



Privacy Policy

01.07.2026

Wenn Sie eines unserer Angebote nutzen, verarbeitet die MHS Print GmbH Ihre personenbezogenen Daten. Mit diesen Datenschutzhinweisen informieren wir Sie, wie und warum wir Ihre Daten verarbeiten und wie wir gewährleisten, dass sie vertraulich bleiben und geschützt sind.

We take data protection seriously: as a matter of principle, we only process personal data if this is necessary for the provision of a service or offer or if it is provided voluntarily by the user. We also use technical and operational security measures to protect personal data against accidental or intentional manipulation, loss, destruction or access by unauthorised persons. We regularly review and modernise these precautions.

Privacy policy for applications

If you have applied for a job with us, you will find the necessary data protection information [here](#).

Data protection at a glance

What data do we collect?

- Inventory data (e.g., names, addresses)
- Contact details (e.g., email, phone numbers)
- Content data (e.g., entries in online forms)
- Payment data (e.g., bank details, invoices, payment history)
- Contract data (e.g., subject matter of the contract, term)
- Usage data (e.g., websites visited, interest in content, access times)
- Meta/communication data (e.g., device information, IP addresses, ID)

How do we collect the data?

We collect the data that is generated when you access our digital offers automatically. Otherwise, we collect data based on your entries or messages or through the use of cookies or similar technologies.

What do we use the data for?

Bereitstellung der Inhalte:

- Cookies und ähnliche Technologien
- technische Bereitstellung und Sicherheit
- Unbedingt erforderliche Technologie

Nutzungsanalyse und Produktoptimierung:

- Weiterentwicklung der Nutzerfreundlichkeit

Personalisierte Inhalte und Marketing

- Marketing für eigene Produkte

Um Ihnen weitere Services zur Verfügung zu stellen

Wenn Sie die folgenden Services der MHS Print nutzen - die nicht mehr vom Vertrag mit Werbung umfasst sind - finden die Datenverarbeitungen aufgrund der in der jeweiligen Beschreibung angegebenen Rechtsgrundlagen statt:

- Direktwerbung
- Kontakt und Kommunikation
- Videokonferenzen

Do we share data?

If you have given your consent or we are otherwise legally authorized to do so, we will pass on your personal data to service providers (e.g., hosting, marketing, sales partners, payment service providers) for the above-mentioned purposes. In such cases, we comply with the legal requirements and, in particular, conclude appropriate contracts or agreements with the recipients of your data to protect your data.

We transfer personal data to other companies within our group of companies or grant them access to this data for administrative purposes. This transfer of data is based on our legitimate business and economic interests or takes place if it is necessary to fulfill our contractual obligations or if the consent of the data subjects or legal permission has been obtained.

Do we transfer data to third countries?

In order to use our digital services, it may be necessary to transfer certain personal data to third countries, i.e. countries where the GDPR does not apply. However, we only allow your data to be processed in a third country if the specific requirements of Art. 44 ff. GDPR are met and thus an adequate level of data protection is guaranteed in that country. This means that the third country must either have an adequacy decision by the European Commission or suitable safeguards in accordance with Art. 46 GDPR or one of the conditions of Art. 49 GDPR. **Unless otherwise stated below, we use the currently valid [standard contractual clauses](<https://eur->**

<lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32021D0914&from=DE>

“current version of the standard contractual clauses”) for the transfer of personal data to processors in third countries.

How do we secure the data?

In order to protect your privacy and ensure a level of protection appropriate to the risk, we take technical and organizational measures in accordance with legal requirements, taking into account the state of the art, implementation costs, and the nature, scope, circumstances, and purposes of processing, as well as the varying likelihood and severity of threats to the rights and freedoms of natural persons. These measures ensure the confidentiality, integrity, availability, and resilience of your data. This includes, among other things, the use of recognized encryption methods (SSL or TLS) and pseudonymization.

