



BrainWave Software

Attrian

Datenschutzerklärung

June 2024

1. Einleitung

Die BrainWave Software GmbH (nachfolgend "BrainWave", "wir", "uns" oder "unser") nimmt den Schutz Ihrer personenbezogenen Daten sehr ernst. Diese Datenschutzrichtlinien informieren Sie darüber, welche Daten wir erheben, wie wir diese verwenden und welche Rechte Sie in Bezug auf Ihre Daten haben.

2. Verantwortlicher

Verantwortlich für die Datenverarbeitung im Zusammenhang mit der Nutzung der Plattform Attrian ist:

BrainWave Software GmbH
Konrad Adenauer Allee 35, 86150 Augsburg

[Impressum](#)

[E-Mail Datenschutzbeauftragter](#)

Datenschutzbeauftragter

Noch zu finden

3. Erhobene Daten

3.1 Automatisch erhobene Daten

- **Nutzungsdaten:** Informationen über Ihre Interaktion mit der Plattform, einschließlich IP-Adresse, Browsertyp, Zugriffszeiten, besuchte Seiten und angeklickte Links.
- **Gerätedaten:** Informationen über das Gerät, das Sie für den Zugriff auf die Plattform verwenden, einschließlich Gerätetyp, Betriebssystem und Gerätekennungen.

3.2 Von Ihnen bereitgestellte Daten

- **Registrierungsdaten:** Vorname, Nachname, E-Mail-Adresse, Telefonnummer, Firmenname (bei beruflicher Nutzung), und Passwort.
- **Profilinformationen:** Profilbild, Präferenzen, und andere freiwillig bereitgestellte Informationen.
- **Zahlungsverkehrsdaten:** Bankverbindung, IBAN, Kreditkartendaten, Rechnungsadressen etc.
- **Kommunikationsdaten:** Inhalte von Nachrichten, die Sie an unseren Kundensupport oder andere Nutzer senden.
- Hochgeladene Daten zur Nutzung der Signaturdienste
- Ihre Signatur, falls Sie diese in der Plattform speichern

3.3 Von Dritten erhobenen Daten

Zum Zwecke der Identifizierung und Autorisierung des Nutzers können Daten aus Drittquellen mit Ihrer Zustimmung erhoben werden.

Solche sind:

Öffentliche Quellen und Register wie z.B. Handelsregister.

Daten von verifizierten Dienstleistern: Hierzu können spezialisierte Dienstleister in IT-Sicherheit und Betrugsprävention gehören. Vordergründig können Ihre Daten durch Ihre Einwilligung von Ihrem Arbeitgeber zur zwecke der Identifikation durch den Arbeitgeber erhoben werden.

Automatische Daten aus dem Besuch der Webseite wie IP Adresse und OS Ihres Gerätes.

3.4 Datenteilung zur Zwecke der gesetzlichen und vertraglichen Pflichten.

- **Identifizierungsdaten:** Bei Nutzung der Qualifizierten Elektronischen Signatur werden Ihre Identifizierungsdaten zur Zwecke der Überprüfung und Erstellung der Zertifikate an unseren TSP Halcom CA weitergeleitet.
- **Signaturdaten:** Bei Nutzung des elektronischen Signaturdienstes durch den Trusted Service Provider Halcom CA (QES) werden relevante Signaturdaten verarbeitet.

[Halcom Datenschutz](#)

- **Dateidaten:** Profildaten, Identitätsdaten, sowie Dateien, die Sie hochladen, teilen oder speichern, sowie alle anderen Daten der Plattform hinsichtlich Transaktionen und Nutzung werden in der sicheren Cloud der Concat AG verwaltet.
- **Zahlungsverkehr Daten:** Zur Zwecke der Zahlungsabwicklung werden alleine durch den zertifizierten Anbieter [Stripe](#) erhoben, gespeichert und verwaltet.

4. Verarbeitungszwecke und Rechtsgrundlagen

4.1 Bereitstellung der Dienste

- Zweck: Betrieb und Verwaltung der Plattform, Bereitstellung der Funktionen, die Sie nutzen, Revisionssicherheit.
- Rechtsgrundlage: Erfüllung des Vertrages (Art. 6 Abs. 1 lit. b DSGVO).

