

RealTalk

Detaillierte Funktionsbeschreibung mit datenschutzrechtlichen Ergänzungen für Peer-Chat und Terminbuchung

Ort, Datum: Berlin, Januar 2026

Version: I/2026



Inhaltsverzeichnis

1. Ziel und Zweck des Konzepts	3
2. Funktionsweise von RealTalk	3
2.1 Peer-to-Peer-Beratung (anonymer Chat)	3
2.2 Digitales Terminbuchungstool (Schul-/Jugendsozialarbeit)	4
3. Datenverarbeitung und Rechtsgrundlagen	5
3.1 Welche Daten werden im Peer-Chat verarbeitet?	5
3.2 Zwecke der Verarbeitung	5
3.3 Rechtsgrundlagen	6
3.4 Speicherdauer	6
4. Schutzmaßnahmen und Anonymität	7
4.1 Technische Schutzmaßnahmen	7
4.2 Anonymität im Peer-Chat	7
4.3 Organisatorische Maßnahmen	7
5. Zusatzsysteme, Risiken und Herausforderungen	8
6. Verantwortlichkeiten, Transparenz und Ausblick	9

1. Ziel und Zweck des Konzepts

RealTalk ist ein digitales Angebot des Deutschen Roten Kreuzes e.V., das Jugendliche „RealTalk ist ein digitales Angebot des Deutschen Roten Kreuzes e.V. (Verantwortlicher nach Art. 4 Nr. 7 DS-GVO), das sich an Jugendliche richtet und insbesondere Jugendliche im Alter von etwa 16 bis 20 Jahren in belastenden Lebenssituationen unterstützt.“

Im Mittelpunkt stehen zwei Bausteine:

- ein anonymer Peer-Chat mit gleichaltrigen, geschulten Peers und
- ein digitaler Zugang zur Schul- und Jugendsozialarbeit über ein Terminbuchungstool.

Datenschutz ist dabei besonders wichtig, weil Jugendliche sehr persönliche Themen teilen – etwa zu psychischer Gesundheit, Familie, Schule oder Konflikten. Gleichzeitig sollen sie sich sicher fühlen und möglichst wenig Hürden haben, Hilfe in Anspruch zu nehmen.

RealTalk verfolgt einen Zwei-Stufen-Prozess:

- Stufe 1: niederschwelliger, anonymer Austausch mit Peers im Chat.
- Stufe 2: bei Bedarf digitale Weiterleitung bzw. Vermittlung an professionelle Hilfen am Lebensort der Jugendlichen (z. B. Schulsozialarbeit).

Erfahrungen aus dem Projekt zeigen, dass rund die Hälfte der Beratungen eine Form von Weiterleitung oder Verweis auf professionelle Angebote benötigt. Ziel des Datenschutzkonzepts ist es daher, die Verarbeitung von Daten in beiden Stufen – Peer-Chat und Terminbuchung – verständlich, transparent und rechtskonform zu gestalten und gleichzeitig die Anonymität der Jugendlichen bestmöglich zu schützen.

2. Funktionsweise von RealTalk

2.1 Peer-to-Peer-Beratung (anonymer Chat)

Zugang über RealTalk.help

Jugendliche rufen die Seite RealTalk.help auf und wählen dort, ob sie über WhatsApp oder SMS schreiben möchten. Vor Absenden der ersten Nachricht müssen die Nutzungsbedingungen akzeptiert und die Datenschutzhinweise zur Kenntnis genommen werden. Soweit besondere Kategorien personenbezogener Daten freiwillig mitgeteilt werden, wird eine ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO eingeholt.

Technischer Ablauf und Anonymisierung

- Die Nachricht geht zunächst an den gewählten Messenger-Dienst (z. B. WhatsApp oder SMS).
- Von dort wird sie an den Dienstleister Twilio weitergeleitet.
- Anschließend wird die Nachricht an die RealTalk-Server (gehostet u. a. bei Amazon Web Services – AWS) übertragen und dort weiterverarbeitet.
- Die Telefonnummer der Jugendlichen wird durch einen anonymen Chat-Code ersetzt.