However, we would like to point out that, due to the structure of the Internet, it is possible that the rules of data protection and the above-mentioned security measures may not be observed by other persons or institutions outside our area of responsibility. In particular, unencrypted data disclosed, e.g., by email, may be read by third parties. We have no technical influence on this.

When do we delete the data?

We delete or anonymize your personal data as soon as it is no longer required for the purposes for which we collected or used it.

However, we may still need to store your data until the expiry of the retention obligations and periods imposed by the legislator or supervisory authorities, which may arise from the German Commercial Code, the German Fiscal Code, and the German Money Laundering Act (usually 6 to 10 years). In addition, we may retain your data until the expiry of the statutory limitation periods (i.e., usually 3 years, but in individual cases up to 30 years) if this is necessary for the assertion, exercise, or defense of legal claims. After that, the relevant data will be deleted.

What rights do you have?

- Information
- Deletion
- Correction
- Objection

You can contact the data protection officer with your request by mail or by email at swmh-datenschutz@atarax.de.

This privacy policy is updated from time to time. The date of the last update can be found at the beginning of this information.

How we make our content available to you

Cookies and similar technologies

If cookies, device identifiers, or other personal data are stored or accessed on your device for processing purposes, this is done on one of the legal bases of Art. 6 GDPR.

In order to be able to provide the telemedia service you have expressly requested, we also take into account the provisions of Section 25 of the German Telecommunications Digital Services Data Protection Act (TDDDG), in particular the requirement under Section 25 (2) No. 2 TDDDG.

You can find an overview of the technologies used under Privacy settings.

Types and functions of cookies

Cookies are text files that contain data from visited websites or domains and are stored by a browser on users' devices. A cookie primarily serves to store information about a user during or after their visit to an online offering. The stored information may include, for example, language settings on a website, login status, a shopping cart, or video interactions. The term “cookies” also includes other technologies that perform the same functions as cookies (e.g., when user information is stored using pseudonymous online identifiers, also known as “user IDs”).

There are the following types of cookies and functions:

- **Temporary cookies (also known as session cookies):** Temporary cookies are deleted at the latest after a user leaves an online offering and closes their browser.
- **Permanent cookies:** Permanent cookies remain stored even after the browser is closed. This allows, for example, the login status to be saved or preferred content to be displayed directly when the user visits a website again. Similarly, the interests of users, which are used for reach measurement or marketing purposes, can be stored in such a cookie.
- **First-party cookies:** First-party cookies are set and used by us to process user information.
- **Third-party cookies:** Third-party cookies are mainly used by advertisers (so-called third parties) or other partners to process user information.
- **Strictly necessary (also: essential or necessary) cookies:** These cookies ensure functions without which these digital offerings could not be used as desired. They may be absolutely necessary for the operation of a website, for example to store logins or other user entries, or for security reasons.
- **Analysis and statistics cookies:** These cookies enable us to analyze the use of our digital offerings, in particular to measure reach—i.e., clicks, visits, and visitor numbers. The aim is to statistically determine the number of visits and visitors and their surfing behavior (duration, origin) and thus obtain market-wide comparable values. The information collected is evaluated in aggregate form in order to derive improvements and optimizations for our products.
- **Marketing and personalization cookies:** Cookies are also used to store a user's interests or behavior (e.g., viewing certain content, using functions, etc.) in a user profile. Such profiles are used, for example, to display content to users that corresponds to their potential interests.

This process is also referred to as “tracking,” i.e., tracking the potential interests of users. If we use cookies or tracking technologies, we will provide separate information about this in our privacy policy or when obtaining consent.

Technical provision and security

When our offer is used, we automatically employ essential technologies and process the following information:

- Information about the accessing device and the software used
- Date and time of access
- Websites from which the user accesses our website or which the user visits via our website
- IP address

The collection of these logs and their temporary storage and processing are necessary to ensure system security and integrity (in particular to ward off and defend against attempts at attack or damage) and are carried out in accordance with our legitimate interest (§ 25 (2) No. 2 TDDDG, Art. 6 (1) f GDPR).

