raising awareness in your social environment), do not make provocative comments.

Intensification phase

- The hostility increases, spreads to other platforms (such as Facebook or the comments section of local newspapers) and can become more violent.
- Rapid development within a few days or even hours.
- **Activate the crisis team.**
- Activate the support network.

Climax/intervention phase

- Your pre-formulated threat scenarios come true.
- The climax of a crisis can be a single event (e.g. a private home address is published) or several incidents of this kind.
- You receive countless comments on your social media channels within a few hours.
- **You implement measures for your analogue and digital security.**
- Keep calm and take your time.

De-escalation

- The hostility decreases and you are no longer the centre of attention.
- You formulate and, where appropriate, publish a statement about the situation.
- **Stay cautious!**
- Conserve resources because the crisis is not over yet.
- There may be further peaks because the topic on which you are being attacked keeps coming up.

The calm after the storm

- You can go back to your normal daily routine.
- **You can reflect on the crisis and evaluate how you have dealt with it.**
- You thank everyone who has supported you.
- If necessary, you implement changes.

4 Acutely affected – what are the specific steps in dealing with a crisis?

Step 1: Keep calm

A crisis situation can be very emotionally stressful and trigger strong feelings.

- Seek support and talk to people close to you about how you feel in this situation.
- Talk to experts at counselling centres or therapists who can support and stabilise you emotionally.
- Create a balance for yourself and consciously engage in activities that give you strength. Think in advance about which activities come into question: meeting up with friends, sports, other hobbies.
- **Fix a time limit (e.g. a maximum of two hours a day) and select a location (e.g. only outside in the park) for dealing with the crisis.** By limiting the time, you can create distance from the acute situation and stress.

Step 2: Activate the crisis team

The crisis coordinator organises a meeting and informs the crisis team about the content of the crisis, the background and the role of each person. Depending on the size of the team, some people will have various roles. **If the team lacks expertise, you should arrange for external support, e.g. from HateAid.** The sooner counselling centres or the police are informed and involved, the better they will be able to provide recommendations for action.

Step 3: Don’t freeze, take action!

Even if a crisis can be extremely overwhelming, you can and should take action. To make it easier for you, you will find a crisis plan poster in the appendix of this brochure. **Use it to distribute the tasks in your crisis team.**

Step 4: Learn from the crisis!

You have been able to take measures to actively deal with the situation. The attacks slowly decrease and the situation normalises. As soon as you can get back to your normal routine, take some time to process the situation. Talk to the crisis team about the crisis situation and analyse how you dealt with it.

Ask yourself the following questions and document the answers:

- Who has supported you? Whom do you want to thank?
- What went well? What gave you strength?
- What went badly? What help and support did you wish for but did not receive?
- What do you want to change in order to be better prepared in the future?
- What happened before the crisis (or in the initial phase) that could serve as a warning signal for future crisis situations?

You will find a summary of possible courses of action and a crisis plan to complete individually at the end of this brochure.

5 Contact us

For the latest information on access and conditions for our counselling service, please check this website: hateaid.org/en/consultation/

By phone

+ 49 (0)30 25208838

By chat

hateaid.org

It is also possible to chat with us. To access our chat, cookies must be activated on our website. A chat bubble will then appear at the bottom right.

Please refer to our website for the office hours of our chat counselling service.

By reporting form

hateaid.org/en/reporting-form

Content can be forwarded to us using the reporting form.
All relevant information should be included in the description of the report. This includes, for example, legally compliant screenshots and links to the relevant platforms on which digital violence has occured.

By email

beratung@hateaid.org

It is possible to send us an email. This should describe the case in detail and include all relevant information including legally compliant screenshots and links to the relevant platforms on which digital violence is taking place.

General questions about our consultation can also be sent to us by email.

By app

hateaid.org/meldehelden-app/

You can also get in touch with us via our free MeldeHelden app. The app is available for download from the Google Play Store and the App Store.

