

tetratteam unterliegt den europäischen und nationalen Datenschutzrechten und verpflichtet sich zu deren Einhaltung – insbesondere der Datenschutz-Grundverordnung.

Diese Verpflichtung ist umfassend. Weder verarbeiten wir bzw. unser Mitarbeiter*innen personenbezogene Daten ohne ausdrückliche Befugnis noch machen wir anderen Personen oder Stellen die von uns verarbeiteten personenbezogenen Daten unbefugt zugänglich.

Unter einer Verarbeitung versteht die Datenschutz-Grundverordnung (DSGVO) jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten, insbesondere

- das Erheben und das Erfassen
- die Speicherung
- die Anpassung oder Veränderung
- das Auslesen oder das Abfragen
- die Offenlegung, Übermittlung oder Bereitstellung
- das Löschen oder die Vernichtung.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder beispielsweise durch Namen, Adresse oder sonstige Kennung identifizierbare natürliche Person beziehen. Die Verwendung anonymisierter Daten beispielsweise für statistische Auswertungen unterliegt nicht der Datenschutzrichtlinie.

Prinzipien der Datenverarbeitung

1. Rechtmäßigkeit

Personenbezogene Daten werden gesetztes- und regelkonform erhoben und verarbeitet.

2. Zweckbindung

Der jeweilige Zweck für den die personenbezogenen Daten erhoben und verarbeitet werden, wird zuvor definiert

3. Transparenz

Betroffene werden über die Verwendung Ihrer Daten in Kenntnis gesetzt. Im Rahmen der Erhebung werden die Betroffenen über nachfolgende Punkte in Kenntnis gesetzt

- den Zweck der Datenverarbeitung
- die Verantwortliche Stelle
- Ggf. Dritte an die, die Daten weitergegeben werden könnten. Dabei kann auch eine Gruppe von Empfängern definiert werden, wenn es der Übersichtlichkeit und Transparenz der Informationsverpflichtung dient.

4. Datensparsamkeit und Datenvermeidung

Bereits vor der Verarbeitung personenbezogener Daten ist die Notwendigkeit der Erhebung bzw. der Erhebungsumfang zur Zweckerreichung zu prüfen. Wenn es zur Zweckerreichung ausreichend ist, werden anonymisierte bzw. statistische Daten genutzt.

Personenbezogene Daten werden nicht auf Vorrat für mögliche zukünftige Zwecke gespeichert, es sei denn, dies ist durch das nationale Recht vorgeschrieben.

5. Löschung

Nach dem Ablauf der geschäftsbedingten bzw. gesetzlichen Aufbewahrungsfristen, werden personenbezogene Daten, die nicht mehr erforderlich sind, gelöscht.

6. Sachliche Richtigkeit und Datenaktualität

Die erhobenen personenbezogenen Daten sind korrekt, und soweit erforderlich und möglich auch auf dem neuesten Stand zu speichern bzw. zu aktualisieren.

7. Datensicherheit und Datenvertraulichkeit

Personenbezogene Daten werden in der persönlichen Interaktion vertraulich behandelt. Um die widerrechtliche Verarbeitung oder Weitergabe zu verhindern bzw. dem Verlust, der Veränderung oder der Zerstörung entgegen zu wirken, werden angemessene, organisatorische und technische Maßnahmen ergriffen. Diese Maßnahmen werden veröffentlicht.