The storage period for this log data is usually seven days; for reliable detection of AI bots, it is 30 days. From this point on, this specific server log data is anonymized based on our legitimate interest in statistical evaluation to assess AI bots and their impact on our content (Art. 6 (1) f GDPR).

The legal basis for the aforementioned data processing is our legitimate interest pursuant to Art. 6 para. 1 sentence 1 lit. f) GDPR.

Essential technology

The following tools and cookies are strictly necessary technologies, i.e., essential for providing our services as requested by the user.

The legal basis for the data processing described below is our legitimate interest pursuant to Art. 6 (1) (f) GDPR.

Google Tag Manager

The Google Tag Manager service is an organizational tool that enables us to control services. The tool only uses the IP address to establish a connection to the server and to function technically. Otherwise, no personal data is processed by the tool itself. Tag Manager ensures that other services are only executed if the conditions (tags) specified in Tag Manager are met. This allows us to ensure, for example, that tools requiring consent are only loaded after you have given your consent. Tag Manager does not access the data processed by the tools.

Consent management

In order to obtain and store your consent under data protection law, we use the consent management platform from Sourcepoint (Sourcepoint Technologies, Inc., 228 Park Avenue South, #87903, New York, NY 10003-1502, United States). This platform uses strictly necessary cookies to query the consent status and thus display the corresponding content.

The data is stored for a maximum of 13 months.

Cookie	Purpose	Duration	Type
consentUUID	UniqueUserID to store the user's consent status	12 months	Cookie
_sp_su	Identification of users for sampling consent rates reporting	12 months	Cookie
_sp_user_consent	UniqueUserID to retrieve the user's consent status stored in our database if necessary	Unlimited	Local storage
_sp_local_state	Determines whether a user has seen the	unlimited	local storage

Cookie	Purpose	Duration	Type
	consent banner so that it is only shown once		
_sp_non_keyed_ local_state	Information about the metadata and the user's UniqueUserID	unlimited	local storage

How we optimize our products

Further development of user-friendliness

We use cookies and tracking tools to optimize our digital offerings based on your usage. To do this, we measure the development of reach and the use of content and functions, and use A/B testing to determine which variants users prefer.

When you contact us

Contacting us

When you contact us, we only collect personal data (e.g. name, e-mail address, telephone number) if you provide it to us voluntarily. This information is expressly provided on a voluntary basis. The purpose of processing your data is to process and respond to your enquiry. This is also

our legitimate interest in data processing in accordance with Art. 6 para. 1 sentence 1 lit. f) GDPR.

In the case of a telephone enquiry, your data will also be processed by telephone applications and in some cases also via a voice dialogue system in order to support us in the distribution and processing of enquiries.

We will delete your data that we have received in the course of contacting you as soon as your request has been fully processed and no further communication with you is required or requested by you.

When we advertise our products

Direct marketing

We also use your contact data beyond contract-related use for advertising purposes. This is only done if you have expressly consented (Art. 6 para. 1 lit. a) GDPR) or on the basis of our legitimate interest in a personalised customer approach or direct advertising (Art. 6 para. 1 lit. f) GDPR), for example for information about the same and similar products of our company (Section 7 para. 3 UWG).

If you no longer wish to receive advertising, you can withdraw your consent or object to advertising at any time.

The data processed by us will be deleted as soon as they are no longer required for their intended purpose, you have objected to the advertising and the deletion does not conflict with any statutory retention requirements.

- per Mail an info@mhsprint.de
- schriftlich an MHS Print GmbH Zeppelinstraße 116 73730 Esslingen (bitte Mailadresse und den Namen von der Registrierung angeben)
- durch einen Klick auf den Abmelde-Link am Ende der Mail

Marketing for own products

In order to show you adverts for our own products, we use the services of advertising partners or cooperate with advertising partners and advertising networks (remarketing). These use cookies, pixels or similar technical means to display and analyse advertisements.

