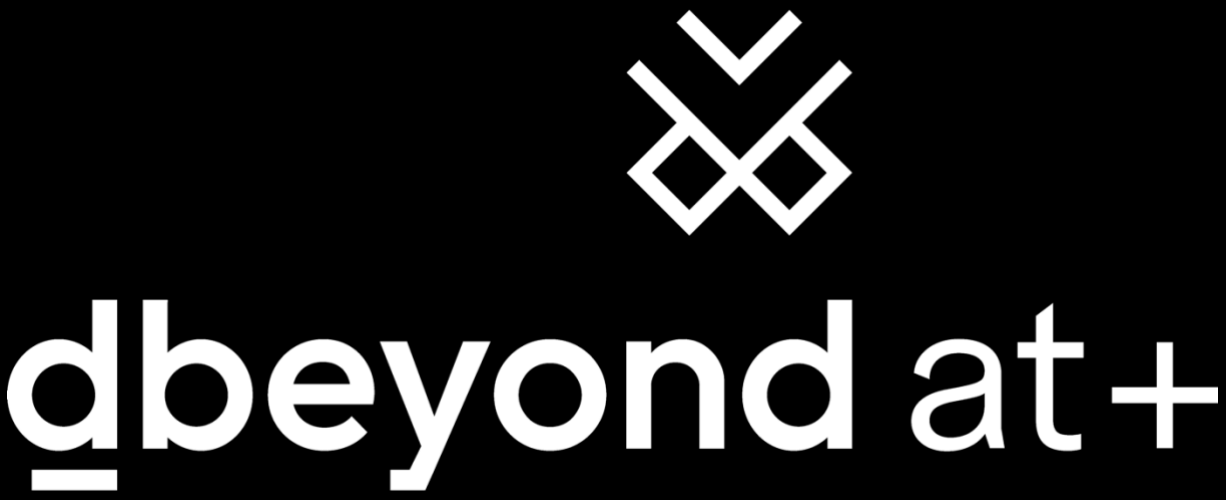

Leitlinie

Datenschutz

1 | Inhaltsverzeichnis

1 | INHALTSVERZEICHNIS 2
2 | DATENSCHUTZZIELE 3
3 | GELTUNGSBEREICH / GELTUNGSDAUER UND ÄNDERUNG DER DATENSCHUTZLEITLINIE 3
4 | GESETZLICHE ANFORDERUNGEN 4
5 | BEGRIFFSBESTIMMUNGEN 4
6 | VERANTWORTLICHKEITEN 5
7 | GRUNDSÄTZE FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN (ART. 5 DS-GVO) 5
8 | SICHERSTELLUNG DER BETROFFENENRECHTE 6
9 | RECHTMÄßIGKEIT DER VERARBEITUNG 7
10 | ÜBERMITTLUNG PERSONENBEZOGENER DATEN 8
11 | AUFTRAGSVERARBEITUNG 8
12 | VERTRAULICHKEIT DER VERARBEITUNG 8
13 | DATENSCHUTZMAßNAHMEN 9
14 | VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN 10
15 | DATENSCHUTZ-FOLGENABSCHÄTZUNG 10
16 | UMGANG MIT DATENSCHUTZVORFÄLLEN 10
17 | DATENSCHUTZKONTROLLE 10

2 | Datenschutzziele

Die dbeyond at+ GmbH verpflichtet sich zur Einhaltung der national und international geltenden Datenschutzrechte. Die Wahrung des Datenschutzes stellt eine wichtige Basis für vertrauensvolle Geschäftsbeziehungen und für die Zusammenarbeit innerhalb der Organisation dar.

Die Datenschutzleitlinie und das Datenschutz-Management-System gewährleisten das in den Gesetzen vorgegebene, angemessene Datenschutzniveau und schaffen entscheidende Rahmenbedingungen für die Erhebung, Verarbeitung, Nutzung und Weitergabe von personenbezogenen Daten. Die vorliegende Datenschutzleitlinie dient als Leitfaden für alle Mitarbeitenden und externen Partner, um einen hohen Standard im Datenschutz zu gewährleisten.

