Technische Spezifikation und rechtliche Einordnung der bchic Web-Analyse (Stand 28.08.2025)

1. Grundlagen und Funktionsprinzip

Dieser Abschnitt beschreibt die Zielsetzung, die grundlegende Funktionsweise sowie die rechtliche Abgrenzung der von bchic Analytics verarbeiteten Daten.

1.1 Einwilligungsfreie Web-Analyse

Die Zielsetzung von bchic Analytics ist die Bereitstellung einer präzisen und datenschutzkonformen Web-Analyse. Herkömmliche Analyseverfahren erfordern aufgrund der Verarbeitung personenbezogener Daten und/oder des Zugriffs auf Endgeräte eine aktive Nutzereinwilligung (Consent) gemäß DSGVO und TDDDG. Dies führt in der Praxis zu unvollständigen Datensätzen und beeinträchtigt die Nutzererfahrung. bchic Analytics wurde konzipiert, um eine technisch und rechtlich robuste Alternative zu bieten, die aussagekräftige Analysedaten ohne das Erfordernis einer Nutzereinwilligung ermöglicht, um sowohl die Datenlage als auch die Web-Erfahrung der Benutzer zu verbessern.

1.2 Funktionsprinzip im Überblick

Das System basiert auf dem Prinzip des "Privacy-by-Design". Die Datenerfassung erfolgt serverseitig (Server-Side Tracking), ohne dass Informationen auf dem Endgerät des Nutzers gespeichert oder von diesem ausgelesen werden (cookieless). Eingehende Anfragen an den Tracking-

Technical Specification and Legal Classification of bchic Web Analytics (Date: 2025-08-28)

1. Foundations and Operating Principle

This section describes the objective, the fundamental mode of operation, and the legal classification of the data processed by bchic Analytics.

1.1 Consent-Free Web Analytics

The objective of bchic Analytics is to provide precise and data-protection-compliant web analytics. Conventional analysis methods require active user consent in accordance with the GDPR and TDDDG due to the processing of personal data and/or access to end devices. In practice, this leads to incomplete data sets and negatively impacts the user experience. bchic Analytics was designed to offer a technically and legally robust alternative that enables meaningful analysis data without the need for user consent, thereby improving both the data quality and the web experience of the users.

1.2 Overview of the Operating Principle

The system is based on the "Privacy-by-Design" principle. Data collection takes place server-side (server-side tracking) without information being stored on or read from the user's end device (cookieless). Incoming requests to the tracking server undergo an immediate, irreversible

Server durchlaufen einen unmittelbaren, unumkehrbaren Anonymisierungsprozess. Personenbezogene Rohdaten, insbesondere die vollständige IP-Adresse, werden zu keinem Zeitpunkt gespeichert. Die anonymisierten Signale werden ausschließlich zu aggregierten Statistiken verarbeitet, die keine Rückschlüsse auf das Verhalten einzelner Personen zulassen.

anonymization process. Personal raw data, specifically the complete IP address, is never stored at any time. The anonymized signals are processed exclusively into aggregated statistics that do not allow conclusions to be drawn about the behavior of individual persons.

1.3 Abgrenzung zu personenbezogenen Daten

Die Datenschutz-Grundverordnung (DSGVO) findet Anwendung auf die Verarbeitung personenbezogener Daten (definiert in Art. 4 Nr. 1 DSGVO). Gemäß Erwägungsgrund 26 der DSGVO finden die Grundsätze des Datenschutzes keine Anwendung auf anonymisierte Informationen, d.h. Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Durch das in Kapitel 2 detailliert beschriebene Anonymisierungsverfahren stellt bchic Analytics sicher, dass die für die Analyse verarbeiteten Daten zu keinem Zeitpunkt die Identifizierung einer Person ermöglichen. Folglich handelt es sich bei den resultierenden Analysedaten nicht um personenbezogene Daten im Sinne der DSGVO. Daraus ergibt sich, dass für deren Verarbeitung keine Rechtsgrundlage nach Art. 6 DSGVO (z.B. eine Einwilligung) erforderlich ist.