References & Notes

1 See https://lexikon.stangl.eu/16034/psychosoziale-krise

2 See forsa (2023): Hate Speech. Forsa-Studie 2023. Zentrale Untersuchungsergebnisse. URL: https://www.medienanstalt-nrw.de/fileadmin/user_upload/NeueWebsite_0120/Themen/Hass/forsa_LFMNRW_Hassrede2023_Praesentation.pdf (05.12.2024)

3 See Das NETTZ, Gesellschaft für Medienpädagogik und Kommunikationskultur, HateAid und Neue deutsche Medienmacher*innen als Teil des Kompetenznetzwerks gegen Hass im Netz (ed.) (2024): Lauter Hass – leiser Rückzug. Wie Hass im Netz den demokratischen Diskurs bedroht. Ergebnisse einer repräsentativen Befragung. Berlin. URL: https://kompetenznetzwerk-hass-im-netz.de/download_lauterhass.php

4 See forsa (2024): Die Situation ehrenamtlicher Bürgermeisterinnen und Bürgermeister. Ergebnisse einer Befragung für die Körber-Stiftung. URL: https://koerber-stiftung.de/projekte/demokratie-beginnt-vor-ort/.

5 The UK charity Protection Against Stalking describes stalking as ‘a pattern of fixated and obsessive behaviour which is repeated, persistent, intrusive and causes fear of violence or engenders alarm and distress in the victim’. Forms of stalking in the digital space are, for example, repeated messages on social media, by text message or email.

6 Enter the name of the search engine and ‘deletion request according to GDPR’ in the search engine. In the search results, you will find the relevant online forms with which you can request erasure.

7 Further information on your right to erasure under the GDPR and the requirements can be found here: https://www.bfdi.bund.de/EN/Fachthemen/Inhalte/Technik/SDM.html

8 Similar measures are also provided in other European countries, e.g. in Norway, vulnerable persons can apply to the police for the use of fictitious personal data, see § 9-3 Folkeregisterloven in conjunction with §§ 14 a, 14 b Lov om politiet; in Sweden, you can either apply for protected population register data, confidentiality marking or new identity details (for further details see https://www.skatteverket.se/servicelankar/otherlanguages/inenglishengelska/individualsandemployees/protectedidentity); in Great Britain where there is no obligation to register, it is possible, for example, to apply for an anonymous entry in the electoral register in accordance with the Representation of the People Act 1983.

9 Hacking generally refers to the process of technically attacking devices, software or networks. The aim is often to damage the owners of the devices, files or programmes.

10 Phishing is the attempt to steal data (such as passwords or credit card numbers) using fake websites, email addresses or text messages.

11 Cyber incident response refers to the process of responding to IT threats such as cyber attacks or IT security threats. For example in Germany, the Federal Office for Information Security offers support and advice on organisations that can help with the cyber incident response process on their website.

Imprint

Published by
HateAid gGmbH
Greifswalder Straße 4
10405 Berlin
Germany

Telephone: +49 (0) 30 25208802
Email: kontakt@hateaid.org
hateaid.org

Registered office of the company:
Berlin
Register court:
Local court of Berlin-Charlottenburg
Commercial register number:
HRB 203883 B
VAT ID No.: DE322705305

CEOs: Anna-Lena von Hodenberg and Josephine Ballon
Person accountable according to the German Press Law: Anna-Lena von Hodenberg (HateAid gGmbH)
Editing: Basma Bahgat, Katharina Heffe, Anna-Lena von Hodenberg, Samara Feldmann, Eva Pasch, Anna Wegscheider, Stefanie Zacharias
Design: Regina Buschmeier
Print: Umweltdruck Berlin GmbH

Exclusion of liability
The information in this brochure has been drafted with our utmost care and expertise. This guide does not replace individual (legal) advice. The publishers assume no liability for the accuracy, completeness and up-to-dateness of the information.

The first edition of this publication was developed and printed in 2022 as part of the funding of the “Kompetenznetzwerk Hass im Netz” by the German Federal Ministry for Family Affairs, Senior Citizens, Women and Youth‘s “Demokratie leben!“ programme.

This new edition was fundamentally revised, translated and published independently by HateAid gGmbH in 2025.

Donations

As a nonprofit organisation, we rely on donations.

Make the internet a better place and become a HateAid supporter.

Your regular donation flows directly into our daily work – and thus into the diversity of opinion in our democracy.

With just 10 euros per month, you can make it clear that **hate is not an opinion**.

