

Information gemäß §§ 15, 16 KDG

1. Wer ist für die Datenverarbeitung verantwortlich?

Für die Verarbeitung der uns überlassenen Daten ist ausschließlich verantwortlich die

- Kath. Pfarrgemeinde St. Konrad
- Kath. Pfarrgemeinde St. Heinrich
- Kath. Pfarrgemeinde St. Laurentius
- Kath. Pfarrgemeinde St. Martinus
- Kath. Pfarrgemeinde St. Peter
- Kath. Pfarrgemeinde St. Sebastian

Vertreten durch Pfarrer Thorsten Aymanns
Ahornstraße 51
52074 Aachen

Betriebliche Datenschutzbeauftragte:
Christiane Banse
Klosterplatz 7, 52062 Aachen
+49 241 452-260
christiane.banse@bistum-aachen.de

2. Wozu werden die Daten verwendet?

Die von Ihnen, bzw. Ihrem Kind erhobenen Daten werden ausschließlich verwendet:

- zur Anmeldung zur Firmung
- Einteilung in Vorbereitungsgruppen
- Erstellung von Gruppenlisten für die Gruppenleitenden
- zur Kontaktpflege während des Vorbereitungskurses
- zur Abhaltung von inhaltlichen Treffen per Videokonferenz-System Webex, Zoom, ecclesias, Wonder.me
- zur inhaltlichen Vorbereitung per interaktive Plattformen, beispielsweise padlet und mentimeter
- zur Planung und Durchführung von digitalen Quizaktionen per Plattform Actionbound
- zur interaktiven Gestaltung per Plattform Ginlo, indem Fotos und Medien miteinander geteilt werden, aber auch zur Durchführung von vertraulichen Gesprächen.

Dies beruht auf der Grundlage von § 6 Abs. 1 lit. a KDG (Vorschriften des Kirchenrechtes), § 6 Abs. 1 lit. b KDG (Ihre Einwilligung) und § 6 Abs. 1 lit. f KDG (Interesse der Pfarrgemeinde an der Verkündigung und Seelsorge).

3. Warum müssen die Daten erhoben werden und wie lange werden Sie gespeichert und an wen werden die Daten weitergegeben?

Zur Registrierung der Sakramentenspendung ist die Erhebung der Daten aus kirchenrechtlichen Gründen erforderlich, in diesem Kontext erfolgt auch die Speicherung:

- Vorname, Name des Kindes, Name des Firmpaten / der Firmpatin und Tag der Firmung werden nach kirchenrechtlichen Vorschriften gespeichert.
- Alle anderen Daten (Telefonnummer, Emailadressen) werden 2 Jahren nach der Firmung gelöscht.
- In diesem Zeitraum können Sie bei besonderen Ereignissen in der Pfarre per E-Mail benachrichtigt werden.

4. Umgang mit Daten im Rahmen der Videokonferenzen

Für die Kommunikation in Gruppen werden verschiedene Tools für Videokonferenzen genutzt. Dabei werden die Services von Ecclesias, Webex, wonder.me und Zoom verwendet, die im Rahmen verschiedener (Klein-) Gruppenarbeiten verwendet werden.

Die Anlage eines Nutzerkontos ist bei diesen Diensten nicht erforderlich. Auch ein Softwaredownload ist nicht erforderlich. Die Teilnehmer können über einen Standardbrowser (Chrome oder Edge) teilnehmen.

Für die Organisation und Planung der Konferenzen werden gültige E-Mailadressen, Vor- und Nachnamen genutzt.

Alle Informationen, die im Rahmen einer Videokonferenz ausgetauscht werden, z.B. Ton, Video, Chat, Teilen des Bildschirms, werden verschlüsselt übertragen und teilweise temporär bei den Dienstleistern gespeichert. Nach der Konferenz werden die Daten gelöscht.