4.2 Verbesserung der Dienste

- Zweck: Analyse der Nutzung der Plattform zur Verbesserung der Dienste und Nutzererfahrung.
- Rechtsgrundlage: Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO).

4.3 Kommunikation

- Zweck: Bearbeitung von Anfragen, Support, und Kommunikation mit Nutzern.
- Rechtsgrundlage: Erfüllung des Vertrages und berechtigtes Interesse (Art. 6 Abs. 1 lit. b und f DSGVO).

4.4 Marketing und Werbung

- Zweck: Zusendung von Marketingmaterialien und Werbung, sofern Sie dem zugestimmt haben.
- Rechtsgrundlage: Einwilligung (Art. 6 Abs. 1 lit. a DSGVO).

4.5 Einhaltung rechtlicher Verpflichtungen

- Zweck: Einhaltung gesetzlicher Anforderungen insbesondere der eIDAS und DSGVO, sowie Rechtsdurchsetzung und Schutz unserer Rechte.
- Rechtsgrundlage: Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 lit. c DSGVO).

5. Speicherung der Dokumente innerhalb der Plattform Attrian

5.1 Zweck und Dauer der Speicherung

- Zweck: Speicherung der Dokumente zur Nutzung der Plattformfunktionen, einschließlich Hochladen, Teilen, Signieren und Archivieren von Dokumenten.
- Dauer: Dokumente werden so lange gespeichert, wie dies für die Erfüllung des Vertrages erforderlich ist oder wie es gesetzliche Aufbewahrungsfristen vorsehen. Archivierte Dokumente können auf Anfrage gelöscht werden, sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

5.2 Zugriff und Sicherheit

- Zugriffsrechte: Nur autorisierte Nutzer haben Zugriff auf die gespeicherten Dokumente. Der Zugriff kann je nach Nutzerrolle und Berechtigung variieren.
- Sicherheitsmaßnahmen: Implementierung von Verschlüsselungsmechanismen und Zugangskontrollen, um die Vertraulichkeit und Integrität der gespeicherten Dokumente zu gewährleisten.

6. Datenschutzbestimmungen hinsichtlich Filesharing

6.1 Erhobene Daten

- Teilen von Dateien: Informationen über die geteilten Dateien, einschließlich Dateiname, Dateigröße, und Freigabeempfänger.
- Nutzerinformationen: Kontaktinformationen der Personen, mit denen Dateien geteilt werden.

6.2 Zweck und Rechtsgrundlage

- Zweck: Ermöglichung des Teilens von Dateien zwischen Nutzern der Plattform.
- Rechtsgrundlage: Erfüllung des Vertrages (Art. 6 Abs. 1 lit. b DSGVO).

6.3 Sicherheitsmaßnahmen

- Zugriffskontrollen: Nur berechtigte Personen haben Zugriff auf die geteilten Dateien.
- Nachverfolgung: Protokollierung der Freigabeaktivitäten, um Missbrauch zu verhindern.

7. Identifizierung von Personen für die qualifizierte elektronische Signatur (QES)

1.Daten Erhebung

1.1 ERHOBENE DATEN

- Identifikationsdaten: Vorname, Nachname, Geburtsdatum, Adresse, Ausweisdokumente (z.B. Personalausweis oder Reisepass).

1.2 ZWECK UND RECHTSGRUNDLAGE

- Zweck: Überprüfung der Identität zur Ermöglichung der QES.
- Rechtsgrundlage: Erfüllung rechtlicher Verpflichtungen und Vertragserfüllung (Art. 6 Abs. 1 lit. b und c DSGVO).

2.Übermittlung der Identifikationsdaten an Halcom CA

2.1 ZWECK UND RECHTSGRUNDLAGE

- Zweck: Übermittlung der Identifikationsdaten an den Trusted Service Provider Halcom CA zur Beantragung der QES.
- Rechtsgrundlage: Vertragserfüllung und berechtigtes Interesse (Art. 6 Abs. 1 lit. b und f DSGVO).