3 | Geltungsbereich / Geltungsdauer und Änderung der Datenschutzleitlinie

Die Datenschutzleitlinie ist zentraler Bestandteil des Datenschutz-Management Systems der dbeyond at+ GmbH und beschreibt die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten und den Einsatz datenverarbeitender Systeme. Die Einhaltung dieser Leitlinie ist verpflichtend für alle Mitarbeitenden der Organisation sowie für Externe, die als Dienstleistende oder Nutzende von datenverarbeitenden Systemen mitwirken. Die Leitlinie untersteht einer regelmäßigen Überprüfung und wird bei Bedarf an rechtliche oder organisatorische Änderungen angepasst. Sie gilt, bis sie außer Kraft gesetzt wird oder durch eine aktualisierte Fassung ersetzt wird.

4 | Gesetzliche Anforderungen

Die Verarbeitung personenbezogener Daten ist verbindlich in der EU-Datenschutz-Grundverordnung (DSGVO), dem Bundesdatenschutzgesetz (BDSG) sowie weiteren nationalen Vorschriften geregelt. Diese gesetzlichen Regelungen haben Vorrang, sofern die Einhaltung dieser Leitlinie zu einem Verstoß gegen sie führen würde.

5 | Begriffsbestimmungen

5.1 Personenbezogene Daten

Personenbezogene Daten werden gemäß Art. 4 Nr. 1 DS-GVO als sämtliche Informationen definiert, die sich auf eine identifizierte oder identifizierbare natürliche Person (die sogenannte „betroffene Person") beziehen. Eine natürliche Person gilt dabei als identifizierbar, wenn sie direkt oder indirekt identifiziert werden kann, insbesondere durch die Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer Online-Kennung oder durch ein oder mehrere spezifische Merkmale. Diese Merkmale können Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität der betreffenden Person sein.

Besondere Kategorien personenbezogener Daten umfassen gemäß Art. 9 Abs. 1 DS-GVO Informationen, die Rückschlüsse auf die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie die Gewerkschaftszugehörigkeit zulassen. Ebenfalls dazu zählen genetische und biometrische Daten zur eindeutigen Identifizierung einer Person, Gesundheitsdaten sowie Angaben zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

5.2 Verarbeitung

Gemäß Art. 4 Nr. 2 DS-GVO umfasst der Begriff der Verarbeitung sämtliche analogen oder digitalen Vorgänge, die im Zusammenhang mit personenbezogenen Daten stehen. Dazu zählen unter anderem das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen und Verwenden von Daten. Ebenso gehört die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung dazu, ebenso wie der Abgleich oder die Verknüpfung, die Einschränkung sowie das Löschen oder die Vernichtung personenbezogener Daten.

6 | Verantwortlichkeiten

Die Geschäftsführung ist verantwortlich für die Datenverarbeitung und damit für die Einhaltung dieser Leitlinie und für die Einhaltung der Datenschutzgesetze.
Für wirksame Maßnahmen zur Einhaltung bzw. für Konsequenzen bei Zuwiderhandlung ist die Geschäftsführung verantwortlich.

Die Führungskräfte haben die Aufgabe, organisatorische, personelle und technische Maßnahmen einer ordnungsgemäßen Datenverarbeitung sicherzustellen.

7 | Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO)

7.1 Rechtmäßigkeit

Personenbezogene Daten werden in Übereinstimmung mit den Grundsätzen von Rechtmäßigkeit und Treu und Glauben verarbeitet. Eine Verarbeitung erfolgt ausschließlich dann, wenn sie durch gesetzliche Bestimmungen der DS-GVO, des BDSG oder anderer vorrangiger Rechtsvorschriften vorgeschrieben oder ausdrücklich erlaubt ist, oder wenn eine Einwilligung der betroffenen Person vorliegt.

7.2 Zweckbindung

Personenbezogene Daten werden ausschließlich für rechtmäßige und zuvor klar definierte Zwecke verarbeitet. Sollten die Verarbeitungszwecke nachträglich geändert werden, ist eine erneute Überprüfung der bestehenden Rechtsgrundlage erforderlich.

