OFEK e.V., Postfach 58 03 16, 10413 Berlin

Privacy policy
Valid as of 21 July 2025

The operators of these pages take the protection of your personal data very seriously. We treat your personal data confidentially and in accordance with the statutory data protection regulations and this privacy policy.

When you use this website, various personal data are collected. Personal data is data with which you can be personally identified. This privacy policy explains what data we collect and what we use it for. It also explains how and for what purpose this is done, whether your personal data is transmitted and how long we keep it.

Note on the responsible entity
The responsible party is the natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data (e.g. names, e-mail addresses, etc.).
The responsible party for data processing on this website and the services offered on it is:

OFEK e.V. – Beratungsstelle bei antisemitischer Gewalt und Diskriminierung
Register court: Amtsgericht Charlottenburg
Register of associations: VR 37581 B
Sales tax identification number: 27 / 674 / 51693
Management: Marina Chernivsky
Phone: (+49) (0)30 610 80 458
E-mail: kontakt@ofek-beratung.de
Address: Postfach 58 03 16, 10413 Berlin

Data Protection Officer:
Email: datenschutz@ofek-beratung.de

Data processing on our website

Cookies / Cookie banner

This website partly uses so-called cookies. Cookies do not cause any damage to your computer and do not contain viruses. Cookies serve to make our offer more user-friendly, more effective and safer. Cookies are small text files that are stored on your computer and saved by your browser.

Most of the cookies we use are so-called “session cookies”. They are automatically deleted after the end of your visit. Other cookies remain stored on your terminal device until you delete them. These cookies allow us to recognize your browser on your next visit.

With the help of the cookie banner, you can inform yourself at the beginning of your visit and at any time about the cookies used by us and our service providers and set which cookies may be used or give your consent to the use of cookies, insofar as this is legally required.

In addition, you can set your browser so that you are informed about the setting of cookies and only allow cookies in individual cases, exclude the acceptance of cookies for certain cases or in general and activate the automatic deletion of cookies when closing the browser. When deactivating cookies, the functionality of this website may be limited.

Cookies that are required to carry out the electronic communication process are stored on the basis of Art. 6 (1) lit. f GDPR due to the legitimate interest of the provider. The provider has a legitimate interest in storing cookies for the technically error-free and optimized provision of its services. Insofar as other cookies (e.g. cookies for the analysis of your surfing behavior) are stored, these are treated separately in this privacy policy.

The necessary cookies used on our website include those set by the service provider “Complianz” (Complianz B.V., Kalmarweg 14-5, 9723 JG Groningen, The Netherlands) to store the cookie settings you have made and any consents you have given. Complianz is installed on our servers, so no connection is made to the servers of Complianz's provider. Complianz stores a cookie in your browser in order to be able to assign the consents given to you or their revocation. The data collected in this way is stored until you request us to delete it, delete the Complianz cookie yourself or the purpose for storing the data no longer applies. Mandatory legal

storage obligations remain unaffected. The legal basis for this is Art. 6 para. 1 lit. c GDPR.

Server log files
The provider of the website automatically collects and stores information in so-called server log files, which your browser automatically transmits to us. These are:
- Browser type and version
- Operating system used
- Referrer URL
- Host name of the accessing computer
- Time of the server request
- IP address

This data is not merged with other data sources.

The server log files are stored on the basis of Art. 6 para. 1 lit. f GDPR in the legitimate interest of the provider. The provider has a legitimate interest in the creation of server log files for the technically error-free and optimized provision of its services. The server log files are deleted 365 days after their collection.

Separate consent to data processing for consulting purposes
In order to give you the opportunity to consent to the processing of your personal data in the context of our consultation after you have contacted us anonymously by telephone or e-mail, we use a corresponding form on a subpage of our website.

We use the e-mail address you provide there to carry out the so-called “double opt-in procedure” in order to prevent the misuse of your e-mail address by requesting a confirmation that is sent to the email address provided. In addition, we use the e-mail address you provide there together with your name, IP address, time and date as well as the subject of your consent in order to be able to document this in an evidential manner.