Adverts can be adapted to the respective user, for example by using information from the browser on usage (such as pages visited, visiting times, length of stay). User-specific adverts are also possible. In addition, analyses of reach or for billing purposes can be carried out in pseudonymised form. The details of the services used, co-operation partners and individual objection options are presented below.

The legal basis for data processing is your consent in accordance with Art. 6 para. 1 lit. a) GDPR.

When you contact us

Contacting us

When you contact us, we only collect personal data (e.g. name, e-mail address, telephone number) if you provide it to us voluntarily. This information is expressly provided on a voluntary basis. The purpose of processing your data is to process and respond to your enquiry. This is also our legitimate interest in data processing in accordance with Art. 6 para. 1 sentence 1 lit. f) GDPR.

In the case of a telephone enquiry, your data will also be processed by telephone applications and in some cases also via a voice dialogue system in order to support us in the distribution and processing of enquiries.

We will delete your data that we have received in the course of contacting you as soon as your request has been fully processed and no further communication with you is required or requested by you.

Videokonferenzen

1. Microsoft Teams

Wir nutzen das Tool „Microsoft Teams“, um Telefonkonferenzen, Online-Meetings, Videokonferenzen und/oder Web-Konferenzen durchzuführen (nachfolgend: „Online-Meetings“). „Microsoft Teams“ ist ein Service der Microsoft Corporation (Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, USA). Wenn wir Online-Veranstaltungen aufzeichnen wollen, werden wir Ihnen das vorab transparent mitteilen und – soweit erforderlich – um eine Zustimmung bitten. Die Tatsache der Aufzeichnung wird Ihnen zudem in der MS-Teams-App angezeigt.

Hinweis: Soweit Sie die Internetseite von „Microsoft Teams“ aufrufen, ist der Anbieter von „Microsoft Teams“ für die Datenverarbeitung verantwortlich. Ein Aufruf der Internetseite ist für die Nutzung von „Microsoft Teams“ jedoch nur erforderlich, um sich die Software für die Nutzung von „Microsoft Teams“ herunterzuladen.

Wenn Sie die „Microsoft Teams“-App nicht nutzen wollen oder können, können Sie „Microsoft Teams“ auch über Ihren Browser nutzen. Der Dienst wird dann insoweit auch über die Website von „Microsoft Teams“ erbracht.

Bei der Nutzung von „Microsoft Teams“ werden verschiedene Datenarten verarbeitet. Der Umfang der Daten hängt dabei auch davon ab, welche Angaben zu Daten Sie vor bzw. bei der Teilnahme an einem „Online-Meeting“ machen.

Folgende personenbezogene Daten sind Gegenstand der Verarbeitung:

- Angaben zum Benutzer: z. B. Anzeigename („Display name“), ggf. E-Mail-Adresse, Profilbild (optional), bevorzugte Sprache
- Meeting-Metadaten: z. B. Datum, Uhrzeit, Meeting-ID, Telefonnummern, Ort
- Text-, Audio- und Videodaten: Sie haben ggf. die Möglichkeit, in einem „Online-Meeting“ die Chatfunktion zu nutzen. Insoweit werden die von Ihnen gemachten Texteingaben verarbeitet, um diese im „Online-Meeting“ anzuzeigen. Um die Anzeige von Video und die Wiedergabe von Audio zu ermöglichen, werden entsprechend während der Dauer des Meetings die Daten vom

Mikrofon Ihres Endgeräts sowie von einer etwaigen Videokamera des Endgeräts verarbeitet. Sie können die Kamera oder das Mikrofon jederzeit selbst über die „Microsoft Teams“-Applikationen abschalten bzw. stummstellen.

Die Chatinhalte werden bei der Verwendung von Microsoft Teams protokolliert. Dateien, die Benutzer in Chats freigeben, werden im OneDrive for Business-Konto des Benutzers gespeichert, der die Datei freigegeben hat. Die Dateien, die Teammitglieder in einem Kanal freigeben, werden auf der SharePoint-Website des Teams gespeichert.