2.2 EINWILLIGUNG

- Einwilligung: Nutzer müssen der Übermittlung ihrer Identifikationsdaten an Halcom CA zustimmen.

3. Überprüfung der Identität und Feststellung der Echtheit

3.1 ERHOBENE DATEN

- Identitätsprüfung: Vorname, Nachname, Geburtsdatum, Adresse, Ausweisdokumente, biometrische Daten (sofern erforderlich).

3.2 ZWECK UND RECHTSGRUNDLAGE

- Zweck: Sicherstellung der Echtheit der Identität zur Nutzung der QES.
- Rechtsgrundlage: Vertragserfüllung und rechtliche Verpflichtung (Art. 6 Abs. 1 lit. b und c DSGVO).

3.3 RECHTE UND FREIGABEN

- Einwilligung: Nutzer müssen der Identitätsprüfung und der Verarbeitung der entsprechenden Daten zustimmen.

4.Berechtigungen und Ablehnung der Identifikation

4.1 BERECHTIGUNGEN VON BRAINWAVE UND HALCOM

- Überprüfung: BrainWave ist berechtigt, die übermittelten Identifikationsdaten zu überprüfen.

Halcom Ca. ist berechtigt, die übermittelten Identifikationsdaten zu überprüfen.

- Entscheidung: BrainWave behält sich das Recht vor, die Identifikation bei negativen Prüfungsergebnissen abzulehnen.

4.2 ABLEHNUNG DER IDENTIFIKATION

- Mitteilung: Im Falle einer Ablehnung der Identifikation wird der Nutzer entsprechend informiert.
- Konsequenzen: Eine Ablehnung der Identifikation kann zur Verweigerung des Zugangs zu bestimmten Diensten führen, insbesondere zur QES.

8. Identifizierung juristischer Personen

1. Datenerhebung:

1.1. ERHOBENE DATEN

- Unternehmensdaten: Firmenname, Rechtsform, Handelsregisternummer, Umsatzsteuer-Identifikationsnummer, Geschäftssitz, Kontaktinformationen (Telefonnummer, E-Mail-Adresse).
- Vertreterdaten: Vorname, Nachname, Geburtsdatum, Adresse, Ausweisdokumente (z.B. Personalausweis oder Reisepass) der vertretungsberechtigten Personen.

1.2. ZWECK UND RECHTSGRUNDLAGE:

- Zweck: Überprüfung der Identität und Rechtsfähigkeit der juristischen Person zur Nutzung der Plattform Attrian.
- Rechtsgrundlage: Vertragserfüllung und rechtliche Verpflichtung (Art. 6 Abs. 1 lit. b und c DSGVO).

3. Anforderungen an die vollständige Identifikation

1. UNTERNEHMENSNACHWEISE:

- Einreichung aktueller Unternehmensdokumente wie Handelsregistorauszug, Gesellschafterliste, Satzung oder andere relevante Dokumente, die die rechtliche Existenz und Vertretungsberechtigung des Unternehmens belegen.

2. VERTRETERNACHWEISE:

- Einreichung der Ausweisdokumente der vertretungsberechtigten Personen.
- Nachweis der Vertretungsbefugnis durch entsprechende Dokumente wie Vollmachten oder Beschlüsse.

4. Verarbeitungszwecke und Aufbewahrung

1. ZWECK DER VERARBEITUNG:

- Überprüfung der rechtlichen Identität und Vertretungsbefugnis zur Nutzung der qualifizierten elektronischen Signatur (QES) und anderer Dienstleistungen auf der Plattform Attrian.

2. DAUER DER AUFBEWAHRUNG:

- Identifikationsdaten werden für die Dauer des Vertragsverhältnisses gespeichert und anschließend gemäß den gesetzlichen Aufbewahrungsfristen gelöscht.

5. Übermittlung der Identifikationsdaten an Halcom CA

1. ZWECK UND RECHTSGRUNDLAGE:

- Zweck: Übermittlung der Identifikationsdaten an den Trusted Service Provider Halcom CA zur Beantragung der QES.
- Rechtsgrundlage: Vertragserfüllung und berechtigtes Interesse (Art. 6 Abs. 1 lit. b und f DSGVO).

