

KONFORMITÄT

DATENSCHUTZ RICHTLINIE

DATENSCHUTZRICHTLINIE

1. ZWECK UND ANWENDUNGSBEREICH

Egebant ist dem Grundsatz verpflichtet, die Vertraulichkeit aller Interessengruppen zu schützen, mit denen eine Geschäftsbeziehung besteht, einschließlich, aber nicht beschränkt auf Kunden, Lieferanten, Mitarbeiter und Subunternehmer. In Anlehnung an diesen Grundsatz hat das Unternehmen die vorliegende Datenschutzrichtlinie (die „Richtlinie“) verabschiedet.

2. DEFINITIONEN

Geltende Datenschutzgesetze bezeichnet sämtliche in der Türkei (Gesetz zum Schutz personenbezogener Daten) geltenden und im Rahmen der Verarbeitung personenbezogener Daten anwendbaren Gesetze und Vorschriften im Zusammenhang mit Datenschutz oder Datensicherheit.

Personenbezogene Daten bezeichnet sämtliche Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (die „betroffene Person“) beziehen. Eine Identifizierung kann durch Bezugnahme auf ein oder mehrere Merkmale erfolgen, wie einen Namen, eine Identifikationsnummer, Standortdaten, Online-Kennungen oder ein oder mehrere Merkmale, die für die physische, psychische, genetische, geistige, wirtschaftliche, kulturelle oder soziale Identität einer betroffenen Person spezifisch sind.

Mitarbeiter bezeichnet sämtliche fest angestellten Mitarbeiter, leitenden Angestellten, Voll- oder Teilzeitbeschäftigten, relevanten externen Berater sowie Zeitarbeitskräfte, die im Namen der Egebant-Gesellschaften handeln und dieser Richtlinie unterliegen.

Verarbeitung oder Verarbeiten bezeichnet jeden auf personenbezogene Daten angewendeten Vorgang, wie das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen, Verbreiten oder anderweitige Bereitstellen, den internationalen Transfer, die Anpassung oder Kombination, die Einschränkung, das Löschen oder die Vernichtung.

Auftragsverarbeiter bezeichnet jede Person und jede Einheit, die dieser Richtlinie unterliegt und im Namen von Egebant personenbezogene Daten verarbeitet. **Datenschutzverletzung** bezeichnet die unbeabsichtigte oder rechtswidrige Vernichtung, den Verlust, die Veränderung, die unbefugte Offenlegung von oder den unbefugten Zugang zu personenbezogenen Daten.

Sicherheitsmaßnahmen bezeichnet rechtliche, organisatorische oder technische Maßnahmen, die auf die Integrität, Verfügbarkeit und Vertraulichkeit personenbezogener Daten abzielen und Datenschutzverletzungen verhindern, abmildern oder beheben sollen.

Besondere Kategorien personenbezogener Daten bezeichnet personenbezogene Daten einer betroffenen Person über deren Rasse oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Merkmale, biometrische Daten, Gesundheit, Sexualleben, sexuelle Orientierung oder strafrechtliche Verurteilungen.

3. VERANTWORTLICHKEITEN

a. Mitarbeiter sind verpflichtet, diese Richtlinie einzuhalten, wenn sie im Rahmen ihrer gewöhnlichen Geschäftstätigkeiten personenbezogene Daten verarbeiten.

b. Die oberste Leitung des Unternehmens ist dafür verantwortlich, die Einhaltung dieser Richtlinie sicherzustellen, einschließlich der Aufrechterhaltung einer angemessenen Governance-Struktur und der Bereitstellung der für die Einhaltung und Umsetzung erforderlichen Ressourcen.

c. Mitarbeiter müssen unverzüglich über die Ethik-Hotlines Bericht erstatten, wenn sie vermuten oder erfahren, dass diese Richtlinie im Widerspruch zu einer lokalen Gesetzgebung oder Vorschrift steht oder dass eine Praxis des Unternehmens gegen diese Richtlinie verstößt.

d. Das Unternehmen kann zusätzliche Richtlinien, Verfahren oder Praktiken einführen, um die Einhaltung dieser Richtlinie oder der lokalen Datenschutzgesetze sicherzustellen.

3. ALLGEMEINE RICHTLINIE

a. Das Unternehmen ist bestrebt, personenbezogene Daten in Übereinstimmung mit dieser Richtlinie und den geltenden Datenschutzgesetzen zu verarbeiten. Sehen die geltenden Datenschutzgesetze ein höheres Schutzniveau vor als diese Richtlinie, ist das Unternehmen verpflichtet, diese Gesetze und Vorschriften einzuhalten.