1.3 Distinction from Personal Data

The General Data Protection Regulation (GDPR) applies to the processing of personal data (defined in Art. 4 No. 1 GDPR). According to Recital 26 of the GDPR, the principles of data protection do not apply to anonymous information, i.e., information which does not relate to an identified or identifiable natural person. Through the anonymization process described in detail in Chapter 2, bchic Analytics ensures that the data processed for analysis never enables the identification of a person. Consequently, the resulting analysis data does not constitute personal data within the meaning of the GDPR. It follows that no legal basis under Art. 6 GDPR (e.g., consent) is required for their processing.

2. Technische Architektur und Datenverarbeitung

Dieser Abschnitt beschreibt die technische Infrastruktur, den gesamten Datenverarbeitungszyklus von der

2. Technical Architecture and Data Processing

This section describes the technical infrastructure, the entire data processing cycle from collection to storage, and the

Erfassung bis zur Speicherung sowie die implementierten Sicherheitsmaßnahmen zum Schutz der Systemintegrität und der Daten.

2.1 Datenerfassung: Server-Side Tracking ohne Endgerätezugriff.

Die Datenerfassung erfolgt über ein asynchrones JavaScript-Skript, das auf der Website des Kunden implementiert wird. Beim Aufruf einer Seite durch einen Nutzer sendet dieses Skript eine Anfrage (Request) an unsere Server-Infrastruktur.

• Übertragene Rohdaten: Diese initiale Anfrage enthält technische Metadaten, die für die Verarbeitung notwendig sind: die IP-Adresse des Nutzers, den User-Agent-String des Browsers, die aufgerufene URL sowie den Referrer.

• Kein Endgerätezugriff: Das Skript führt keine Operationen aus, die auf Informationen im Endgerät des Nutzers zugreifen oder diese dort speichern. Es werden weder Cookies gesetzt oder ausgelesen, noch wird auf den Local Storage des Browsers zugegriffen.

• Unmittelbare Verarbeitung: Die übermittelten Rohdaten werden ausschließlich im flüchtigen Speicher (RAM) des Servers für den nachfolgend beschriebenen, sofortigen Anonymisierungsprozess vorgehalten und zu keinem Zeitpunkt auf Festplatten oder in Datenbanken gespeichert.

2.2 Anonymisierungsverfahren: Hashing, Salting und Salt-Rotation

Unmittelbar nach Eingang der Anfrage wird ein unumkehrbarer

implemented security measures to protect system integrity and data.

2.1 Data Collection: Server-Side Tracking without End Device Access

Data collection is performed via an asynchronous JavaScript script implemented on the customer's website. When a user visits a page, this script sends a request to our server infrastructure.

• Transmitted Raw Data: This initial request contains technical metadata necessary for processing: the user's IP address, the browser's User-Agent string, the requested URL, and the referrer.

• No End Device Access: The script performs no operations that access information on the user's end device or store information there. No cookies are set or read, nor is the browser's Local Storage accessed.

• Immediate Processing: The transmitted raw data is held exclusively in the volatile memory (RAM) of the server for the immediate anonymization process described below and is never stored on hard drives or in databases at any time.

2.2 Anonymization Procedure: Hashing, Salting, and Salt Rotation

Immediately upon receipt of the request, an irreversible anonymization process is

Anonymisierungsprozess durchgeführt, um jeglichen Personenbezug zu entfernen.

1. Hash-Generierung: Aus der IP-Adresse, dem User-Agent sowie einer für jede Kunden-Website einzigartigen ID (Website-ID) wird ein kryptographischer Hash-Wert (z.B. mittels SHA-256) generiert. Dieser Hash dient als temporärer, anonymer Identifikator für einen einzelnen Besuch. Die Einbeziehung der Website-ID stellt sicher, dass für denselben Nutzer auf zwei unterschiedlichen Websites, die bchic Analytics einsetzen, zwei völlig verschiedene, nicht korrelierbare Hash-Werte erzeugt werden. Ein Cross-Site-Tracking ist damit technisch ausgeschlossen.