7.3 Transparenz

Betroffene Personen werden entsprechend den gesetzlichen Vorgaben über die jeweilige Datenverarbeitung informiert. Diese Information wird präzise, transparent, verständlich und leicht zugänglich bereitgestellt und erfolgt in einer klaren und einfachen Sprache.

7.4 Datenvermeidung und Datensparsamkeit

Die Verarbeitung personenbezogener Daten wird so gestaltet, dass sie sowohl in quantitativer als auch in qualitativer Hinsicht auf das notwendige Maß zur Erreichung des jeweiligen Zwecks beschränkt ist. Soweit der Zweck es erlaubt und der Aufwand im Verhältnis zum angestrebten Ziel angemessen ist, werden anonymisierte Daten verwendet.

7.5 Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten werden sachlich korrekt, vollständig und – sofern erforderlich – stets aktuell verarbeitet. Durch geeignete Maßnahmen wird gewährleistet, dass fehlerhafte, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

7.6 Speicherbegrenzung und Löschung

Personenbezogene Daten werden grundsätzlich nur so lange verarbeitet, wie es zur Erreichung der jeweiligen Zwecke erforderlich ist, sofern keine anderweitigen gesetzlichen, vertraglichen oder satzungsgemäßen Aufbewahrungspflichten bestehen.

7.7 Integrität und Vertraulichkeit

Personenbezogene Daten werden durch geeignete technische und organisatorische Maßnahmen geschützt, um unberechtigten Zugriff, unrechtmäßige Verarbeitung, Offenlegung sowie versehentlichen Verlust, Veränderung oder Zerstörung zu verhindern. Diese Schutzmaßnahmen orientieren sich am Stand der Technik, berücksichtigen die Risiken der Verarbeitung und den spezifischen Schutzbedarf. Die Anforderungen an diese Maßnahmen sind integraler Bestandteil des Informationssicherheits-managementsystems der dbeyond at+ GmbH.

8 | Sicherstellung der Betroffenenrechte

Im Rahmen der gesetzlichen Bestimmungen stehen allen betroffenen Personen gegenüber der dbeyond at+ GmbH die nachfolgenden Rechte zu:

- Recht auf Auskunft (Art. 15 DS-GVO)
- Recht auf Berichtigung (Art. 16 DS-GVO)
- Recht auf Löschen (Art. 17 DS-GVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)

- Recht auf Datenübertragbarkeit (Art. 19 DS-GVO)
- Recht auf Widerspruch (Art. 21 DS-GVO)
- Recht, nicht einer automatisierten Einzelentscheidung unterworfen zu sein (Art. 22 DS-GVO)
- Recht auf Widerruf der Einwilligung (Art. 7 Abs 2 DS-GVO)

Den Betroffenen steht das Recht zu, sich an eine Aufsichtsbehörde für Datenschutz wenden zu können. Die für die dbeyond at+ GmbH grundsätzlich zuständige Behörde ist der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Postfach 102932, 70025 Stuttgart.

9 | Rechtmäßigkeit der Verarbeitung

Wir verarbeiten personenbezogenen Daten nur, wenn die Rechtmäßigkeit der Verarbeitung nach Art. 6 DSGVO sichergestellt ist. Die Rechtmäßigkeit der Verarbeitung wird geprüft und in den Verzeichnissen der Verarbeitungstätigkeiten dokumentiert. Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

10 | Übermittlung personenbezogener Daten

Auch für die Übermittlung personenbezogener Daten muss ein Erlaubnistatbestand vorliegen. Der Empfänger muss außerdem zur Zweckbindung der Datenverarbeitung verpflichtet sein. Drittstaatempfänger müssen ein gleichwertiges Datenschutzniveau gewährleisten.

11 | Auftragsverarbeitung

Bei einer Auftragsverarbeitung behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung. Der Auftragnehmer unterliegt den Weisungen des Auftraggebers.