Zulässigkeit der Datenverarbeitung

1. Daten von Interessent*innen / Mandant*innen

Die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn einer der folgenden Sachverhalte zutrifft:

- Der/die Betroffene hat Daten selbstständig (beispielsweise über das Kontaktformular, telefonisch oder via E-Mail) im Rahmen einer Interessenbekundung übermittelt. Das Interesse kann sich beispielsweise auf den Bezug von einmaligen oder regelmäßigen Informationen (z.B. Newsletter) oder auf eine Beratung und/oder Vermittlung von Versicherungs-, Anlage- oder Finanzierungsinstrumenten beziehen
- Der/die Betroffene hat im Rahmen eines Maklervertrags oder einer Werbemaßnahme (z.B. Messe) explizit Interesse an einmaligen oder regelmäßigen Informationen bestätigt.
- Die Verarbeitung ist notwendig, um auf das jeweilige Beratungs- und/oder Vermittlungsinteresse bezogene Angebote zu erstellen oder einzuholen
- Die Verarbeitung ist notwendig um im Rahmen einer Risikoprüfung die gewünschte Deckungsmöglichkeit eines Risikos abschätzen zu können
- Die Verarbeitung ist notwendig, um den erfolgreichen Abschluss eines gewünschten Geschäfts bzw. einer Risikodeckung herbeizuführen
- Die Verarbeitung ist zur Rechnungslegung, aus buchhalterischen Gründen oder zur Forderungsdurchsetzung notwendig
- Die Verarbeitung ist zur Erfüllung von Vertragspflichten, z.B. der laufenden Betreuung notwendig
- Die Verarbeitung ist notwendig, um gesetzlich vorgeschriebenen Erhebungen oder Prüfungen Folge zu leisten (z.B. Geldwäsche, sonstige Prüfungspflichten)

Die Datenverarbeitung ist - außer im Falle der selbstständigen Übermittlung - nur zulässig, wenn eine explizite schriftliche Einwilligung des/der Betroffenen vorliegt.

Hat der/die Betroffene der Verwendung persönlicher Daten zu Informations- und Werbezwecken explizit widersprochen, so ist eine Verwendung für diese Zwecke unzulässig.

2. Datenschutzerklärung

Die Betroffenen werden über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen einer Datenschutzerklärung hingewiesen.

Auf unseren Webseiten und ggfls. Apps werden die Betroffenen ebenfalls im Rahmen von Datenschutz- bzw. „Cookie“-Hinweisen informiert. Dabei sind diese Hinweise leicht erkennbar, unmittelbar erreichbar und dauerhaft verfügbar für die Betroffenen implementiert.

Die Anlage und Auswertung von individuellen Nutzerprofilen erfolgt grundsätzlich nicht. Statistische Auswertungen der Webseitennutzung erfolgen immer anonymisiert.

3. Daten von Mitarbeiter*innen

Die Anbahnung, Begründung, Durchführung oder die Beendigung eines Arbeits-, Anstellungs- oder Dienstverhältnisses kann eine Verarbeitung personenbezogener Daten erforderlich machen oder in unserem berechtigten Interesse sein. Ist dies der Fall, so darf sie erfolgen.

Ein berechtigtes Interesse kann beispielsweise in der Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche, in der Abwehr von Angriffen auf die unternehmenseigene IT-Infrastruktur oder der wirtschaftlichen Bewertung des Unternehmens begründet sein.

Bei begründetem Verdacht auf einen Gesetzes- oder Richtlinienverstoß (z.B. Datenschutzrichtlinie, Betriebsordnung) kann es zu einer zeitlich befristeten Protokollierung der Nutzung des Intranets und Internets, der E-Mail-Adressen, der Telefonanlage(n) und der internen sozialen Netzwerke kommen.

Im Rahmen von Bewerbungen erhaltene Daten werden unter Berücksichtigung beweisrechtlicher Fristen nach einer erteilten Ablehnung gelöscht. Ist der Auswahlprozess ausgegliedert und wird mit Hilfe Dritter durchgeführt, so stellen wir vertraglich sicher, dass mit den Daten datenschutzrechtlich korrekt umgegangen wird.

Eine Datenverarbeitung ist immer dann zulässig, wenn diese aufgrund staatlicher Vorschriften oder kollektivrechtlicher Belange (Tarifvertrag) verlangt, vorausgesetzt oder gestattet und hinsichtlich Art und Umfang der gesetzlich zulässigen Verarbeitung auch erforderlich ist.