2. Salting: Um eine Identifizierung durch den Abgleich mit vorberechneten Hash-Listen (Rainbow Tables) zu verhindern, wird der generierte Hash mit einer zufälligen, geheimen Zeichenkette, einem sogenannten "Salt", versehen.

3. Tägliche Salt-Rotation: Dieser Salt wird systemweit alle 24 Stunden automatisch und unumkehrbar ausgetauscht. Dies hat zur Folge, dass der Hash-Wert für denselben Nutzer am Folgetag ein völlig anderer ist. Dadurch wird die Erstellung von nutzerbasierten, geräteübergreifenden oder langfristigen Verhaltensprofilen technisch unmöglich gemacht.

4. Verwerfen der Rohdaten: Nach Abschluss dieses Prozesses, der in Millisekunden abläuft, werden die ursprüngliche IP-Adresse und der User-Agent vollständig und permanent aus dem Arbeitsspeicher verworfen. Das Ergebnis ist ein anonymer Datensatz, der lediglich einen für 24 Stunden gültigen, nicht

carried out to remove any personal reference.

1. Hash Generation: A cryptographic hash value (e.g., via SHA-256) is generated from the IP address, the User-Agent, and a unique ID (Website-ID) for each customer website. This hash serves as a temporary, anonymous identifier for a single visit. Including the Website-ID ensures that two completely different, non-correlatable hash values are generated for the same user on two different websites using bchic Analytics. Cross-site tracking is thus technically excluded.

2. Salting: To prevent identification through comparison with pre-calculated hash lists (rainbow tables), the generated hash is appended with a random, secret character string, a so-called "Salt".

3. Daily Salt Rotation: This Salt is automatically and irreversibly exchanged system-wide every 24 hours. As a result, the hash value for the same user is completely different the following day. This makes the creation of user-based, cross-device, or long-term behavioral profiles technically impossible.

4. Discarding Raw Data: Upon completion of this process, which takes place in milliseconds, the original IP address and User-Agent are completely and permanently discarded from the working memory. The result is an anonymous data set containing only a fingerprint valid for 24 hours (which cannot be reverse-engineered) and non-personal event data (e.g., page views, session duration).

zurückrechenbaren Fingerprint sowie nicht-personenbezogene Event-Daten (z.B. Seitenaufruf, Verweildauer) enthält.

2.3 Datenhaltung: Serverstandort, Provider und Aufbewahrungsdauer

Unsere gesamte Server-Infrastruktur wird bei der Hetzner Online GmbH, einem deutschen, nach DIN ISO/IEC 27001 zertifizierten Provider, betrieben. Der primäre Standort für die Datenverarbeitung und -speicherung ist der Rechenzentrumspark in Falkenstein, Deutschland. Zur Gewährleistung der Hochverfügbarkeit werden redundante Systeme in weiteren EU-Standorten des Providers in Nürnberg (Deutschland) und Helsinki (Finnland) vorgehalten. Es findet zu keinem Zeitpunkt ein Datentransfer in Drittstaaten statt. Der Provider gewährleistet die physische Sicherheit der Infrastruktur durch mehrstufige Zugangskontrollen und eine 24/7-Überwachung der Hochsicherheitsbereiche. Die Speicherung umfasst ausschließlich anonymisierte und aggregierte Statistikdaten. Die Aufbewahrungsfristen sind wie folgt definiert: Aggregierte Monats- und Jahresstatistiken werden für maximal 24 Monate zur Analyse von Langzeittrends vorgehalten. Detailliertere, anonymisierte Tagesdaten werden nach 1 Jahr turnusmäßig gelöscht.