Vorgaben zur Erteilung eines Auftrags zur Datenverarbeitung:

- Der Auftragnehmer ist geeignet, um die erforderlichen technischen und organisatorischen Schutzmaßnahmen zu gewährleisten.
- Die Erteilung des Auftrags erfolgt in Textform, alle Weisungen und Verantwortlichkeiten werden dokumentiert.
- Die vorgegebenen Vertragsstandards werden eingehalten.
- Der Auftraggeber überzeugt sich vor Beginn und bei Bedarf während der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers.
- Erfolg die Datenverarbeitung grenzüberschreitend, sind die jeweiligen nationalen Anforderungen zu erfüllen und es muss ein gleichwertiges Datenschutzniveau nachgewiesen werden.
- Zusätzlich werden mit den Dienstleistern Verträge abgeschlossen, die sicherstellen, dass die Datenschutzvorgaben eingehalten werden

12 | Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen der Vertraulichkeit. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist allen Mitarbeitern untersagt. Sie dürfen nur Zugang zu Daten haben, wenn dies für ihre jeweiligen Aufgaben notwendig ist und diese nicht für private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder ihnen zugänglich machen. Auch nach Beendigung des Beschäftigungsverhältnisses bleibt diese Verpflichtung bestehen.

13 | Datenschutzmaßnahmen

13.1 Technische und organisatorische Maßnahmen

Die dbeyond at+ GmbH setzt geeignete technische und organisatorische Maßnahmen um, die sich am Schutzbedarf der personenbezogenen Daten orientieren. Dabei werden Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigt. Ziel ist es, ein dem Risiko angemessenes Schutzniveau sicherzustellen und die Verarbeitung im Einklang mit den gesetzlichen Vorgaben durchzuführen. Diese Maßnahmen werden regelmäßig überprüft und bei Bedarf aktualisiert. Insbesondere werden personenbezogene Daten vor unbefugtem Zugriff, unrechtmäßiger Verarbeitung, versehentlichem Verlust, Veränderung oder Zerstörung geschützt.

13.2 Privacy by Design / Privacy by Default

Im Rahmen von Risikobewertungen werden IT-Systeme und Anwendungen so gestaltet, dass sie den Vorgaben des Art. 25 DSGVO entsprechen. Dabei finden sowohl die Prinzipien des Datenschutzes durch Technikgestaltung (Privacy by Design) als auch datenschutzfreundliche Voreinstellungen (Privacy by Default) Berücksichtigung.

13.3 Verpflichtung auf Vertraulichkeit

Sämtliche Beschäftigte sowie externe Personen, die im Rahmen ihrer Tätigkeit mit personenbezogenen Daten der dbeyond at+ GmbH in Berührung kommen, werden zur Wahrung der Vertraulichkeit und zur Einhaltung aller externen sowie internen Vorgaben verpflichtet.

13.4 Schulungen

Die dbeyond at+ GmbH hat ein Schulungskonzept etabliert, das verpflichtende Grundschulungen für sämtliche Beschäftigte sowie fachspezifische Weiterbildungen umfasst.

14 | Verzeichnis von Verarbeitungstätigkeiten

Die dbeyond at+ GmbH unterhält ein zentrales Verzeichnis der Verarbeitungstätigkeiten, in dem alle Prozesse, bei denen personenbezogene Daten verarbeitet werden, gemäß den Anforderungen des Art. 30 DSGVO dokumentiert sind.

15 | Datenschutz-Folgenabschätzung

Wenn eine Verarbeitung, insbesondere durch den Einsatz neuer Technologien, voraussichtlich ein hohes Risiko für die Betroffenen mit sich bringt, wird gemäß Art. 35 DSGVO eine Datenschutz-Folgenabschätzung durchgeführt.

16 | Umgang mit Datenschutzvorfällen

Die Überprüfung von Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 und 34 DSGVO erfolgt auf Basis eines festgelegten Verfahrens. Wenn erforderlich, werden diese an die zuständige Datenschutzbehörde gemeldet.

17 | Datenschutzkontrolle

Durch regelmäßige Datenschutzkontrollen und -audits werden die Einhaltung aller Richtlinien zum Datenschutz sowie die Aktualität der technischen und organisatorischen Maßnahmen und Verfahren überprüft.