Es erfolgt eine Weitergabe der Verkehrs- und Inhaltsdaten aus der Videokonferenz an den Betreiber des Systems. Die Inhaltsdaten (Bild und Ton) sind verschlüsselt und werden nach der Sitzung gelöscht, die Verkehrsdaten (IP-Adresse, Standortdaten, Anmeldename, etc.) werden nach der Sitzung gelöscht.

Auch die Services Webex, wonder.me und Zoom werden entsprechend der europäischen Datenschutzgrundverordnung bereitgestellt. Für den Betrieb werden auch Dienstleister im europäischen und außereuropäischen Ausland, vorwiegend den USA, genutzt. Die Dienstleister verpflichten sich ein adäquates Datenschutzniveau sicherzustellen.

Details dazu finden sie in den Datenschutzbedingungen der Dienstleister:

Zoom

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

Folgende personenbezogene Daten sind Gegenstand der Verarbeitung:

- Angaben zum Benutzer: Vorname, Nachname, Telefon (optional), E-Mail-Adresse, Passwort (wenn „Single-Sign-On“ nicht verwendet wird), Profilbild (optional), Abteilung (optional)
- Meeting-Metadaten: Thema, Beschreibung (optional), Teilnehmer-IP-Adressen, Geräte-/Hardware-Informationen
- Bei Aufzeichnungen (optional): MP4-Datei aller Video-, Audio- und Präsentationsaufnahmen, M4A-Datei aller Audioaufnahmen, Textdatei des Online-Meeting-Chats.
- Bei Einwahl mit dem Telefon: Angabe zur eingehenden und ausgehenden Rufnummer, Ländername, Start- und Endzeit. Ggf. können weitere Verbindungsdaten wie z.B. die IP-Adresse des Geräts gespeichert werden.
- Text-, Audio- und Videodaten: Sie haben ggf. die Möglichkeit, in einem „Online-Meeting“ die Chat-, Fragen- oder Umfragenfunktionen zu nutzen. Insoweit werden die 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.

Um an einem „Online-Meeting“ teilzunehmen bzw. den „Meeting-Raum“ zu betreten, sind zumindest Namensangaben erforderlich.

Eine Aufzeichnung findet nicht statt. Darauf werden auch die Teilnehmer hingewiesen.

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.

Personenbezogene Daten werden grundsätzlich dann gelöscht, 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. Näheres dazu unter: <https://www.zoom.us>

Cisco Webex

Bei der Nutzung von „Cisco Webex“ werden verschiedene Arten personenbezogener Daten verarbeitet. Der Umfang der Datenverarbeitung hängt dabei auch davon ab, welche Angaben vor bzw. bei der Teilnahme an einem Webmeeting gemacht und welche Einstellungen vorgenommen werden.

Folgende personenbezogene Daten sind Gegenstand der Verarbeitung:

- Angaben zum Benutzer: Name, Vorname, E-Mail-Adresse
- Meeting-Metadaten: Thema, Beschreibung (optional), Teilnehmer-IP-Adressen, Geräte-/Hardware-Informationen
- Bei Aufzeichnungen: MP4-Datei aller Video-, Audio- und Präsentationsaufnahmen, M4A-Datei aller Audioaufnahmen, Textdatei des Online-Meeting-Chats.
- Bei Einwahl mit dem Telefon: Angabe zur eingehenden und ausgehenden Rufnummer, Ländername, Start- und Endzeit. Ggf. können weitere Verbindungsdaten wie z. B. die IP-Adresse des Geräts gespeichert werden.
- Text-, Audio- und Videodaten: Es besteht die Möglichkeit, in einem Webmeeting die Chat-, Fragen- oder Umfragefunktionen zu nutzen. Die Textangaben werden verarbeitet, um diese im Webmeeting anzuzeigen und ggf. aufzuzeichnen. Um die Anzeige von Video und die Wiedergabe von Audio zu ermöglichen, werden entsprechend während der Dauer des Meetings die Daten vom Mikrofon des Endgeräts sowie von einer etwaigen Videokamera des Endgeräts verarbeitet.

Es besteht die Möglichkeit, die Kamera oder das Mikrofon jederzeit über die „Cisco Webex“-Applikationen abzuschalten bzw. stummzustellen.