2.4 Datensicherheit: Verschlüsselung, Schutzmaßnahmen und Zugriffskontrolle

Der Schutz der Daten und der Systemintegrität wird durch eine durchgängige Verschlüsselungsstrategie sowie mehrstufige technische und organisatorische Maßnahmen

2.3 Data Storage: Server Location, Provider, and Retention Period

Our entire server infrastructure is operated by Hetzner Online GmbH, a German provider certified according to DIN ISO/IEC 27001. The primary location for data processing and storage is the data center park in Falkenstein, Germany. To ensure high availability, redundant systems are maintained at other EU locations of the provider in Nuremberg (Germany) and Helsinki (Finland). At no time does a data transfer to third countries take place. The provider guarantees the physical security of the infrastructure through multi-level access controls and 24/7 monitoring of high-security areas. Storage is limited exclusively to anonymized and aggregated statistical data. Retention periods are defined as follows: Aggregated monthly and annual statistics are kept for a maximum of 24 months for the analysis of long-term trends. More detailed, anonymized daily data is deleted on a regular basis after 1 year.

2.4 Data Security: Encryption, Protective Measures, and Access Control

Data protection and system integrity are guaranteed by a consistent encryption strategy and multi-level technical and organizational measures. All data transmissions, both from the user to the

gewährleistet. Sämtliche Datenübertragungen, sowohl vom Nutzer zum Server als auch systemintern, erfolgen ausschließlich über eine erzwungene TLS 1.3 Verschlüsselung (in-transit). Die Hochverfügbarkeit des Dienstes wird durch redundant ausgelegte Aktiv-Standby-Systeme und ein resilientes internes Warteschlangensystem sichergestellt. Ein kontinuierliches externes Monitoring dient der proaktiven Erkennung und Behebung von Systemstörungen. Der administrative Zugriff auf die Produktionssysteme unterliegt strengen internen Richtlinien. Er folgt dem „Principle of Least Privilege“, erfordert eine Multi-Faktor-Authentifizierung und ist auf autorisierte Mitarbeiter mit Sitz in Deutschland beschränkt. Um die Datenhoheit innerhalb der EU zu wahren, werden unsere Entwicklungsprozesse zudem auf einer eigenständig gehosteten GitLab-Instanz betrieben. Alle Mitarbeiter sind vertraglich zur Vertraulichkeit verpflichtet, und es besteht durch die technische Entkopplung unseres Systems zu keinem Zeitpunkt ein Zugriff auf die Systeme oder Daten unserer Kunden.

server and internally within the system, take place exclusively via enforced TLS 1.3 encryption (in-transit). The high availability of the service is ensured by redundant active-standby systems and a resilient internal queuing system. Continuous external monitoring serves for the proactive detection and rectification of system faults. Administrative access to production systems is subject to strict internal policies. It follows the "Principle of Least Privilege," requires multi-factor authentication, and is limited to authorized employees based in Germany. To maintain data sovereignty within the EU, our development processes are also operated on an independently hosted GitLab instance. All employees are contractually bound to confidentiality, and due to the technical decoupling of our system, there is no access to our customers' systems or data at any time.

3. Implementierung und rechtliche Bewertung

Dieser Abschnitt beschreibt den Prozess der technischen Implementierung sowie die daraus resultierende rechtliche Bewertung der Konformität von bchic Analytics mit der Datenschutz-Grundverordnung (DSGVO) und dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TDDDG).

3. Implementation and Legal Assessment

This section describes the process of technical implementation and the resulting legal assessment of bchic Analytics' conformity with the General Data Protection Regulation (GDPR) and the Telecommunications-Telemedia Data Protection Act (TDDDG).

3.1 Technische Implementierung des Tracking-Skripts

Die Integration von bchic Analytics ist bewusst ressourcenschonend und unkompliziert gestaltet, um den technischen Aufwand auf Kundenseite zu minimieren.

• Standard-Implementierung: Die Basisfunktion der Web-Analyse wird durch das Hinzufügen einer einzigen Zeile JavaScript-Code in den <head>-Bereich des HTML-Dokuments der Website aktiviert. Für diese Standardanalyse sind keine weiteren serverseitigen Anpassungen, Datenbankänderungen oder Konfigurationen erforderlich.

• Optionale Erweiterung (Event-Tracking): Sollen spezifische Nutzerinteraktionen wie das Klicken von Buttons, das Absenden von Formularen oder andere Events erfasst werden, kann dies durch das Hinzufügen von einfachen HTML-Attributen (z.B. data-bchic-event="...") zu den entsprechenden Elementen auf der Website realisiert werden. Diese Konfiguration ist optional und erfordert keinen zusätzlichen JavaScript-Code.