2. EINWILLIGUNG:

Die juristische Person muss der Übermittlung ihrer Identifikationsdaten an Halcom CA zustimmen.

Dies erfolgt regelmäßig durch die Zustimmung des Vertretungsbefugten.

6. Überprüfung der Identität und Feststellung der Echtheit

1. ERHOBENE DATEN:

- Firmenname, Rechtsform, Handelsregisternummer, Umsatzsteuer-Identifikationsnummer, Geschäftssitz, Kontaktinformationen, Ausweisdokumente und Vertretungsnachweise der vertretungsberechtigten Personen.

2. ZWECK UND RECHTSGRUNDLAGE:

- Zweck: Sicherstellung der Echtheit der Identität der juristischen Person und ihrer Vertreter zur Nutzung der QES.
- Rechtsgrundlage: Vertragserfüllung und rechtliche Verpflichtung (Art. 6 Abs. 1 lit. b und c DSGVO).

3. RECHTE UND FREIGABEN:

- Die vertretungsberechtigten Personen müssen der Identitätsprüfung und der Verarbeitung der entsprechenden Daten zustimmen.

7. Berechtigungen und Ablehnung der Identifikation

1. BERECHTIGUNGEN VON BRAINWAVE:

- Überprüfung: BrainWave und Halcom Ca ist berechtigt, die übermittelten Identifikationsdaten zu überprüfen.
- Entscheidung: BrainWave behält sich das Recht vor, die Identifikation bei negativen Prüfungsergebnissen abzulehnen.

2. ABLEHNUNG DER IDENTIFIKATION:

- Mitteilung: Im Falle einer Ablehnung der Identifikation wird die juristische Person entsprechend informiert.
- Konsequenzen: Eine Ablehnung der Identifikation kann zur Verweigerung des Zugangs zu bestimmten Diensten führen, insbesondere zur QES.

8. Einwilligung und Rechte der betroffenen Personen

1. EINWILLIGUNG:

- Die vertretungsberechtigten Personen müssen der Verarbeitung ihrer Identifikationsdaten zustimmen, bevor die Identifikation durchgeführt wird.

2. RECHTE DER BETROFFENEN PERSONEN:

- Die betroffenen Personen haben das Recht, Auskunft über die von ihnen verarbeiteten Daten zu erhalten, Berichtigung oder Löschung ihrer Daten zu verlangen und der Verarbeitung ihrer Daten zu widersprechen.

9. Ihre Rechte

1. Auskunftsrecht

Sie haben das Recht, Auskunft über die von uns verarbeiteten personenbezogenen Daten zu erhalten (Art. 15 DSGVO).

2. Berichtigungsrecht

Sie haben das Recht, die Berichtigung unrichtiger oder unvollständiger personenbezogener Daten zu verlangen (Art. 16 DSGVO).

3. Löschungsrecht

Sie haben das Recht, die Löschung Ihrer personenbezogenen Daten zu verlangen, sofern die gesetzlichen Voraussetzungen dafür vorliegen (Art. 17 DSGVO).

4 Einschränkung des Rechts

Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen (Art. 18 DSGVO).

5 Widerspruchsrecht

Sie haben das Recht, der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen (Art. 21 DSGVO).

6 Recht auf Datenübertragbarkeit

Sie haben das Recht, Ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten einem anderen Verantwortlichen zu übermitteln (Art. 20 DSGVO).

7 Widerrufsrecht

Sie haben das Recht, eine erteilte Einwilligung zur Verarbeitung Ihrer personenbezogenen Daten jederzeit zu widerrufen (Art. 7 Abs. 3 DSGVO).

10. Datensicherheit

Wir setzen technische und organisatorische Sicherheitsmaßnahmen ein, um Ihre Daten gegen zufällige oder vorsätzliche Manipulation, Verlust, Zerstörung oder den Zugriff unberechtigter Personen zu schützen.