Soweit personenbezogene Daten von Beschäftigten verarbeitet werden, ist § 26 BDSG die Rechtsgrundlage der Datenverarbeitung. Sollten im Zusammenhang mit der Nutzung von „Microsoft Teams“ personenbezogene Daten nicht für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich, gleichwohl aber elementarer Bestandteil bei der Nutzung von „Microsoft Teams“ sein, so ist Art. 6 Abs. 1 lit. f) DSGVO die Rechtsgrundlage für die Datenverarbeitung. Unser Interesse besteht in diesen Fällen an der effektiven Durchführung von „Online-Meetings“.

Im Übrigen ist die Rechtsgrundlage für die Datenverarbeitung bei der Durchführung von „Online-Meetings“ Art. 6 Abs. 1 lit. b) DSGVO. Eine Aufzeichnung von Online-Meetings erfolgt ausschließlich dann, wenn wir Sie hierüber im Voraus informiert haben und Sie der Aufzeichnung zugestimmt haben. Die Rechtsgrundlage ist in diesem Fall Art. 6 Abs. 1 lit. a DSGVO.

Personenbezogene Daten, die im Zusammenhang mit der Teilnahme an „Online-Meetings“ verarbeitet werden, werden grundsätzlich nicht an Dritte weitergegeben, sofern sie nicht gerade zur Weitergabe bestimmt sind. Beachten Sie bitte, dass Inhalte aus „Online-Meetings“ wie auch bei persönlichen Besprechungstreffen häufig gerade dazu dienen, um Informationen mit Kunden, Interessenten oder Dritten zu kommunizieren und damit zur Weitergabe bestimmt sind.

Weitere Empfänger: Der Anbieter von „Microsoft Teams“ erhält notwendigerweise Kenntnis von den o.g. Daten, soweit dies im Rahmen unseres Auftragsvertrags mit „Microsoft Teams“ vorgesehen ist.

Eine Datenverarbeitung außerhalb der Europäischen Union (EU) erfolgt grundsätzlich nicht, da wir unseren Speicherort auf

Rechenzentren in der Europäischen Union beschränkt haben. Wir können aber nicht ausschließen, dass das Routing von Daten über Internetserver erfolgt, die sich außerhalb der EU befinden. Dies kann insbesondere dann der Fall sein, wenn sich Teilnehmende an „Online-Meeting“ in einem Drittland aufhalten.

Da Microsoft seinen Sitz in den USA hat, haben wir mit Microsoft einen Auftragsverarbeitungsvertrag geschlossen, der den Anforderungen von Art. 28 DSGVO entspricht. Ein angemessenes Datenschutzniveau ist zum einen durch den Abschluss der sog. EU-Standardvertragsklauseln garantiert. Als ergänzende Schutzmaßnahmen haben wir ferner unsere Konfiguration so vorgenommen, dass für die Durchführung von „Online-Meetings“ nur Rechenzentren in der EU, dem EWR bzw. sicheren Drittstaaten wie z.B. Kanada oder Japan genutzt werden.

Weitere Informationen finden Sie im Datenschutzhinweis von Microsoft: <https://privacy.microsoft.com/de-de/privacystatement>
www.microsoft.com/de-de/trust-center

Die Daten sind während des Transports über das Internet jedoch verschlüsselt und somit vor einem unbefugten Zugriff durch Dritte gesichert.

Wir löschen personenbezogene Daten grundsätzlich dann, wenn kein Erfordernis für eine weitere Speicherung besteht. Ein Erfordernis kann insbesondere dann bestehen, wenn die Daten noch benötigt werden, um vertragliche Leistungen zu erfüllen, Gewährleistungs- und ggf. Garantieansprüche prüfen und gewähren oder abwehren zu können. Im Falle von gesetzlichen Aufbewahrungspflichten kommt eine Löschung erst nach Ablauf der jeweiligen Aufbewahrungspflicht in Betracht.