Eine Verarbeitung besonders schutzwürdiger Daten darf nur unter ganz bestimmten Voraussetzungen erfolgen. Besonders schutzwürdige Daten sind definiert als Daten über Gesundheit und Sexualleben, politische Meinung, rassische und ethnische Herkunft, über Gewerkschaftszugehörigkeit, über religiöse oder philosophische Überzeugung der Betroffenen.

Insoweit Mitarbeiter*innen auch Interessent*innen oder Mandant*innen gem. Punkt 1. sind, gelten für die entsprechenden Zwecke die dort getroffenen Vorgaben.

Weiterleitung von Daten

Die Übermittlung personenbezogener Daten an unternehmensinterne oder externe Empfänger erfolgt nur unter Beachtung der Zulässigkeit, wie zuvor beschrieben.

Vor einer Übermittlung wird sichergestellt, dass der/die Empfänger*in auf die ausschließliche Verwendung des bereits bei Erhebung festgelegten Zwecks verpflichtet ist, soweit die Betroffenen selbst nicht explizit einer weitergehenden Verwendung zugestimmt haben.

Werden die Daten an Empfänger*innen in einem Drittstaat übermittelt, so überprüfen wir, ob dort mindestens ein mit den rechtlichen Anforderungen der DSGVO vergleichbarer Datenschutz gewährleistet ist.

Erfolgt die Übermittlung aufgrund gesetzlicher Verpflichtungen (z.B. Beibringung in grenzüberschreitenden steuerstrafrechtlichen Ermittlungsverfahren) eines Drittstaates, ist dies auch ohne vorherige Prüfung eines gleichwertigen Datenschutzniveaus möglich.

Rechte der Betroffenen

Betroffene können Auskunft darüber verlangen, welche personenbezogenen Daten über sie gespeichert wurden, woher diese Daten stammen und zu welchem Zweck sie gespeichert werden.

Die spezielleren Auskunftsrechte im Arbeitsrecht (z.B. das Einsichtsrecht in die Personalakte) bestehen davon unabhängig und darüberhinausgehend fort.

Kommt es zur Übermittlung von Daten an Dritte, so ist über die Identität des/der Empfänger*in bzw. die Kategorien von Empfänger*innen Auskunft zu erteilen.

Den Betroffenen steht ein Recht auf Berichtigung bzw. Ergänzung ihrer personenbezogenen Daten zu, wenn diese unvollständig oder unrichtig gespeichert sind.

Die Weitergabe von Daten an Dritte zu Werbezwecken findet grundsätzlich nicht statt.

Darüber hinaus sind Betroffene berechtigt, die Löschung der gespeicherten personenbezogenen Daten zu verlangen, soweit dem keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Insbesondere sind die Daten dann zu löschen, wenn es an einer Rechtsgrundlage für die Verarbeitung fehlt bzw. diese weggefallen ist oder aber der Zweck der Verarbeitung (z.B. durch Zeitablauf) entfallen ist.

Betroffene haben ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung ihrer Daten, soweit ihr schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation im jeweiligen Einzelfall den Interessen an einer Verarbeitung durch uns vorgeht.

Besteht jedoch eine Rechtspflicht zur Durchführung der Datenverarbeitung so können wir auch bei Vorliegen einer besonderen persönlichen Situation nicht zum Verzicht auf Verarbeitung oder zum Löschen verpflichtet werden.

Technisch-organisatorische Maßnahmen

Um personenbezogene Daten zu jeder Zeit vor dem unberechtigten Zugriff, der unrechtmäßigen Verarbeitung bzw. deren Weitergabe sowie gegen Verfälschung und Verlust oder gar Zerstörung zu schützen ergreifen wir umfassende technisch-organisatorische Maßnahmen, die wir veröffentlichen, um entsprechende Transparenz herzustellen.