Personenbezogene Daten, die im Zusammenhang mit der Teilnahme an Webmeetings verarbeitet werden, werden grundsätzlich nicht an Dritte weitergegeben, sofern sie nicht zur Weitergabe bestimmt sind. Der Anbieter von „Cisco Webex“ erhält notwendigerweise Kenntnis von den oben genannten Daten.

Die personenbezogenen Daten werden bis zum Wegfall des Zwecks der Datenverarbeitung oder nach Ablauf gesetzlicher oder behördlicher Aufbewahrungspflichten gespeichert.

Genauereres hier finden Sie unter: <https://www.webex.com/de/index.html>

Wonder.me

Bei der Plattform „wonder.me“ werden folgende personenbezogenen Daten erhoben: Vor- und Nachnamen, Emailadresse. Außerdem werden Cookies und Nutzungsdaten wie IP-Adressen, der Browsertyp, das Nutzungsdatum, die Nutzungsdauer, die Geräte-ID sowie die Diagnosedaten verarbeitet. Personenbezogene Daten der Teilnehmer einer Online-Veranstaltung werden nicht an Dritte weitergegeben. Die Daten werden gelöscht, sobald der Zweck der Speicherung, der mit der Nutzung der Plattform für konkrete einzelne Online-Meetings verbunden ist, nicht mehr vorliegt.

<https://www.wonder.me/policies/privacy-policies>

Ecclesias

Bei der Nutzung des Videokonferenz-Tools werden verschiedene Datenarten verarbeitet. Für Teilnehmer des Meetings ist die Namensangabe erforderlich. Dieser Name wird für die Dauer der Teilnahme an dem jeweiligen Online-Meeting verarbeitet und anschließend gelöscht.

Auch etwaige Audio-, Video- oder Chatinhalte werden nur während des jeweiligen Online-Meetings verarbeitet.

Zum technischen Betrieb werden nachfolgende Daten verarbeitet:

IP-Adresse: Um das Online-Meeting durchführen zu können, wird zwingend die von dem Endgerät verwendete IP-Adresse verarbeitet. Die IP-Adresse wird nach Angaben des Dienstleisters für die Dauer von sieben Tagen auf seinen Servern gespeichert, in dem Interesse Angriffe auf die Webseiten erkennen und abwehren zu können mit der Rechtsgrundlage § 6 Abs. 1 lit. g KDG.

Name des Meetings und ggf. Passwort: Bei Einrichtung eines Online-Meetings wird ein Name für das Online-Meeting vom Veranstalter gewählt. Zusätzlich kann ein Passwort für die Teilnahme am Online-Meeting vorgesehen werden. Diese Daten werden nur bis zur Beendigung des jeweiligen Online-Meetings verarbeitet und anschließend gelöscht. Allerdings kann der Name von „Online-Meetings“ sowie Datum, Uhrzeit und Dauer des „Online-Meeting“ in Ihrem Browser lokal gespeichert werden. Wenn Sie die Daten nicht weiter verfolgen zu können, sollten der Browser-Cache gelöscht werden.

E-Mail-Adresse: Auch eine optionale Emailadresse kann angegeben werden. Diese E-Mail-Adresse wird dann verwendet, um ein Profilfoto vom Dienst „Gravatar“ abzurufen und anzuzeigen. Gravatar-Profilfotos werden nur angezeigt, wenn zu der angegebenen E-Mail-Adresse ein öffentliches Gravatar-Bild abgerufen werden kann.

Nutzungsdaten und Cookies: Der Dienstleister gibt an, die Nutzungsdaten nur anonymisiert zu speichern. Weitere Informationen in der Datenschutzerklärung des Erzbistum Hamburg zu diesem Videokonferenzsystem.

Personenbezogene Daten, die im Zusammenhang mit der Teilnahme an der Videokonferenz verarbeitet werden, werden grundsätzlich nicht an Dritte weitergegeben, sofern sie nicht gerade zur Weitergabe bestimmt sind.