Für Peers und Peer-Support sind nur dieser Code und der Inhalt der Nachrichten sichtbar – keine Namen, keine Telefonnummern, keine Adressen.

Ablauf einer Beratung

- Nach der ersten Nachricht erhält die ratsuchende Person eine automatische Willkommensnachricht:
 - Bestätigung, dass die Anfrage eingegangen ist,
 - Hinweis, dass ein Peer gesucht wird,
- Erklärung von Dauer und Grenzen des Formats (max. 60 Minuten, keine Therapie, keine Notfallhotline).
- Nimmt ein Peer den Chat an, wird der Chat exklusiv für 60 Minuten diesem Peer zugeordnet. Die ratsuchende Person sieht, dass sie nun mit einem Peer verbunden ist.
- Kurz vor Ablauf der Zeit wird der Chat automatisch mit Vorankündigungen (z. B. 15 und 5 Minuten vorher) beendet.
- Peers sind geschult, keine Klarnamen, Wohnorte oder andere identifizierende Daten zu erfragen und ggf. darauf hinzuweisen, dass solche Details nicht notwendig sind.

Rolle von Peer-Support und RealTalk-Team

- Während der Schichten sind Peer-Support-Personen erreichbar (z. B. per Teams/Signal), falls Peers sich unsicher oder überfordert fühlen.
- In Ausnahmefällen (z. B. akute Suizidgefahr, Ankündigung schwerer Straftaten, Kinderschutzfälle) kann das RealTalk-Team über definierte Abläufe eingebunden werden.
- Hierfür gibt es eigene Krisenleitfäden und klare Regeln, wann und wie Daten in engen Grenzen weitergegeben werden dürfen oder müssen.

2.2 Digitales Terminbuchungstool (Schul-/Jugendsozialarbeit)

Über RealTalk.help können Jugendliche – je nach Standort – zusätzlich einen Termin bei der Schulsozialarbeit oder anderen beteiligten Fachkräften buchen. Technisch sieht das so aus:

- RealTalk zeigt auf der Plattform eine Verlinkung zum Terminangebot des jeweiligen Standorts/ des DRK-Kreisverbandes.
- Die eigentliche Terminvereinbarung läuft über Microsoft Bookings (MS 365) der Schulsozialarbeit oder des Trägers.
- Jugendliche können dort z. B. wählen:
 - gewünschte Person,
 - Zeitpunkt,
 - ggf. Ort oder Format (vor Ort / online).

Die für die Terminvergabe eingegebenen personenbezogenen Daten werden ausschließlich in den Systemen der beteiligten Träger verarbeitet. RealTalk erhält keinen Zugriff auf diese Inhalte; die datenschutzrechtliche Verantwortung liegt vollständig beim jeweiligen Träger.

Langfristig soll dieses Terminmodul so weiterentwickelt werden, dass:

- auch andere Kontexte (offene Jugendarbeit, Jugendzentren, Beratungsstellen) eingebunden werden können,
- Standorte, die kein Microsoft 365 nutzen oder kein Online-Tool möchten, alternative, datenschutzkonforme Wege nutzen können (z. B. nur Informationsseite, andere Tools).

Ziel ist es, den Zugang zu Jugendsozialarbeit und insbesondere Schulsozialarbeit zu vereinfachen, weil viele Probleme dauerhaft am Lebensort der Jugendlichen bearbeitet werden müssen und RealTalk diesen Schritt erleichtern möchte.

3. Datenverarbeitung und Rechtsgrundlagen

3.1 Welche Daten werden im Peer-Chat verarbeitet?

Im Rahmen des Peer-Chats können u. a. verarbeitet werden:

- bei der ersten Kontaktaufnahme
 - Mobilfunknummer (wird in einen Chat-Code überführt),
 - Datum und Uhrzeit der Kontaktaufnahme,
 - Inhalt der ersten Nachricht;
- während der Beratung
 - alle weiteren Nachrichten (Text, ggf. Emojis, kurze Sprachnachrichten),
 - freiwillig genannte Angaben zur Person (z. B. Alter, Schulform, Familiensituation),
 - sehr sensible Daten (z. B. zur psychischen und körperlichen Gesundheit, Gewalterfahrungen, sexuellen Orientierung) – diese zählen zu den „besonderen Kategorien personenbezogener Daten“;
- technische Metadaten
 - Zeitpunkt des Sendens/Empfangs,
 - Informationen, ob eine Nachricht zugestellt oder gelesen wurde.