• Performance: Das Skript wird asynchron (async und oder defer) geladen. Dies stellt sicher, dass das Laden des bchic-Skripts das Rendern der Website und somit die wahrgenommene Ladezeit für den Endnutzer nicht blockiert oder negativ beeinflusst.

3.2 Rechtliche Bewertung gemäß DSGVO

Die Konformität mit der Datenschutz-Grundverordnung (DSGVO) basiert auf dem fundamentalen Prinzip, dass bchic

3.1 Technical Implementation of the Tracking Script

The integration of bchic Analytics is deliberately designed to be resource-efficient and uncomplicated to minimize the technical effort on the client side.

• Standard Implementation: The basic function of the web analysis is activated by adding a single line of JavaScript code to the <head> section of the website's HTML document. No further server-side adjustments, database changes, or configurations are required for this standard analysis.

• Optional Extension (Event Tracking): If specific user interactions such as clicking buttons, submitting forms, or other events are to be recorded, this can be achieved by adding simple HTML attributes (e.g., data-bchic-event="...") to the corresponding elements on the website. This configuration is optional and requires no additional JavaScript code.

• Performance: The script is loaded asynchronously (async and or defer). This ensures that the loading of the bchic script does not block or negatively influence the rendering of the website and thus the perceived loading time for the end user.

3.2 Legal Assessment according to GDPR

Conformity with the General Data Protection Regulation (GDPR) is based on

Analytics keine personenbezogenen Daten verarbeitet.

• Anwendungsbereich der DSGVO: Gemäß Art. 2 Abs. 1 DSGVO findet diese Anwendung auf die Verarbeitung personenbezogener Daten. Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

• Bedeutung der Anonymisierung: Der Erwägungsgrund 26 der DSGVO stellt klar: „Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen […].“

• Anwendung auf bchic analytics: Wie in Kapitel 2.2 dargelegt, durchläuft jede erfasste Information einen sofortigen und unumkehrbaren Anonymisierungsprozess. Darüber hinaus werden die anonymisierten Datenpunkte ausschließlich in aggregierter Form weiterverarbeitet. Das bedeutet, dass individuelle Nutzerpfade (User Journeys) oder Sitzungsaufzeichnungen weder gespeichert noch in den Auswertungen dargestellt werden. Analysen, wie beispielsweise die Ermittlung beliebter Seitenabfolgen, basieren stets auf einem kollektiven, zusammengefassten Datensatz. Es ist technisch unmöglich, die spezifische Abfolge von Aktionen einer Einzelperson nachzuvollziehen.

• Schlussfolgerung: Da das Endprodukt der Datenverarbeitung – die aggregierten Statistiken – keine Informationen enthält, die die Identifizierung einer natürlichen Person ermöglichen, handelt es sich um anonymisierte Daten. Folglich fällt die

the fundamental principle that bchic Analytics does not process personal data.

• Scope of the GDPR: According to Art. 2 Para. 1 GDPR, it applies to the processing of personal data. According to Art. 4 No. 1 GDPR, personal data constitutes any information relating to an identified or identifiable natural person.

• Significance of Anonymization: Recital 26 of the GDPR clarifies: "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person […]."

• Application to bchic analytics: As outlined in Chapter 2.2, every piece of information collected undergoes an immediate and irreversible anonymization process. Furthermore, the anonymized data points are further processed exclusively in aggregated form. This means that individual user journeys or session recordings are neither stored nor displayed in the evaluations. Analyses, such as determining popular page sequences, are always based on a collective, summarized data set. It is technically impossible to trace the specific sequence of actions of an individual person.