Der von uns für den Betrieb dieser Videokonferenz eingesetzte Anbieter (Erzbistum Hamburg) ist ebenfalls Empfänger von Daten. Er hat mit dem technischen Dienstleister (Metaways) einen Auftragsverarbeitungsvertrag abgeschlossen, der den Anforderungen von §. 29 KDG entspricht. Dieser Dienstleister trägt insbesondere Sorge dafür, dass alle erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit nach § 26 KDG eingehalten werden.

Der Service von Ecclesias wird entsprechend der europäischen Datenschutzgrundverordnung und des Katholischen Datenschutzgesetzes betrieben. Der Betrieb erfolgt in einem Rechenzentrum in Deutschland (Hamburg). Genaueres dazu: <https://www.ecclesias.de/konferenz>

Ginlo

ginlo Private ist ein internetbasierter, plattformübergreifender Dienst zum sicheren Austausch von Nachrichten zwischen Nutzern von mobilen Endgeräten. Bei der Registrierung und während der Nutzung von ginlo Private werden folgende personenbezogene Daten verarbeitet:

Mobilrufnummer

Die Mobilrufnummer wird zunächst verwendet, um in der Registrierungsphase einen Bestätigungscode zuzusenden. Im Anschluss wird diese Nummer als Hashwert und damit nicht wieder im Klartext herstellbar auf dem ginlo Server gespeichert. Bei der Anmeldung auf ginlo und bei der Zustimmung des Zugriff auf die Telefonbuch-Kontakte des Smartphones werden die Mobilrufnummern zum Abgleich als Hashwert auf den ginlo Server geladen und anschließend wieder gelöscht. ginlo Nutzer, die eine Mobilrufnummer in ihrem Telefonbuch gespeichert haben, werden bei der Synchronisation ihrer ginlo Kontakte über die entsprechende Anmeldung informiert.

E-Mail-Adresse

Optional kann jeder ginlo Private Nutzer in seinen Kontakten eine E-Mail-Adresse hinzufügen. Diese wird ebenso als Hashwert auf dem ginlo Server gespeichert und kann von anderen ginlo Nutzern als Suchkriterium verwendet werden.

Profilname und Profilbild

Optional kann jeder ginlo Private Nutzer einen Anzeigenamen und/oder ein Bild (Avatar) in seinem Profil hinterlegen. Diese Daten werden auf dem ginlo Server verschlüsselt gespeichert und in der Nachrichtenübersicht und den Kontakten angezeigt.

ginlo ID / QR-Code

Während der Registrierung erzeugt ginlo eine achtstellige ginlo ID, die genau einem Account zugeordnet ist und beim Login oder als Suchfunktion verwendet werden kann. Sie ist Bestandteil aller ginlo Kontakte und wird auch im eigenen Profil angezeigt. Zur ginlo ID wird ein Barcode generiert und zum Scannen durch Ihre Kontakte bereit gestellt.

Kommunikationsdaten

Die Kommunikationsdaten einschließlich aller Dateien werden in verschlüsselter Form lokal auf dem eigenen Gerät gespeichert und auch während des Transportes verschlüsselt – dies ist eine echte Ende-zu-Ende Verschlüsselung. Auch während der Zwischenspeicherung auf unseren Servern sind personenbezogene Daten voll verschlüsselt.

Rechtsgrundlagen der Verarbeitung

Die Verarbeitung Ihrer Mobilrufnummer stützt sich auf den Art. 6 Abs. 1 lit. b DSGVO und ist notwendig für die Erfüllung eines Vertrags, an dem Sie beteiligt sind.

Das Suchen und Gefundenwerden über den Hashwert der Mobilrufnummer oder der E-Mail-Adresse, die Anzeige Ihres Profilnamens und Ihres Profilbildes sowie die Übertragung Ihrer verschlüsselten Kommunikationsdaten setzen Ihr Einverständnis voraus; deshalb erfolgt in diesen Fällen die Verarbeitung nach 6 Abs. 1 lit. a DSGVO.