Für Auswertung und Qualitätssicherung werden Teile dieser Daten später pseudonymisiert oder anonymisiert. Aggregierte Gruppenauswertungen machen keine Rückschlüsse auf einzelne Personen mehr möglich.

3.2 Zwecke der Verarbeitung

Die Daten werden u. a. zu folgenden Zwecken verarbeitet:

- Bereitstellung des Peer-Chats
 - also um überhaupt mit einem Peer schreiben zu können, Antworten zu versenden und technische Abläufe sicherzustellen;
- Durchführung der Beratung

- z. B. zur Einschätzung der Situation, zum Anknüpfen an vorherige Nachrichten, zur Unterstützung in Krisen;
- Qualitätssicherung und Supervision
 - z. B. zur fachlichen Begleitung der Peers, zur Reflexion schwieriger Fälle, zur Einhaltung des Schutzkonzepts;
- Analyse und Weiterentwicklung
 - z. B. um zu prüfen, wie oft der Dienst genutzt wird, welche Themen häufig vorkommen und wie Übergänge zu professionellen Hilfen funktionieren;
- Forschung und Evaluation
 - in enger Zusammenarbeit mit Forschungseinrichtungen können pseudonymisierte/anonymisierte Daten genutzt werden, um Wirksamkeit, Reichweite und Zielgruppen besser zu verstehen.

3.3 Rechtsgrundlagen

Wesentliche Rechtsgrundlagen der Datenverarbeitung im Rahmen von RealTalk sind:

- Art. 6 Abs. 1 lit. b DS-GVO
 - zur Erfüllung des Nutzungsverhältnisses / der Beratung (Bereitstellung des Peer-Chats, Kommunikation, Qualitätssicherung als Teil der Dienstleistung);
- Art. 6 Abs. 1 lit. a DS-GVO i. V. m. Art. 9 Abs. 2 lit. a DS-GVO
 - Einwilligung der Jugendlichen, insbesondere für sensible Daten (Gesundheitsdaten, sehr persönliche Informationen), die sie freiwillig mitteilen;
- Art. 6 Abs. 1 lit. f DS-GVO (berechtigtes Interesse)
 - z. B. zur Sicherstellung der technischen Stabilität, zur Abwehr von Missbrauch, zur pseudonymisierten Auswertung und zur Weiterentwicklung des Angebots;
- Art. 89 DS-GVO i.V.m. § 27 BDSG
 - für die Nutzung von Daten zu wissenschaftlichen Forschungs- und Evaluationszwecken, in der Regel in pseudonymisierter oder anonymisierter Form;
- für die Terminbuchung über Microsoft Bookings
 - regelmäßig Art. 6 Abs. 1 lit. b (Terminvereinbarung) und lit. f (effiziente Organisation der Schulsozialarbeit) DS-GVO, ggf. Art. 6 Abs. 1 lit. a DS-GVO für bestimmte Tracking- oder Komfortfunktionen.

Das Angebot richtet sich im Peer-Chat an Jugendliche ab 16 Jahren. Präventions- und Beratungsdienste dürfen nach Erwägungsgrund 38 DS-GVO unmittelbar gegenüber den Jugendlichen erbracht werden, sofern sie deren Wohl dienen und verantwortungsbewusst umgesetzt werden.