Dies beinhaltet beispielsweise auch die Erstellung von digitalen Sicherheitskopien (sogenannte backups), welche eine Wiederherstellung verlorengangener Daten ermöglichen. Dazu werden in der Regel externe Datenspeicher genutzt, in denen die Daten verschlüsselt sind.

Bereits vor der Einführung neuer Datenverarbeitungsverfahren, namentlich neuer IT-Systeme im Rahmen technischer Umstellungen in unserem Unternehmen legen wir technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten fest und implementieren sie in Kooperation mit qualifizierten IT-Expert*innen.

Dabei orientieren wir uns an folgenden Parametern:

- dem jeweiligen Stand der Technik
- dem von der Verarbeitung ausgehenden Risiko
- dem jeweiligen Schutzbedarf der Daten.

Überprüfung & Evaluierung

Die bereits erwähnten und an anderer Stelle ausführlich beschriebenen technisch-organisatorischen Maßnahmen sind Teil eines Datenschutzsicherheitsmanagements und unterliegen der ständigen Anpassung an technische und organisatorische Entwicklungen.

Wir überprüfen und evaluieren diese Maßnahmen laufend in Kooperation mit qualifizierten IT-Expert*innen. Auf Verlangen der zuständigen Datenschutzaufsichtsbehörde:

Berliner Beauftragte*r für den Datenschutz
An der Urania 4-10, 10787 Berlin
mailbox@datenschutz-berlin.de

stellen wir sämtliche diesbezügliche Dokumente zur Verfügung. Unabhängig davon obliegt es der zuständigen Aufsichtsbehörde im gesetzlichen Rahmen eigene Überprüfungen der Einhaltung dieser Datenschutzrichtlinie vorzunehmen.

Auftragsdatenverarbeitung

Soweit wir Aufträge zur Datenverarbeitung (ADV) an Dritte (Auftragnehmer) vergeben, so werden wir an diese folgende Anforderungen stellen:

- Die Auftragnehmer haben die für den Datenschutz gesetzlich gebotenen technischen und organisatorischen Schutzmaßnahmen sicherzustellen.
- Die Verpflichtung zu den entsprechenden Maßnahmen werden im Rahmen der Auftrags dokumentiert
- Gegebenenfalls sind auch durch uns darüber hinaus gestellte Schutzanforderungen einzuhalten.
- Vor Beginn der Auftragsdatenverarbeitung durch die Auftragnehmer, müssen diese die Einhaltung der gesetzlichen Schutzanforderungen durch eine Zertifizierung nachweisen.

Werden Auftragsdaten grenzüberschreitend verarbeitet, sind die nationalen Vorschriften zur Weitergabe personenbezogener Daten ins Ausland einzuhalten. Beispielsweise dürfen Transferierungen (z.B. Serverdienste) von persönlichen Daten aus der EU in einen Drittstaat nur bei Sicherstellung des Datenschutzniveaus der EU im jeweiligen Drittstaat des Auftragnehmers stattfinden.

Datenschutzvorfälle

Sollte es trotz der umfassenden Schutzmaßnahmen zu einem sogenannten Datenschutzvorfall kommen sind alle unsere Berater*innen bzw. Mitarbeiter*innen verpflichtet, wahrgenommene Datenschutzverstöße bzw. Verstöße gegen die Datenschutzrichtlinie unverzüglich zu melden, damit wir unsererseits unserer Meldepflicht bei der Datenschutzaufsichtsbehörde nachkommen können.

Das betrifft insbesondere folgende Fälle:

- die unrechtmäßige Übermittlung personenbezogener Daten an Dritte,
- der unrechtmäßige Zugriff durch einen Dritten auf personenbezogene Daten
- der umfassende Verlust personenbezogener Daten

Verantwortlichkeiten & Sanktionen

Die Geschäftsführung unseres Unternehmens ist auch für die ordnungsgemäße Datenverarbeitung verantwortlich. Aus ihrer Stellung heraus erwächst die Verpflichtung zur Sicherstellung der gesetzlichen und derjenigen Vorgaben, die in dieser Datenschutzrichtlinie genannt sind.