Hier werden Anmeldedaten gespeichert. Auch die Inhalte werden gespeichert, allerdings mit einem persönlichen Schlüssel des Nutzers, so dass ein Zugriff durch den Dienstleister technisch nicht möglich ist. Die Nutzerdaten werden nach Abschluss des Vertrages gelöscht. Für alle übrigen Daten erfolgt keine Weitergabe und damit auch nicht in ein Drittland oder an eine internationale Organisation.

Die ginlo.net GmbH gibt die personenbezogenen Daten nicht an Dritte weiter und wird dies auch in Zukunft nicht tun, es sei denn, dies ist gesetzlich vorgeschrieben, für den Vertragszweck erforderlich oder Sie haben ausdrücklich eingewilligt.

Das ginlo-Unternehmen setzt Auftragsverarbeiter ein. Die externen Dienstleister verarbeiten die personenbezogenen Daten nur auf dokumentierter Weisung der ginlo.net GmbH. Als externe Dienstleister kommen z.B. Betreiber von Rechenzentren und Internetdiensten sowie Leitungsanbieter oder Zahlungsdienstleister mit Sitz in Deutschland in Betracht.

Die personenbezogenen Daten werden gelöscht oder gesperrt, sobald der Zweck der Speicherung entfällt.

Eine Speicherung kann darüber hinaus aufgrund gesetzlicher Aufbewahrungsfristen erfolgen. Eine Sperrung oder Löschung der Daten erfolgt auch dann, wenn eine gesetzlich vorgeschriebene Speicherfrist abläuft, es sei denn, dass eine Erforderlichkeit zur weiteren Speicherung der Daten für einen Vertragsabschluss oder eine Vertragserfüllung besteht.

Website

Die beim Besuch unserer Website verarbeiteten Daten werden nach 7 Tagen automatisch gelöscht.

Formulardaten werden in Tickets umgewandelt und gemeinsam mit Support-E-Mails in einem CRM-System verarbeitet. Diese Daten werden am Ende des auf die letztmalige Kontaktaufnahme folgenden Jahres gelöscht, da ginlo auch einer Nachweispflicht unterliegt. Für Abrechnungszwecke relevante Daten werden nach Ablauf der gesetzlichen Aufbewahrungspflicht gelöscht.

ginlo App

Nachrichten werden Ende-zu-Ende-verschlüsselt auf unseren Servern nur zwischengespeichert. Auf dem Server wird jede Nachricht 90 Tage nach dem Versand gelöscht. Nachrichten, die während dieser 90 Tage auf dem Server verfügbar sind, werden zwischen mehreren Endgeräten des gleichen ginlo Business Nutzerkontos synchronisiert, sodass diese Nachrichten auf allen verwendeten Endgeräten verfügbar sind.

Jeder ginfo Nutzer kann beim Versand einer Nachricht festlegen, ob diese Nachricht nach einer bestimmten Zeit, zu einem bestimmten Zeitpunkt oder nach dem Lesen dieser Nachricht automatisch gelöscht wird. Teile von Chats oder komplette Einzelchats können ebenfalls vom Nutzer gelöscht werden.

Ein Nutzerkonto kann inklusive aller seiner Dateien auf den Servern restlos vom Nutzer selbst unter den Profileinstellungen entfernt werden. Dazu ist die Eingabe des Gerätepasswortes notwendig.

Nicht mehr genutzte Nutzerkonten werden am Ende des auf die letzte Nutzung folgenden Kalenderjahres automatisch gelöscht. Während dieser Zeit ist eine Reaktivierung des Accounts durch den Nutzer möglich. Spätestens ab dem Zeitpunkt der Löschung bleibt die Suchfunktion anderer Nutzer ergebnislos.

5. Umgang mit Daten im Rahmen interaktiver Tools

Mentimeter

Dieses Tool wird im Rahmen der Firmvorbereitung ohne Registrierung oder Anmeldung genutzt, also ohne Eingabe personenbezogener Daten.

Im Falle der Eingabe personenbezogener Daten werden diese gelöscht oder gesperrt, sobald der Zweck der Speicherung entfällt.