3.4 Speicherdauer

- Technische Logdaten der Website (z. B. Server-Logfiles) werden in der Regel nach sieben Tagen gelöscht, sofern kein Verdacht auf Missbrauch besteht.
- *Chatinhalte werden für die Dauer der laufenden Beratung gespeichert und anschließend für Zwecke der internen Qualitätssicherung längstens drei Monate vorgehalten. Danach erfolgt Löschung oder Anonymisierung entsprechend dem internen Löschkonzept.*

- Daten aus Terminbuchungen werden von den jeweiligen Trägern (z. B. DRK-Kreisverbände, Schulen) entsprechend ihren gesetzlichen Aufbewahrungspflichten und internen Richtlinien gespeichert.

Die genauen Fristen und Verfahren sind in internen Lösch- und Bereinigungskonzepten geregelt und werden regelmäßig überprüft.

4. Schutzmaßnahmen und Anonymität

Um die Daten der Jugendlichen bestmöglich zu schützen, setzt RealTalk technische und organisatorische Maßnahmen um:

4.1 Technische Schutzmaßnahmen

- Verschlüsselung der Web- und Plattformkommunikation (z. B. TLS/HTTPS).
- Hosting auf professionellen Servern (u. a. AWS), mit vertraglich geregelten Datenschutzstandards.
- Nutzung zertifizierter Dienste (z. B. Anbieter mit EU-Standorten bzw. EU-US Data Privacy Framework oder Standardvertragsklauseln). Zugriffsbeschränkungen: nur besonders berechtigte Personen dürfen auf Systemdaten zugreifen, niemals auf mehr als für ihre Aufgabe nötig.
- Einsatz von CDNs (Google Cloud CDN, Amazon CloudFront) zur sicheren und stabilen Bereitstellung der Website.
- Einsatz eines Consent-Tools (Usercentrics), um Einwilligungen zu Cookies und Tracking rechtssicher einzuholen. Webanalyse-Dienste werden ausschließlich mit vorheriger Einwilligung genutzt; der Peer-Chat bleibt unabhängig hiervon voll funktionsfähig.

4.2 Anonymität im Peer-Chat

Die Anonymität bezieht sich auf die Beratungsebene: Peers erhalten ausschließlich den Chat-Code. Auf Systemebene erfolgt eine pseudonymisierte Verarbeitung, da technische Identifikatoren temporär verarbeitet werden.

- Telefonnummern werden durch anonyme Chat-Codes ersetzt; Peers sehen nur Code + Chatinhalt.
- Peers werden geschult, keine identifizierenden Daten zu erfragen und aktiv darauf hinzuweisen, dass Namen, Adressen oder Social-Media-Handles nicht nötig sind.
- Es gibt Textbausteine, die die Jugendlichen freundlich daran erinnern, keine de-anonymisierenden Informationen zu teilen.
- Bildversand ist eingeschränkt bzw. untersagt, um zusätzliche Risiken zu vermeiden.
- Blocklisten/Filter verhindern bestimmte beleidigende oder gefährdende Begriffe, soweit technisch möglich.

4.3 Organisatorische Maßnahmen

- Vertraulichkeit und Schweigepflicht:
Mitarbeitende des RealTalk-Teams unterliegen der beruflichen Schweigepflicht nach § 203 StGB. Peers und Peer-Support sind vertraglich verpflichtet, strikt vertraulich zu handeln; sie werden umfassend zu ihren Verschwiegenheitspflichten geschult.

- **Ausnahmen in Notfällen:**

In eng begrenzten Fällen kann oder muss die Schweigepflicht durchbrochen werden – etwa bei:

- akuter Suizidgefahr,
- Ankündigung schwerer Straftaten (z. B. Amoklauf, Terrorangriff, Mord),
- schwerwiegender Kindeswohlgefährdung.

Hier greifen die gesetzlichen Regelungen (z. B. § 138, § 323c, § 34 StGB) und interne Notfallabläufe. Die Weitergabe von Daten erfolgt dann so zielgenau und minimal wie möglich, etwa an Polizei oder Jugendamt.

- **Schulung und Supervision:**

Peers und Peer-Support werden intensiv ausgebildet:

- zu Datenschutz und Anonymität,
- zum Umgang mit sensiblen Inhalten,
- zu Krisenleitfäden und Schutzkonzepten.