• Conclusion: Since the end product of the data processing – the aggregated statistics – contains no information that allows the identification of a natural person, it constitutes anonymized data. Consequently, the processing of this data does not fall within the scope of the GDPR. Since no personal data is processed, no legal basis under Art. 6 Para. 1 GDPR (such

Verarbeitung dieser Daten nicht in den Anwendungsbereich der DSGVO. Da keine personenbezogenen Daten verarbeitet werden, ist keine Rechtsgrundlage aus Art. 6 Abs. 1 DSGVO (wie z.B. die Einwilligung) für den Betrieb der Analyse erforderlich.

3.3 Rechtliche Bewertung gemäß TDDDG

Die Konformität mit dem TDDDG basiert darauf, dass bchic Analytics nicht in den Schutzbereich des Gesetzes fällt.

• Anwendungsbereich des § 25 TDDDG: § 25 Abs. 1 TDDDG regelt die Einwilligungspflicht für „die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind“. Diese Regelung zielt primär auf den Einsatz von Cookies, Local Storage und ähnlichen Technologien ab.

• Funktionsweise von bchic Analytics: Das von bchic Analytics verwendete JavaScript-Skript führt keine der in § 25 TDDDG genannten Handlungen aus. 1. Es werden keine Informationen (wie Cookies oder Tracking-IDs) auf dem Endgerät des Nutzers (z.B. Computer, Smartphone) gespeichert. 2. Es wird nicht auf bereits im Endgerät gespeicherte Informationen zugegriffen.

• Schlussfolgerung: Da die tatbestandlichen Voraussetzungen des § 25 TDDDG nicht erfüllt sind, findet die Vorschrift keine Anwendung. Eine Einwilligung des Nutzers ist aus diesem Grund nicht erforderlich. Die Ausnahme für technisch unbedingt erforderliche Dienste (§ 25 Abs. 2 TDDDG) muss nicht in Anspruch genommen werden, da der Anwendungsbereich des Gesetzes bereits von vornherein nicht eröffnet ist.

as consent) is required for the operation of the analysis.

3.3 Legal Assessment according to TDDDG

Conformity with the TDDDG (Telecommunications-Telemedia Data Protection Act) is based on the fact that bchic Analytics does not fall within the protective scope of the Act.

• Scope of § 25 TDDDG: § 25 Para. 1 TDDDG regulates the obligation to obtain consent for "the storage of information in the end-user's terminal equipment or access to information already stored in the terminal equipment". This regulation primarily targets the use of cookies, Local Storage, and similar technologies.

• Functionality of bchic Analytics: The JavaScript script used by bchic Analytics does not perform any of the actions mentioned in § 25 TDDDG. 1. No information (such as cookies or tracking IDs) is stored on the user's end device (e.g., computer, smartphone). 2. No access is made to information already stored in the end device.

• Conclusion: Since the factual requirements of § 25 TDDDG are not met, the provision does not apply. For this reason, user consent is not required. The exception for strictly necessary services (§ 25 Para. 2 TDDDG) does not need to be invoked, as the scope of the Act is not opened from the outset.

Gesamtfazit der rechtlichen Bewertung:

Der Betrieb von bchic Analytics erfordert keine Nutzereinwilligung, da durch die technische Konzeption weder personenbezogene Daten im Sinne der DSGVO verarbeitet werden, noch ein zustimmungspflichtiger Zugriff auf die Endeinrichtung des Nutzers im Sinne des TDDDG stattfindet.

Overall Conclusion of the Legal Assessment:

The operation of bchic Analytics does not require user consent, as the technical design ensures that neither personal data within the meaning of the GDPR is processed, nor does access to the user's terminal equipment requiring consent take place within the meaning of the TDDDG.