Konkret werden folgende Informationen gelöscht:

- E-Mail-Adressen der Benutzer User werden nach 12 Monaten gelöscht.
- Bei Presentern nach Aufforderung. IP-Adresse des Benutzers nach 14 Tagen
- IP-Adressen des Präsentierers bis Mentimeter zur Löschung aufgefordert wird (Vertragsende und Löschen des Accounts)
- User Agent (Browser) unbeschränkt bis zur Aufforderung zur Löschung.
- Umfrageinhalte bis zur Aufforderung zur Löschung. Über eine organisatorische Regelung erfolgt die Löschung nach spätestens 14 Tagen. Davon nicht betroffen sind anonyme und aggregierte Umfrageinhalte.

(vgl. <https://www.mentimeter.com/privacy>, Abschnitt 9.1)

Padlet

Die Nutzung des Padlet ist ohne Registrierung möglich. Der Zugriff auf padlet erfolgt über den von der verantwortlichen Person zugesandten Link, mit dem die Teilnehmer zur Mitarbeit eingeladen werden. Die Erstellung eines Nutzerkontos ist nicht erforderlich. Padlet bietet die Funktionen, vielfältige Inhalte miteinander zu teilen, aber auch gleichzeitige Mitarbeit zu ermöglichen. In diesem Fall werden keine personenbezogenen Daten erhoben bzw. ausgewertet. Außerdem werden die Inhalte so gestaltet, dass keine sensiblen und personenbezogenen Daten eingestellt werden. Es kann nicht vollständig ausgeschlossen werden, dass die Daten weitergegeben werden. Jedoch laut Datenschutzerklärung von padlet erfolgt dies

ohne Rückschlüsse auf eine identifizierbare Person. Ohne eine Anmeldung mit Konto speichert Padlet keine personenbezogenen Daten der Nutzer, außer eventuell anonymisierte technische Nutzungsdaten. Näheres zum Datenschutz von padlet unter: <https://padlet.com/about/privacy>

Actionbound

Für die Erstellung eines Actionbound-Accounts wird eine gültige E-Mail-Adresse benötigt. Die Ausnahme bilden die Sofort-Accounts, für die keine personenbezogenen Daten erhoben werden. Die App kann auch ohne Registrierung verwendet werden. Personenbezogene Daten, die dem Dienst actionbound zur Verfügung gestellt werden, werden nicht bearbeitet, ausgewertet und nicht an Dritte weitergegeben. Die Daten werden bei Kündigung des Accounts oder bei Widerruf gelöscht.

Mehr dazu unter folgendem Link: <https://de.actionbound.com/faq-datenschutz>

6. Welche Rechte haben Sie, bzw. Ihr Kind?

- Sie haben das Recht auf Auskunft über die von uns zu Ihrer Person verarbeiteten personenbezogenen Daten. Bei einer Auskunftsanfrage bitten wir um Verständnis dafür, dass wir ggf. Nachweise von Ihnen verlangen, die belegen, dass Sie die Person sind, für die Sie sich ausgeben.
- Ferner haben Sie ein Recht auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung, soweit Ihnen dies gesetzlich zusteht.
- Außerdem haben Sie ein Widerspruchsrecht gegen die Veröffentlichung im Pfarrbrief.
- Sie haben das Recht, Daten, die wir auf Grundlage Ihrer Einwilligung automatisiert verarbeiten, an sich oder an einen Dritten in einem gängigen, maschinenlesbaren Format aushändigen zu lassen. Sofern Sie die direkte Übertragung der Daten an einen anderen Verantwortlichen verlangen, erfolgt dies nur, soweit es technisch machbar ist.
- Da die Erstellung der Fotos zur Veröffentlichung auf Ihrer Einwilligung beruht, haben Sie das Recht, diese Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.
- Schließlich haben Sie das Recht, sich über die Verarbeitung personenbezogener Daten durch uns bei einer Aufsichtsbehörde für den Datenschutz zu beschweren.