Donation account:
Account holder: HateAid
Bank: GLS Bank
IBAN: DE04 4306 0967 1231 5982 03
BIC: GENODEM1GLS

hateaid.org/en/donate/

Crisis plan to complete individually

You will find a summary of possible courses of action and a crisis plan to complete individually here.

Don’t freeze, take action!

What can you do to remain capable of acting and feel safe in a crisis situation?
And who takes on which tasks?

Analogue security

What should you do?	What do you achieve and who is responsible?
Contact the local police station and request a security talk	Assessment of the hazardous situation by experts gives you control and the ability to act. **Security officer:**
	In consultation with the observer of the attacks:
Create legally compliant screenshots	Legally compliant screenshots document the progression of events and content permanently. This is important if you want to defend yourself legally, e.g. by filing a complaint with the police. **Community manager:**
Request address protection measure	You can find more information on this in the main section of the crisis plan. Please bear in mind that your address may be easily found out in other places and inform yourself and find out about protection options at an early stage. **Privacy guardian:**
Change routines and avoid being alone	Vary your daily routines to make it more difficult to find you and make sure you're accompanied whenever possible, especially in public places. **Organise independently**
Change overnight accommodation at short notice	This allows you to create temporary protection and distance, as well as avoid analogue attacks in the event of acute threats. As a preventative measure, draw up a list of people who are close to you and with whom you can stay for a transitional period. **Organise independently**
Inform and sensitise your social environment	Make your social environment, e.g. family, friends and neighbours, aware of your situation and get emotional support if necessary. Sensitise your family members' educational institutions to handle your personal data with particular care. **Inform your own neighbours independently.** **Office colleagues will be informed by the crisis coordinator:**
For events where you are invited as a guest: ask for a registration list, organise security staff and have house rules drawn up.	You get an overview of who is taking part in events and can prepare yourself and avert dangers if necessary. **Independently in consultation with the safeguard for netiquette:**
Consistently press criminal charges	The police will be informed about your situation through reports and can take security measures if necessary. In addition, unknown perpetrators can be identified through appropriate investigative measures and subsequently be brought to justice. **Security officer, if applicable, together with the person against whom the attacks are directed:**

Stand your ground

What should you do?	What do you achieve and who is responsible?
Publish a statement	You can present your own position clearly. **Press spokesperson:**
Get in touch with the local newspaper	You can disseminate your own position to different target groups and give the topic more credibility and importance. **Press spokesperson:**

Digital security

What should you do?	What do you achieve and who is responsible?
Change passwords	Strong passwords reduce the risk of hacking. A password manager can help you with this. This is a tool that generates secure passwords and stores them in a database for you. **Independently in consultation with the IT security officer:**
Set up two-factor authentication	Two-factor authentication impedes hacking attacks because you log in not just with your password, but with additional information. Authentication can be carried out using a code that is sent to you by email, for example. **Independently in consultation with the IT security officer:**
Search for and delete sensitive data on the internet	You protect your own privacy. **Privacy guardian:** (contact HateAid for support if necessary)
Involve external IT expertise if hacking is suspected	Hacking attacks can be dangerous on different levels. With external support, you can restore your own IT security and enhance the investigation of the incident. **IT security officer:**

Social media communication

What should you do?	What do you achieve and who is responsible?
Restrict the comment function on your own social media channels	You customise the comment settings in the comment function (e.g. 'public' → 'private', or a block list for specific terms). **Community manager:**
Deactivate social media accounts for a short time if necessary	Your account will not be deleted but made invisible for a period of time. If you want to use your account again after the crisis, you usually just have to log in again. This ends the deactivation. Deactivating the account temporarily can contribute to more relief and distancing. **Community manager:**
Report content on social media platforms	If legally compliant screenshots have already been created (see left), you can report the content. Ideally, reported content will be deleted by the platform. **Community manager:**
Block attackers on social media platforms	If you report the profiles of the attackers and block them for yourself, these people will not see what you publish in the future and will not be able to contact you. **Community manager:**
Consistently delete comments that contradict the netiquette	You create a safe place for people who want to interact respectfully with you and with others. **Community manager:** **In consultation with the safeguard for netiquette:**
Activate supporters	In this way, you can seek and activate support and solidarity on your channels, e.g. in the form of public encouragement from cooperation partners or counter-speech. **Crisis coordinator:**

Hate Aid