1 Technische und organisatorische Maßnahmen

BWS implementiert und unterhält die folgenden Maßnahmen zur Gewährleistung der Datensicherheit:

- Verschlüsselung: Einsatz von Verschlüsselungstechnologien zum Schutz personenbezogener Daten während der Übertragung und Speicherung.
- Zugriffskontrollen: Einrichtung strenger Zugangskontrollen, um sicherzustellen, dass nur autorisierte Personen Zugriff auf personenbezogene Daten haben.
- Firewalls und Anti-Malware: Verwendung von Firewalls und Anti-Malware-Programmen, um unbefugte Zugriffe und Schadsoftware abzuwehren.
- Sicherheitsupdates: Regelmäßige Aktualisierung der Software und Systeme, um Sicherheitslücken zu schließen und den Schutz vor neuen Bedrohungen zu gewährleisten.
- Datensicherungen: Regelmäßige Erstellung von Datensicherungen, um die Datenintegrität und Verfügbarkeit zu gewährleisten.
- Protokollierung und Überwachung: Implementierung von Protokollierungs- und Überwachungsmechanismen, um Sicherheitsvorfälle schnell zu erkennen und darauf reagieren zu können.

2 Meldung von Sicherheitsvorfällen

Im Falle eines Sicherheitsvorfalls, der die Vertraulichkeit, Integrität oder Verfügbarkeit personenbezogener Daten beeinträchtigen könnte, verpflichtet sich BWS, den betroffenen Nutzer unverzüglich zu informieren. BWS wird angemessene Maßnahmen ergreifen, um den Vorfall zu untersuchen und zu beheben.

3 Schulung und Sensibilisierung

BWS stellt sicher, dass alle Mitarbeiter regelmäßig Schulungen und Sensibilisierungsmaßnahmen in Bezug auf Datenschutz und Datensicherheit erhalten, um ein hohes Maß an Sicherheitsbewusstsein zu gewährleisten.

4 Pflichten der Nutzer

Nutzer der Attrian Plattform sind verpflichtet, ihre Zugangsdaten sicher zu verwahren und dafür zu sorgen, dass unbefugte Dritte keinen Zugriff auf diese Daten erhalten. Nutzer müssen geeignete Sicherheitsmaßnahmen ergreifen, um ihre eigenen Systeme vor unbefugtem Zugriff und Schadsoftware zu schützen.

5. Erfüllung der Anforderungen der DSGVO und des BDSG durch BrainWave Software GmbH (BWS)

1. Artikel 5 DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten

BWS verpflichtet sich, die folgenden Grundsätze bei der Verarbeitung personenbezogener Daten zu beachten:

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
 - BWS stellt sicher, dass die Verarbeitung personenbezogener Daten nur auf einer rechtmäßigen Grundlage erfolgt, wie z.B. der Einwilligung des Betroffenen, der Erfüllung eines Vertrags oder eines berechtigten Interesses.

- BWS verarbeitet personenbezogene Daten in einer fairen und transparenten Weise. Betroffene werden über die Zwecke der Datenverarbeitung und ihre Rechte umfassend informiert.
- **Zweckbindung**
 - Personenbezogene Daten werden nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet.
- **Datenminimierung**
 - BWS verarbeitet nur diejenigen personenbezogenen Daten, die für die Erreichung der Zwecke der Verarbeitung erforderlich sind.
- **Richtigkeit**
- BWS stellt sicher, dass personenbezogene Daten sachlich richtig und auf dem neuesten Stand sind. Unrichtige Daten werden unverzüglich berichtigt oder gelöscht.
- **Speicherbegrenzung**
 - Personenbezogene Daten werden nur so lange gespeichert, wie es für die Zwecke der Verarbeitung erforderlich ist. Danach werden die Daten sicher gelöscht oder anonymisiert.
- **Integrität und Vertraulichkeit**
 - BWS ergreift geeignete technische und organisatorische Maßnahmen, um die Sicherheit personenbezogener Daten zu gewährleisten und sie vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung zu schützen.
- **Rechenschaftspflicht**
 - BWS ist für die Einhaltung der Grundsätze der Datenverarbeitung verantwortlich und kann diese Einhaltung nachweisen.