This data is deleted as soon as you call us to do so or three months after the conclusion of the consultation.

The legal basis for this is your consent pursuant to Art. 6 para. 1 lit a GDPR, if applicable in conjunction with Art. 9 para. 1 lit a GDPR.

YouTube plugins
Our website uses plugins from the YouTube site operated by Google. The operator of the pages is YouTube, LLC, 901 Cherry Ave, San Bruno, CA 94066, USA.

When you visit one of our pages equipped with a YouTube plugin, a connection to the YouTube servers is established. This tells the YouTube server which of our pages you have visited.

If you are logged into your YouTube account, you enable YouTube to assign your surfing behaviour directly to your personal profile. You can prevent this by logging out of your YouTube account.

YouTube is used in the interest of an appealing presentation of our online offers. This represents a legitimate interest within the meaning of Art. 6 para. 1 lit. f GDPR.

For more information on the handling of user data, please refer to YouTube's privacy policy at:
https://www.google.de/intl/de/policies/privacy.

Newsletter
If you would like to receive the newsletter offered on the website, we require an email address from you as well as information that allows us to verify that you are the owner of the specified email address and agree to receive the newsletter. Further data is not collected or only on a voluntary basis.

We use this data exclusively for sending the requested information.

We use MailChimp to send the newsletter. The provider is Rocket Science Group LLC, 675 Ponce De Leon Ave NE, Suite 5000, Atlanta, GA 30308, USA.

When you enter data for the purpose of receiving the newsletter (email address), this data is stored on MailChimp's servers in the USA.
With the help of MailChimp, we can analyze our newsletter campaigns. When you open an email sent with MailChimp, a file contained in the email (so-called web-beacon) connects to the servers of MailChimp in the USA. This makes it possible to determine whether a newsletter message has been opened and which links, if any, have been clicked. In addition, technical information is recorded (e.g. time of retrieval, IP address,

browser type and operating system). This information cannot be assigned to the respective newsletter recipient. It is used exclusively for the statistical analysis of newsletter campaigns. The results of these analyses can be used to better adapt future newsletters to the interests of the recipients.
If you do not want any analysis by MailChimp, you must unsubscribe from the newsletter. For this purpose, we provide a corresponding link in every newsletter message. Furthermore, you can also unsubscribe from the newsletter directly on the website.
For more details, please refer to the privacy policy of MailChimp at: https://mailchimp.com/legal/terms/.

We have concluded a so-called "Data-Processing-Agreement" with MailChimp, in which we oblige MailChimp to protect the data of our customers and not to pass them on to third parties. This agreement can be viewed at the following link: https://mailchimp.com/legal/forms/data-processingagreement/sample-agreement/.

Online presence in social media
We maintain online presences within social networks and platforms in order to be able to communicate with the customers, interested parties and users active there and to inform them about our services there.

We would like to point out that user data may be processed outside the European Union. This may result in risks for the users, because it could, for example, make it more difficult to enforce the rights of the users. With regard to U.S. providers that are certified under the Privacy Shield, we point out that they thereby undertake to comply with the data protection standards of the EU.

Furthermore, user data is usually processed for market research and advertising purposes. For example, usage profiles can be created from the usage behaviour and resulting interests of the users. The usage profiles can in turn be used, for example, to place advertisements within and outside the platforms that presumably correspond to the interests of the users. For these purposes, cookies are usually stored on the users' computers, in which the usage behaviour and interests of the users are stored. Furthermore, data may also be stored in the usage profiles regardless of the devices used by the users (especially if the users are members of the respective platforms and are logged in to them).

The processing of users' personal data is based on our legitimate interests in providing users with effective information and communication with users pursuant to Art. 6 para. 1 lit. f. GDPR. If users are asked by the respective providers for consent to data processing (i.e. declare their consent, e.g. by ticking a checkbox or confirming a button), the legal basis for processing is Art. 6 (1) lit. a., Art. 7 GDPR. For a detailed description of the respective processing and the opt-out options, please refer to the information of the providers linked below.