2. Zoom

Wir nutzen das Tool Zoom (Zoom Video Communications, Inc., 55 Almaden Blvd, Suite 600, San Jose, Kalifornien, USA) um Telefonkonferenzen, Online-Meetings, Videokonferenzen, Webinare oder andere Veranstaltungen durchzuführen. Wenn wir Online-Veranstaltungen aufzeichnen wollen, werden wir Ihnen das vorab transparent mitteilen und – soweit erforderlich – um eine Zustimmung bitten. Die Tatsache der Aufzeichnung wird Ihnen zudem in der Zoom-App angezeigt. Wenn es für die Zwecke der Protokollierung von

Ergebnissen eines Online-Meetings erforderlich ist, werden wir die Chatinhalte protokollieren. Das wird jedoch in der Regel nicht der Fall sein. Im Falle von Webinaren können wir für Zwecke der Aufzeichnung und Nachbereitung von Webinaren auch die gestellten Fragen von Webinar-Teilnehmenden verarbeiten. Bei der Nutzung von Zoom werden verschiedene Datenarten verarbeitet. Der Umfang der Daten hängt dabei auch davon ab, welche Angaben zu Daten Sie vor bzw. bei der Teilnahme an einer Online-Veranstaltung machen. Folgende personenbezogene Daten sind Gegenstand der Verarbeitung:

- Benutzerangaben: Vorname, Nachname, Telefon (optional), E-Mail, Passwort (falls SSO nicht verwendet wird), Profilbild (optional), Abteilung (optional)
- Meeting-Metadaten: Thema, Beschreibung (optional), Teilnehmer-IP-Adressen, Geräte- /Hardware-Informationen
- bei Cloudaufzeichnungen (optional): Mp4 von allen Video-, Audio- und Präsentationen, M4A von allen Audioaufnahmen, Textdatei von allen in Meeting-Chats, Audio-Protokolldatei
- IM-Chat-Protokolle
- Telefonie-Nutzungsdaten (optional): Call In-Nummer, Call Out-Nummer, Ländername, IP-Adresse, 911-Adresse (registrierte Dienstadresse), Start- und Endzeit, Host-Name, Host-E-Mail, MAC-Adresse des verwendeten Geräts
- Text-, Audio- und Videodaten: Sie haben ggf. die Möglichkeit, in einem „OnlineMeeting“ die Chat-, Fragen- oder Umfragefunktionen zu nutzen. Insoweit werden die von Ihnen gemachten Texteingaben verarbeitet, um diese im „Online-Meeting“ anzuzeigen und ggf. zu protokollieren. Um die Anzeige von Video und die Wiedergabe von Audio zu ermöglichen, werden entsprechend während der Dauer des Meetings die Daten vom Mikrofon Ihres Endgeräts sowie von einer etwaigen Videokamera des Endgeräts verarbeitet. Sie können die Kamera oder das Mikrofon jederzeit selbst über die Zoom-Applikationen abschalten bzw. stummstellen Standortdaten.

Um an einer Online-Veranstaltung teilzunehmen bzw. den „Meeting-Raum“ zu betreten, müssen Sie zumindest Angaben zu Ihrem Namen machen. Die Datenverarbeitung erfolgt nach Art. 6 Abs. 1 S. 1 lit. b DSGVO. Eine Aufzeichnung von Online-Meetings erfolgt ausschließlich dann, wenn wir Sie hierüber im Voraus informiert haben und Sie der Aufzeichnung zugestimmt haben. Die Rechtsgrundlage ist in diesem