DATENSCHUTZRICHTLINIE

b. Grundprinzipien

Rechtmäßigkeit und Zweckbindung Das Unternehmen darf personenbezogene Daten nur rechtmäßig, nach Treu und Glauben und für festgelegte, eindeutige und legitime Geschäftszwecke verarbeiten, gestützt auf eine angemessene Rechtsgrundlage gemäß den geltenden Datenschutzgesetzen. Diese Rechtsgrundlage kann die ausdrückliche Einwilligung der betroffenen Person, die Erfüllung eines Vertrags, vorvertragliche Maßnahmen, gesetzliche Verpflichtungen oder berechnete Interessen des Unternehmens sein, sofern diese die Interessen oder Grundrechte und -freiheiten der betroffenen Personen nicht einschränken. Verlangen geltende Gesetze oder interne Richtlinien vom Unternehmen, vor der Verarbeitung bestimmter personenbezogener Daten die ausdrückliche Einwilligung der betroffenen Person einzuholen, wird das Unternehmen diese Einwilligung einholen und die Entscheidung der betroffenen Person umsetzen. Das Unternehmen muss Aufzeichnungen darüber führen, dass es die Einwilligungen der Person eingeholt hat und dass es einen etwaigen Widerruf der Einwilligung umsetzt.

Datenminimierung Das Unternehmen muss die Verarbeitung personenbezogener Daten auf das für die Erreichung des festgelegten Zwecks oder der festgelegten Zwecke erforderliche Mindestmaß an Informationen beschränken. Soweit möglich, sollte das Unternehmen Daten verwenden, die keine Identifizierung der betroffenen Personen ermöglichen. Der Zugang zu diesen Informationen ist auf das Erforderliche zu beschränken. Das Unternehmen wird den Umfang der Verarbeitung, des Zugriffs auf und der Speicherung von personenbezogenen Daten, die für den festgelegten Zweck oder die festgelegten Zwecke erforderlich sind, auf ein Minimum reduzieren. Der Zugang wird auf das erforderliche Wissen beschränkt. Abgesehen von Ausnahmen dürfen personenbezogene Daten nicht einer unbestimmten Anzahl von Personen zugänglich sein.

Wahrung der Richtigkeit und Qualität Das Unternehmen muss stets die Integrität der Verarbeitungsprozesse personenbezogener Daten wahren und die erforderlichen Schritte unternehmen, damit personenbezogene Daten für ihre zweckgemäße Verwendung richtig, vollständig, aktuell und zuverlässig sind.

Speicherung und Löschung personenbezogener Daten Das Unternehmen darf personenbezogene Daten nicht länger als erforderlich speichern. Personenbezogene Daten müssen in Übereinstimmung mit den geltenden Unternehmensrichtlinien, einschließlich der Aufbewahrungsrichtlinie des Unternehmens, und den Aufbewahrungsplänen vernichtet oder anonymisiert werden. Die Unternehmensrichtlinien und Aufbewahrungsprogramme müssen die geschäftlichen Erfordernisse des Unternehmens, gesetzliche Verpflichtungen sowie wissenschaftliche, statistische oder historische Forschungszwecke berücksichtigen.

c. Rechte der betroffenen Person

Das Unternehmen muss Anträge betroffener Personen in Bezug auf personenbezogene Daten prüfen, etwa hinsichtlich des Auskunftsrechts, von Einschränkungen, der Datenübertragbarkeit, der Löschung, des Widerspruchs oder des Widerrufs der Einwilligung.

Das Unternehmen muss auf solche Anträge innerhalb eines Monats antworten und sich bemühen, den Antrag innerhalb der in der Richtlinie zu den Rechten der betroffenen Person festgelegten Frist zu erfüllen.

Das Unternehmen ist nicht verpflichtet, einem Antrag nachzukommen, solange es die betreffenden personenbezogenen Daten der antragstellenden betroffenen Person nicht rechtmäßig zuordnen kann oder soweit der Antrag aufgrund seines wiederholenden Charakters offenkundig unbegründet oder exzessiv ist.

d. Gewährleistung der erforderlichen Sicherheit und Meldung von Sicherheitsverletzungen

Das Unternehmen muss Sicherheitsmaßnahmen anwenden, um die Sicherheit der Daten zu gewährleisten, insbesondere bei Vorgängen, die die Übertragung personenbezogener Daten über drahtlose Netzwerke, tragbare Geräte oder Datenträger betreffen. Diese Maßnahmen müssen den Verarbeitungsvorgang, die Art der betreffenden personenbezogenen Daten sowie die Kosten und die Durchführbarkeit der Umsetzung der Sicherheitsmaßnahmen berücksichtigen.

Die Sicherheitsmaßnahmen müssen in schriftlichen Sicherheitsrichtlinien und -verfahren festgelegt werden.

Mitarbeiter müssen Sicherheitsverletzungen unverzüglich der IT-Abteilung von Egeant melden und Sicherheitsverletzungen in Übereinstimmung mit der Richtlinie zu Datenschutzverletzungen des Unternehmens dokumentieren.

e. Offenlegung personenbezogener Daten

Das Unternehmen darf personenbezogene Daten nur gegenüber Strafverfolgungsbehörden oder Gerichten, Geschäftspartnern, Lieferanten oder Kunden offenlegen, sofern es hierzu ausdrücklich ermächtigt ist und dies im Einklang mit den in der Türkei geltenden Gesetzen und Vorschriften bzw. den geltenden Datenschutzgesetzen steht.