Regelmäßige Supervision und Reflexionsformate unterstützen sie im sicheren Umgang mit belastenden Situationen.

5. Zusatzsysteme, Risiken und Herausforderungen

RealTalk nutzt neben der eigenen Plattform weitere Dienste und Systeme, etwa:

- AWS (Hosting der Anwendung),
- Twilio (Anbindung von WhatsApp/SMS),
- WhatsApp Business (Kommunikationskanal; Ende-zu-Ende-Verschlüsselung der Inhalte, Zugang von WhatsApp zu Metadaten),
- Microsoft 365 / Bookings / Teams (Terminvereinbarung und ggf. Videoberatung durch Schulsozialarbeitende),
- Usercentrics (Cookie- und Consent-Management),
- Google Analytics, Google Tag Manager und Looker Studio (Webanalyse, Datenvisualisierung, nur mit Einwilligung),
- Storyblok (Content-Management der Website).

Damit verbunden sind u. a. folgende Risiken:

- Drittlandübermittlungen (vor allem USA),
- technische Störungen oder Sicherheitslücken,
- unverschlüsselte Übertragung von SMS (auf dem Weg vom Handy der Jugendlichen zum Netzbetreiber),
- Missbrauch einzelner Dienste,
- mögliche Re-Identifikationsrisiken bei Kombination von Daten.

Zur Risikominimierung werden u. a. umgesetzt:

- Auftragsverarbeitungsverträge (AVV) mit allen relevanten Dienstleistern,
- Nutzung von Standardvertragsklauseln und/oder EU-US Data Privacy Framework bei Drittlandübermittlungen,
- strenge Datensparsamkeit (nur so viele Daten, wie wirklich benötigt werden),
- Beschränkung von Funktionen (z. B. kein Adressbuchabgleich bei WhatsApp, kein Bildversand im Peer-Chat),
- Testphasen (z. B. zwei MS-365-Testaccounts) zur frühzeitigen Erkennung von Problemen,
- regelmäßige Überprüfung der Systeme, Sicherheitsupdates und Anpassung an neue rechtliche Vorgaben.

6. Verantwortlichkeiten, Transparenz und Ausblick

Verantwortlicher im Sinne der DS-GVO für RealTalk (Peer-Chat, Plattform):
Deutsches Rotes Kreuz e.V., Generalsekretariat, Carstennstraße 58, 12205 Berlin.

Datenschutzbeauftragter:

advokIT Datenschutz / Weißmann Datenschutz GmbH, erreichbar unter der im allgemeinen Datenschutzhinweis genannten Adresse/E-Mail.

DRK-Kreisverbände und andere Träger
sind eigene Verantwortliche für:

- die Schulsozialarbeit und dort geführte Beratungen,
- die Terminbuchung (z. B. über Microsoft Bookings),
- die Nutzung von Microsoft Teams und internen Systemen.

RealTalk sichert Transparenz durch:

- Datenschutzhinweise auf RealTalk.help,
- FAQ und jugendgerechte Erklärungen auf RealTalk.help,
- klar benannte Ansprechpersonen für Datenschutzfragen,
- die Möglichkeit, Rechte nach DSGVO (Auskunft, Löschung, Berichtigung, Widerspruch etc.) wahrzunehmen.

Ausblick:

Das Datenschutzkonzept wird fortlaufend weiterentwickelt – gemeinsam mit:

- Jugendlichen (z. B. im Projektbeirat),
- Schul- und Jugendsozialarbeitenden,
- Datenschutzexpert*innen und Forschungspartnern.

Geplant sind u. a.:

- eine weitere Anpassung des Termin-Systems an unterschiedliche Kontexte (offene Jugendarbeit, Jugendzentren, Standorte ohne MS 365),
- die Entwicklung verständlicher Materialien in einfacher Sprache und ggf. weiteren Sprachen. So soll gewährleistet werden, dass RealTalk dauerhaft ein sicherer, anonymer und datenschutzkonformer Raum bleibt – und gleichzeitig Brücken zu den professionellen Hilfestrukturen baut, die Jugendliche vor Ort brauchen.