Also in the case of requests for information and the assertion of user rights, we point out that these can be asserted most effectively with the providers. Only the providers have access to the users' data and can take appropriate measures and provide information directly. If you still need help, you can contact us.

We use social media services from the following providers:

- Facebook and Instagram (Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Republic of Ireland) – Privacy Policy: https://www.facebook.com/about/privacy/, Opt-Out: https://www.facebook.com/settings?tab=ads und http://www.youronlinechoices.com.
- Google / YouTube (Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA) – Privacy Policy: https://policies.google.com/privacy, Opt-Out: https://adssettings.google.com/authenticated.
- X (Twitter International Unlimited Company, One Cumberland Place, Fenian Street Dublin 2, D02 AX07, Republic of Ireland) – Privacy Policy: https://twitter.com/de/privacy, Opt-Out: https://twitter.com/personalization.
- Bluesky (Bluesky PBLLC) – Privacy Policy: https://blueskyweb.xyz/support/privacy-policy.
- LinkedIn (LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Republic of Ireland) – Privacy Policy: https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy.
- Linktree (Instant EU GDPR Representative Ltd 69 Esker Woods Drive, Lucan Co. Dublin, Republic of Ireland) – Privacy Policy: https://linktr.ee/s/privacy/, Opt-Out: https://linktr.ee/s/gdpr-form/.

Data processing in the context of consulting via telephone and email
In the context of consulting via telephone and email, we may process personal data to enable contact with you and in the context of the

consultation to record and document the subject of the consultation, to advise you, to refer you to other agencies for legal or psychological advice if you expressly request this, and for anonymous statistical evaluation of our consulting services.

You can, of course, make use of our consulting services without giving your name or other personal characteristics if you wish.

The following categories of data may be processed:
- Names
- Email address, telephone number, postal address
- Consultation facts (events, behavior, date, place, circumstances)
- special personal data such as ethnic origin, political opinions, religious or ideological beliefs or health data

The legal basis for the collection and processing of your personal data is your express consent pursuant to Art. 6 para. 1 lit. a GDPR, possibly in conjunction with Art. 9 para. 1 lit. a GDPR.

Your personal data will only be passed on to third parties for the purpose of arranging further consulting services and on the basis of your express consent.

You can revoke your consent at any time. For this purpose, the contacts indicated above are at your disposal.

We delete your personal data three months after the conclusion of the consultation.

Data processing in the context of press inquiries and general inquiries
To respond to press inquiries to presse@ofek-beratung.de and general inquiries to info@ofekberatung.de, we process the following personal data to establish contact with you and answer your questions:
- Names
- Addresses, telephone numbers

We process this data on the legal basis of Art. 6 para. 1 lit. f GDPR as it is in our legitimate interest to conduct public relations in direct contact with interested parties.

You can object to the processing of your personal data in this context at any time. For this purpose, the contacts indicated above are available to you.

The data will be deleted as soon as your requests have been answered comprehensively.

Transmission of personal data
In the course of processing personal data on this website or during consultation, it may happen that the data is transferred to or disclosed to other bodies, companies, legally independent organizational units or persons.
Recipients of this data may include, for example, service providers commissioned with IT tasks or providers of other services. In such cases, we comply with the legal requirements and conclude contracts or agreements that serve to protect your data with the recipients of your data.

Security measures
In accordance with the legal requirements and taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the different probabilities of occurrence and the extent of the threat to the rights and freedoms of natural persons, we take appropriate technical and organizational measures to ensure a level of protection appropriate to the risk.

These measures include, in particular, safeguarding the confidentiality, integrity and availability of data by controlling physical and electronic access to the data as well as the access, input, transfer, safeguarding of availability and its separation. Furthermore, we have established procedures to ensure the exercise of data subjects' rights, the deletion of data, and responses to data compromise. Furthermore, we take the protection of personal data into account as early as the development or selection of hardware, software and processes in accordance with the principle of data protection, through technology design and through data protection-friendly default settings.

Shortening of the IP address: If IP addresses are processed by us or by the service providers and technologies used and the processing of a

complete IP address is not necessary, the IP address is shortened. With the shortening of the IP address, the identification of a person by their IP address is prevented or at least made significantly more difficult.