Das Unternehmen muss die Auftragsverarbeiter, mit denen es zusammenarbeitet, im Hinblick auf die Vertraulichkeit und Sicherheit personenbezogener Daten sorgfältig auswählen, sie vertraglich verbindlichen Kontrollen unterwerfen und sämtliche geltenden Datenschutzgesetze einhalten.

f. Internationale Übermittlung personenbezogener Daten

Das Unternehmen darf personenbezogene Daten nur unter den in den geltenden Datenschutzgesetzen festgelegten Voraussetzungen übermitteln.

g. Schulung

Mitarbeiter, die im Rahmen ihrer Funktion oder ihrer Aufgaben personenbezogene Daten verarbeiten, müssen regelmäßig in Übereinstimmung mit dieser Richtlinie geschult werden. Die Schulung ist an die Funktion oder Aufgabe des jeweiligen Mitarbeiters anzupassen.

h. Überwachung und Aufzeichnungen

Der Global Data Protection Officer und die lokalen Datenschutzbeauftragten müssen regelmäßige Überprüfungen und Audits durchführen, um die Einhaltung dieser Richtlinie sicherzustellen.

Das Unternehmen muss Aufzeichnungen über seine Datenverarbeitungstätigkeiten führen. Diese Aufzeichnungen sind den Aufsichtsbehörden auf Anfrage zur Verfügung zu stellen.

i. Einhaltung und Ausnahmen

Von den durch diese Richtlinie auferlegten Anforderungen kann nur im Einzelfall, in Ausnahmefällen und nach vorheriger Zustimmung der Geschäftsleitung abgewichen werden.

Mitarbeiter, die gegen diese Richtlinie verstoßen, können mit Disziplinarmaßnahmen belegt werden, einschließlich, als letztes Mittel, der Kündigung des Arbeitsverhältnisses.

5. GEISTIGES EIGENTUM UND DESSEN SCHUTZ

Sämtliches geistiges und gewerbliches Eigentum, das dem Unternehmen gehört oder von diesem entwickelt wird, wird als vertrauliche Information behandelt und geschützt. Hierzu zählen unter anderem Patente, Gebrauchsmuster, gewerbliche Muster und Modelle, Marken, Urheberrechte, Software, Algorithmen, technische Zeichnungen, Berichte, Prozesse, Know-how, Geschäftsgeheimnisse sowie sämtliche vergleichbaren immateriellen Vermögenswerte, die das geistige Eigentum des Unternehmens bilden.

Mitarbeiter, Berater und sämtliche im Namen des Unternehmens handelnde Dritte;

- dürfen die dem Unternehmen gehörenden Elemente des geistigen Eigentums nicht unbefugt kopieren, vervielfältigen, weitergeben oder Dritten offenlegen,
- dürfen im Rahmen ihrer Tätigkeit erlangte Informationen mit Bezug zum geistigen Eigentum nur im erforderlichen Umfang und im Rahmen ihrer Befugnisse nutzen,
- sind verpflichtet, im Einklang mit den internen Regelungen des Unternehmens und den geltenden Rechtsvorschriften zu handeln.

l. Rechte der Parteien am geistigen Eigentum

Das Unternehmen macht es sich zum Grundsatz, die Rechte am geistigen und gewerblichen Eigentum von Kunden, Lieferanten, Geschäftspartnern, Beratern und sonstigen Dritten zu respektieren.

In diesem Rahmen;

- dürfen Dritten gehörende Patente, Urheberrechte, Marken, Software, Designs, technische Dokumente, Geschäftsgeheimnisse und vergleichbare Elemente des geistigen Eigentums nur im Rahmen der jeweiligen Rechtsgrundlage, der Vertragsbestimmungen und der erteilten Genehmigungen genutzt werden,
- ist das Kopieren, Vervielfältigen, Verändern, Verbreiten oder Weitergeben von Dritten gehörenden Elementen des geistigen Eigentums ohne Lizenz, Vertrag oder ausdrückliche schriftliche Genehmigung untersagt,
- die unbefugte Offenlegung vertraulicher oder dem geistigen Eigentum zuzurechnender Informationen Dritter

DATENSCHUTZRICHTLINIE

Sämtliche innerhalb des Unternehmens entwickelten Erfindungen, Designs, Software, Dokumente und vergleichbaren Arbeiten gelten gemäß den geltenden Rechtsvorschriften und den internen Regelungen des Unternehmens als Eigentum des Unternehmens und werden, soweit erforderlich, rechtlich geschützt.

Informationen und Unterlagen, die geistiges Eigentum enthalten, gelten im Rahmen dieser Richtlinie als vertrauliche Daten und werden durch angemessene technische und organisatorische Sicherheitsmaßnahmen vor unbefugtem Zugriff, Offenlegung, Verlust oder Missbrauch geschützt.

Bei einem Verstoß gegen die Bestimmungen dieser Richtlinie können gegen die betreffende(n) Person(en) Disziplinarmaßnahmen verhängt werden; erforderlichenfalls können auch rechtliche und strafrechtliche Schritte eingeleitet werden.

6. HINWEISE

Fragen oder Bedenken zu dieser Richtlinie oder zu Datenschutzangelegenheiten im Allgemeinen sind an die IT-Abteilung zu richten.