Fall Art. 6 Abs. 1 lit. a DSGVO. Ihre personenbezogenen Daten, die im Zusammenhang mit der Teilnahme an unseren Online-Veranstaltungen verarbeitet werden, werden grundsätzlich nicht an Dritte weitergegeben, sofern sie nicht gerade zur Weitergabe bestimmt sind. Der Dienstleister Zoom erhält notwendigerweise Kenntnis von den o.g. Daten, soweit dies im Rahmen unseres Auftragsverarbeitungsvertrages mit ihm vorgesehen ist. Wenn Sie bei Zoom als Benutzer registriert sind, dann können Berichte über Online-Veranstaltungen (Meeting-Metadaten, Daten zur Telefoneinwahl, Fragen und Antworten in Webinaren, Umfragefunktion in Webinaren) bis zu einem Monat bei Zoom gespeichert werden. Ferner behält sich Zoom vor, Ihre Daten mit Ihrer Zustimmung an Dritte weiterzugeben. Da Zoom seinen Sitz in den USA hat, haben wir mit Zoom einen Auftragsverarbeitungsvertrag geschlossen, der den Anforderungen von Art. 28 DSGVO entspricht. Ein angemessenes Datenschutzniveau ist zum einen durch den Abschluss der sog. EU-Standardvertragsklauseln garantiert. Als ergänzende Schutzmaßnahmen haben wir ferner unsere Zoom-Konfiguration so vorgenommen, dass für die Durchführung von „Online-Meetings“ nur Rechenzentren in der EU, dem EWR bzw. sicheren Drittstaaten wie z.B. Kanada oder Japan genutzt werden. Weitere Informationen finden Sie im Datenschutzhinweis von Zoom: <https://zoom.us/de/de/privacy.html>.

Hinweis für die Einladungs-Mail: „Informationen finden Sie unter Datenschutz unter dem Punkt Kontakt/Videokonferenzen.“

Controller

Verantwortlicher im Sinne der DSGVO ist die

MHS Print GmbH

Plieninger Straße 150
70567 Stuttgart

Data Protection Officer

You can contact our Data Protection Officer at:

AGOR AG
Mario Jacobi
Niddastraße 74
D- 60329 Frankfurt am Main

Kontakt für Ihre Datenschutzanfrage

Hier können Sie Ihre Fragen zum Datenschutz stellen.

info@mhsprint.de

Your rights

- In accordance with Art. 15 GDPR, you have the right to request **information** about your personal data processed by us. In this context, you also have the right to receive a copy of your personal data processed by us in accordance with Art. 15 para. 3-4 GDPR.
- In accordance with Art. 16 GDPR, you can immediately request the **correction** of incorrect or the completion of your personal data stored by us.
- In accordance with Art. 17 GDPR, you can request the erasure of your personal data stored by us.
- In accordance with Art. 18 GDPR, you can request the **restriction of the processing** of your personal data.
- In accordance with Art. 20 GDPR, you can request to receive your personal data that you have provided to us in a structured, commonly used and machine-readable format and you can request the **transfer** to another controller.
- In accordance with Art. 7 para. 3 GDPR, you can **revoke** your consent once given to us at any time. This means that the processing carried out on the basis of the consent prior to the revocation was lawful and has the consequence that we may no longer continue the data processing based on this consent in the future.

Right to object

If your personal data is processed on the basis of legitimate interests in accordance with Art. 6 para. 1 sentence 1 lit. f) GDPR or Art. 6 para. 1 sentence 1 lit. e) GDPR, you have the right to object to the processing of your personal data in accordance with Art. 21 GDPR. In the event of such an objection, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

In the case of direct marketing, you have the right to object at any time to the processing of personal data concerning you. If you object to processing for direct marketing purposes, the personal data will no longer be processed for these purposes.

Right to lodge a complaint with the supervisory authority

You have the right to lodge a complaint with a data protection supervisory authority against the processing of your personal data if you feel that your rights under the GDPR have been violated. As a rule, you can contact the supervisory authority of your usual place of residence, your workplace or our company headquarters.

Links to other websites

We link to websites of other providers or have integrated elements from them into our website. This data protection information does not apply to them - we have no influence on these sites and cannot check that others comply with the applicable data protection regulations.

Changes to the privacy policy

We reserve the right to change or adapt this privacy policy at any time in compliance with the applicable data protection regulations.