2. Artikel 24 DSGVO: Verantwortliche Stelle und Maßnahmen zum Datenschutz

- BWS hat geeignete technische und organisatorische Maßnahmen implementiert, um sicherzustellen, dass die Verarbeitung personenbezogener Daten im Einklang mit der DSGVO erfolgt. Dies umfasst regelmäßige Schulungen der Mitarbeiter, interne Audits und die Ernennung eines Datenschutzbeauftragten.

3. Artikel 25 DSGVO: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

- BWS berücksichtigt den Datenschutz bereits bei der Entwicklung neuer Systeme und Prozesse ("Privacy by Design").
- BWS stellt sicher, dass standardmäßig nur die personenbezogenen Daten verarbeitet werden, die für den jeweiligen Zweck erforderlich sind ("Privacy by Default").

4. Artikel 32 DSGVO: Sicherheit der Verarbeitung

- **Verschlüsselung:** BWS verwendet Verschlüsselungstechnologien, um personenbezogene Daten während der Übertragung und Speicherung zu schützen.
- **Zugriffskontrollen:** Strenge Zugangskontrollen stellen sicher, dass nur autorisierte Personen auf personenbezogene Daten zugreifen können.
- **Sicherheitsupdates:** Regelmäßige Sicherheitsupdates und Patch-Management gewährleisten, dass alle Systeme auf dem neuesten Stand und sicher sind.
- **Datensicherungen:** Regelmäßige Sicherung der Daten, um Datenverluste zu verhindern und die Datenintegrität sicherzustellen.
- **Protokollierung und Überwachung:** BWS überwacht die Systeme kontinuierlich, um Sicherheitsvorfälle frühzeitig zu erkennen und zu reagieren.

5. Artikel 33 DSGVO: Meldung von Datenschutzverletzungen an die Aufsichtsbehörde

- BWS hat Verfahren implementiert, um Datenschutzverletzungen zu erkennen, zu melden und darauf zu reagieren.
- Im Falle einer Datenschutzverletzung informiert BWS unverzüglich die zuständige Aufsichtsbehörde innerhalb von 72 Stunden nach Bekanntwerden der Verletzung.

6. Artikel 34 DSGVO: Benachrichtigung der von einer Datenschutzverletzung betroffenen Person

- Wenn die Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, informiert BWS die betroffenen Personen unverzüglich über die Verletzung und gibt dabei klare und verständliche Informationen über die Art der Verletzung und die ergriffenen Maßnahmen.

7. § 9 BDSG: Technische und organisatorische Maßnahmen

- BWS hat technische und organisatorische Maßnahmen getroffen, um die Anforderungen des § 9 BDSG zu erfüllen. Dazu gehören Maßnahmen zur Zugangskontrolle, Eingabekontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungskontrolle.

11. Liste der Dienstleister

Name	Adresse	Zuständigkeit	Tätigkeit	Links
Halcom CA		Trusted service Provider		
Concat AG		Hosting		

HubSpot	Internetpräsenz,CRM und Marketing
Datenschutzbeauftragter	

12. Haftungsausschluss

BWS haftet nicht für Schäden oder Verluste, die durch die Nichterfüllung der Pflichten zur Datensicherheit durch die Nutzer entstehen, außer in Fällen von Vorsatz oder grober Fahrlässigkeit.

13. Änderungen der Datenschutzrichtlinien

BWS behält sich das Recht vor, diese Regelung jederzeit zu ändern. Nutzer werden über wesentliche Änderungen in geeigneter Weise informiert, z.B. durch Benachrichtigungen auf der Plattform oder per E-Mail.

Wir behalten uns das Recht vor, diese Datenschutzrichtlinien jederzeit zu ändern. Änderungen werden auf unserer Website veröffentlicht. Bitte überprüfen Sie diese Richtlinien regelmäßig auf Aktualisierungen.

Attrian Wiki

Company address: Konrad Adenauer Allee 35, 86150, Augsburg

Company Name: BrainWave Software GmbH

Email: office@brainwave-software.de

homepage: <https://www.brainwave-software.de/>

Attrian: <https://attrian-frontend-dev.stack.bw-devops.com/>

Attrian-Wiki: <https://attrian-public-wiki.stack.bw-devops.com/>