4 Systemvergleich: bchic Analytics vs. Cookie-Analysetools

4. System Comparison: bchic Analytics vs. Cookie-Based Tools

Datenerfassung & Endgerätezugriff (bchic Analytics): Server-Side Tracking ohne Endgerätezugriff. Ein leichtes Skript sendet einen Request an den Server. Es werden keine Informationen (Cookies, IDs) auf dem Endgerät des Nutzers gespeichert oder ausgelesen.	Data Collection & End Device Access (bchic Analytics): Server-side tracking without end device access. A lightweight script sends a request to the server. No information (cookies, IDs) is stored on or read from the user's end device.
Datenerfassung & Endgerätezugriff (Cookie-basierte Tools): Client-Side Tracking mit Endgerätezugriff. Es werden Informationen (typischerweise persistente Cookies mit einer eindeutigen Client-ID) auf dem Endgerät des Nutzers gespeichert und bei jedem Besuch ausgelesen.	Data Collection & End Device Access (Cookie-based Tools): Client-side tracking with end device access. Information (typically persistent cookies with a unique Client-ID) is stored on the user's end device and read on every visit.
Personenbezug der Daten (bchic Analytics): Anonyme, aggregierte Daten. Eingehende Rohdaten (IP, User-Agent) werden unmittelbar und unumkehrbar anonymisiert (Hashing, Salting, Rotation) und danach verworfen. Es werden keine individuellen Nutzerprofile oder User	Personal Reference of Data (bchic Analytics): Anonymous, aggregated data. Incoming raw data (IP, User-Agent) is immediately and irreversibly anonymized (hashing, salting, rotation) and then discarded. No individual user profiles or user journeys are stored, only aggregated statistics.

Journeys gespeichert, nur aggregierte Statistiken.	
Personenbezug der Daten (Cookie-basierte Tools): Personenbezogene (pseudonyme) Daten. Die im Cookie gespeicherte Client-ID ist ein pseudonymes Datum nach DSGVO, da sie die Wiedererkennung eines Nutzers ermöglicht. Es werden detaillierte, individuelle Nutzerprofile und Verhaltensprotokolle erstellt. Die IP-Adresse wird verarbeitet.	Personal Reference of Data (Cookie-based Tools): Personal (pseudonymous) data. The Client-ID stored in the cookie is a pseudonymous date under the GDPR as it enables the re-identification of a user. Detailed, individual user profiles and behavioral logs are created. The IP address is processed.
Einwilligungserfordernis (bchic Analytics): Keine Einwilligung erforderlich. Da weder ein Zugriff auf das Endgerät stattfindet (§ 25 TDDDG) noch personenbezogene Daten verarbeitet werden (DSGVO), ist keine Nutzereinwilligung notwendig.	Consent Requirement (bchic Analytics): No consent required. Since neither access to the end device takes place (§ 25 TDDDG) nor personal data is processed (GDPR), no user consent is necessary.
Einwilligungserfordernis (Cookie-basierte Tools): Doppelte Einwilligung zwingend erforderlich. Die Einwilligung wird sowohl für den Cookie-Zugriff (§ 25 TDDDG) als auch für die Verarbeitung der personenbezogenen Daten (Art. 6 DSGVO) benötigt. Dies bedingt den Einsatz eines Consent-Banners.	Consent Requirement (Cookie-based Tools): Double consent mandatory. Consent is required both for cookie access (§ 25 TDDDG) and for the processing of personal data (Art. 6 GDPR). This necessitates the use of a consent banner.
Datenhoheit & Speicherort (bchic Analytics): Vollständige Datenhoheit in der EU. Die gesamte Datenverarbeitung und -speicherung findet ausschließlich auf Servern bei einem deutschen Provider (Hetzner) mit Standorten in der EU (DE, FI) statt. Es erfolgt kein Datentransfer in Drittstaaten.	Data Sovereignty & Storage Location (bchic Analytics): Complete data sovereignty in the EU. The entire data processing and storage takes place exclusively on servers with a German provider (Hetzner) with locations in the EU (DE, FI). There is no data transfer to third countries.

Datenhoheit & Speicherort (Cookie-basierte Tools): Oftmals Datentransfer in Drittstaaten (USA). Viele Anbieter sind US-Unternehmen. Die Daten werden auf US-Servern verarbeitet und gespeichert, was nach dem Schrems-II-Urteil des EuGH ein erhebliches rechtliches Risiko für europäische Unternehmen darstellt.	Data Sovereignty & Storage Location (Cookie-based Tools): Often data transfer to third countries (USA). Many providers are US companies. The data is processed and stored on US servers, which poses a significant legal risk for European companies following the ECJ's Schrems II ruling.