SSL encryption (https): To protect your data transmitted via our online offer, we use SSL encryption. You can recognize such encrypted connections by the prefix https:// in the address bar of your browser.

Children and teenagers

As a matter of principle, persons under the age of 18 should not transmit any personal data to us without the consent of their parents or legal guardians. Furthermore, we expressly point out that we neither explicitly request nor collect personal data from children and young people, nor do we pass it on to third parties.

Data subject rights

Right of access

You may request confirmation from the responsible party as to whether personal data concerning you is being processed by us. If there is such processing, you can request information from the responsible party about the following:

- the purposes for which the personal data are processed;
- the categories of personal data which are processed;
- the recipients or categories of recipients to whom the personal data concerning you have been or will be disclosed;
- the planned duration of the storage of the personal data concerning you or, if concrete information on this is not possible, criteria for determining the storage duration;
- the existence of a right to rectification or erasure of personal data concerning you, a right to restriction of processing by the responsible party or a right to object to such processing;
- the existence of a right of appeal to a supervisory authority;
- any available information on the origin of the data, if the personal data are not collected from the data subject;
- the existence of automated decision-making, including profiling, pursuant to Article 22(1) and (4) of the GDPR and, at least in these cases, meaningful information about the logic involved and the scope and intended effects of such processing for the data subject.

You have the right to request information about whether the personal data concerning you is transferred to a third country or to an international organization. In this context, you may request to be informed about the appropriate safeguards pursuant to Art. 46 GDPR in connection with the transfer.

Right to rectification
You have a right to rectification and/or completion vis-à-vis the responsible party if the personal data processed concerning you are inaccurate or incomplete. The responsible party shall carry out the rectification without undue delay.

Right to restriction of processing
Under the following conditions, you may request the restriction of the processing of personal data concerning you:
- if you contest the accuracy of the personal data concerning you for a period enabling the responsible party to verify the accuracy of the personal data;
- the processing is unlawful and you object to the erasure of the personal data and request instead the restriction of the use of the personal data;
- the responsible party no longer needs the personal data for the purposes of processing, but you need them for the assertion, exercise or defense of legal claims, or
- if you have objected to the processing pursuant to Art. 21 (1) GDPR and it is not yet clear whether the legitimate grounds of the responsible party outweigh your grounds.

Where the processing of personal data concerning you has been restricted, such data may be processed, with the exception of storage, only with your consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or a Member State. If the restriction of processing has been restricted in accordance with the above conditions, you will be informed by the responsible party before the restriction is lifted.

Right to erasure
a) Obligation to delete
You may request the responsible party to delete the personal data concerning you without undue delay, and the responsible party is obliged

to delete such data without undue delay, if one of the following reasons applies:

- The personal data concerning you are no longer necessary for the purposes for which they were collected or otherwise processed.
- You revoke your consent on which the processing was based pursuant to Art. 6 (1) a or Art. 9 (2) a GDPR and there is no other legal basis for the processing.
- You object to the processing pursuant to Art. 21 (1) GDPR and there are no overriding legitimate grounds for the processing, or you object to the processing pursuant to Art. 21 (2) GDPR.
- The personal data concerning you have been processed unlawfully.
- The deletion of the personal data concerning you is necessary for compliance with a legal obligation under Union or Member State law to which the responsible party is subject.
- The personal data concerning you was collected in relation to information society services offered pursuant to Art. 8 (1) GDPR.

b) Information to third parties

If the responsible party has made the personal data concerning you public and is obliged to erase it pursuant to Article 17(1) of the GDPR, it shall take reasonable measures, including technical measures, having regard to the available technology and the cost of implementation, to inform data responsible parties which process the personal data that you, as the data subject, have requested that they erase all links to or copies or replications of such personal data.

c) Exceptions

The right to erasure does not exist insofar as the processing is necessary to

- to exercise the right to freedom of expression and information;
- for compliance with a legal obligation which requires processing under Union or Member State law to which the responsible party is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the responsible party;
- for reasons of public interest in the area of public health pursuant to Art. 9(2)(h) and (i) and Art. 9(3) GDPR;
- for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes pursuant to Article 89(1) of the GDPR, insofar as the right referred to in Section a) is likely

to render impossible or seriously prejudice the achievement of the purposes of such processing, or
- for the assertion, exercise or defense of legal claims.