Die konkrete Umsetzung der genannten Grundsätze obliegt allerdings allen Berater*innen und Mitarbeiter*innen des Unternehmens. Diese haben die Geschäftsführung auch bei einer Kontrolle der Aufsichtsbehörde umgehend darüber in Kenntnis zu setzen.

Die Geschäftsführung ist dazu verpflichtet, die Aufsichtsbehörde, ggfls. auch - soweit entsprechend gesetzlicher Vorgaben benannt - den/die Datenschutzbeauftragte/n* in seiner/ihrer Tätigkeit vollumfänglich zu unterstützen und in den Optimierungsprozessen zu fördern.

Die Geschäftsführung hat sicherzustellen, dass sämtliche Mitarbeiter*innen zum Thema Datenschutz geschult sind und auch auf dem aktuellen Stand bleiben.

Missbrauch bei der Datenverarbeitung kann unter Umständen auch strafrechtliche Konsequenzen haben. Die Geschäftsführung wird sich in solchen Fällen für eine reibungslose Kommunikation und Zusammenarbeit mit den Strafjustizbehörden einsetzen.

Datenmissbrauch durch eigene Berater*innen oder Mitarbeiter*innen wird nicht toleriert und - soweit nachweisbar - mit arbeits- bzw. gesellschaftsrechtlichen Konsequenzen beantwortet.

Begriffserklärungen

Personenbezogene Daten

Personenbezogene Daten sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Bestimmbar ist eine Person z.B. dann, wenn der Personenbezug durch eine Verknüpfung von Informationen mit möglicherweise vorhandenem Zusatzwissen hergestellt werden kann.

Anonymisierung

Anonymisiert sind Daten dann, wenn ein Personenbezug dauerhaft und von niemandem mehr hergestellt werden kann bzw. wenn der Personenbezug nur mit einem unverhältnismäßig hohen Aufwand an Arbeitskraft, Zeit und Kosten wiederhergestellt werden könnte.

Besonders schutzwürdige Daten

Besonders schutzwürdige Daten sind Daten über die rassistische und ethnische Herkunft, über politische Meinungen, über religiöse und philosophische Überzeugungen, über eine Gewerkschaftszugehörigkeit oder über die Gesundheit oder die sexuelle Orientierung der Betroffenen. Aufgrund der Rechtsprechung sind diese Datenkategorien als besonders schutzwürdig eingestuft.

Betroffene

Betroffene im Sinne dieser Datenschutzrichtlinie sind alle natürlichen Personen, über die Daten verarbeitet werden.

Verantwortliche

Verantwortliche in unserem Unternehmen sind diejenigen, deren Tätigkeit mit einer Datenverarbeitung verbunden ist. Im Zweifelsfall und im Fall von Datenschutzvorfällen ist die Geschäftsführung des Unternehmens verantwortlich.

Datenschutzvorfall

Datenschutzvorfälle sind datenschutzrechtlich relevante Ereignisse, die entweder den Verlust oder die Zerstörung von Daten oder datenschutzrechtliche Verstöße begreifen.

Einwilligung

Einwilligung ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.

Datenschutzbeauftragte/r

Nach den aktuellen gesetzlichen Bestimmungen ist in einem Unternehmen ein/e Datenschutzbeauftragte/r zu benennen, soweit mindestens zehn im Unternehmen beschäftigte Personen mit der Datenverarbeitung betraut sind. Dies ist in unserem Unternehmen nicht der Fall.

Auskunftsersuchen oder Beschwerden können Betroffene direkt an die Geschäftsführung richten:

Oliver Ginsberg, Tel.: 6110188-0, info@tetratteam.de