Right to information
If you have asserted the right to rectification, erasure or restriction of processing against the responsible party, the responsible party is obliged to inform all recipients to whom the personal data concerning you have been disclosed of this rectification or erasure of the data or restriction of processing, unless this proves impossible or involves a disproportionate effort.
You have the right against the responsible party to be informed about these recipients.

Right to data portability
You have the right to receive the personal data concerning you that you have provided to the responsible party in a structured, common and machine-readable format. You also have the right to transfer this data to another responsible party without hindrance from the responsible party to whom the personal data was provided, provided that
- the processing is based on consent pursuant to Art. 6 (1) a GDPR or Art. 9 (2) a GDPR or on a contract pursuant to Art. 6 (1) b GDPR and
- the processing is carried out with the help of automated procedures.

In exercising this right, you also have the right to have the personal data concerning you transferred directly from one responsible party to another responsible party, insofar as this is technically feasible. Freedoms and rights of other persons must not be affected by this.
The right to data portability does not apply to processing of personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the responsible party.

Right of objection
You have the right to object at any time, on grounds relating to your particular situation, to the processing of personal data relating to you which is carried out on the basis of Article 6(1)(e) or (f) GDPR; this also applies to profiling based on these provisions.

You may object at any time by writing to the following address:
datenschutz@ofek-beratung.de
OFEK e.V. –Beratungsstelle bei antisemitischer Gewalt und Diskriminierung
Postfach 58 03 16, 10413 Berlin

The responsible party shall no longer process the personal data concerning you unless it can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defense of legal claims.
If the personal data concerning you is processed for the purposes of direct marketing, you have the right to object at any time to processing of the personal data concerning you for the purposes of such marketing; this also applies to profiling, insofar as it is related to such direct marketing.
If you object to the processing for direct marketing purposes, the personal data concerning you will no longer be processed for these purposes.
You have the possibility, in connection with the use of information society services, notwithstanding Directive 2002/58/EC, to exercise your right to object by means of automated procedures using technical specifications.

Right to revoke the declaration of consent under data protection law
You have the right to revoke your declaration of consent under data protection law at any time. The revocation of consent does not affect the lawfulness of the processing carried out on the basis of the consent until the revocation.

Automated decision in individual cases including profiling
You have the right not to be subject to a decision based solely on automated processing - including profiling - which produces legal effects vis-à-vis you or similarly significantly affects you. This does not apply if the decision

- is necessary for the conclusion or fulfilment of a contract between you and the responsible party,
- is permitted by legislation of the Union or the Member States to which the responsible party is subject and that legislation contains appropriate measures to safeguard your rights and freedoms and your legitimate interests, or
- is done with your express consent.

However, these decisions may not be based on special categories of personal data pursuant to Article 9(1) of the GDPR, unless Article 9(2)(a) or (g) of the GDPR applies and appropriate measures have been taken to protect the rights and freedoms and your legitimate interests.
With regard to the cases mentioned in a) and c), the responsible party shall take reasonable steps to safeguard the rights and freedoms as well as your legitimate interests, which include at least the right to obtain the intervention of a person on the part of the responsible party, to express his or her point of view and to contest the decision.

Right to lodge a complaint with a supervisory authority
Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your residence, place of work or place of the alleged infringement, if you consider that the processing of personal data relating to you infringes the GDPR.

The supervisory authority to which the complaint has been lodged shall inform the complainant of the status and outcome of the complaint, including the possibility of a judicial remedy under Article 78 GDPR.

Privacy policy update
Since we adapt this data protection declaration as soon as changes in the data processing carried out by us make this necessary, we ask you to inform yourself regularly about its content.

We will inform you as soon as any changes require your cooperation (e.g. consent) or other individual notification.

Where we provide contact information in this Privacy Policy, please note that addresses may change over time and check the information before contacting us.