



**KUNDO** The 'xT' logo consists of a blue circle containing a white 'x' and a teal circle containing a white 'T'.

# Leitlinie Datenschutz und Datensicherheit

- Für die ObergfellTechnologyGroup AG und die KUNDO xT GmbH -



ObergfellTechnologyGroup AG



## Inhalt

Zielsetzung der Datenschutzleitlinie .....	3
Verantwortlichkeiten .....	3
Datenschutzbeauftragter .....	4
Geltungsbereich .....	4
Bedeutung des Datenschutzes .....	5
Datenschutzziele .....	5
Grundsätze .....	6
Vertraulichkeit der Verarbeitung .....	7
Sicherheit der Verarbeitung .....	7
Kontrolle von Datenschutz und Datensicherheit .....	8
Vorfälle im Bereich Datenschutz und Datensicherheit .....	8
Sanktionen .....	8
Inkrafttreten der Datenschutzleitlinie .....	8



ObergfellTechnologyGroup AG



## Zielsetzung der Datenschutzleitlinie

Wir als Unternehmen verpflichten uns zur Einhaltung datenschutzrechtlicher Bestimmungen im Rahmen der Europäischen Datenschutz-Grundverordnung (EU-DSGVO). Die Wahrung datenschutzrechtlicher Vorgaben dient als Fundament jeglicher vertrauensvollen Beziehungen zu Mitarbeitern und Kunden, Lieferanten und Partnern und soll das Thema Datenschutz sowie Datensicherheit in unserem Unternehmen zum Schutz der Betroffenen sowie des Unternehmens stetig weiterentwickeln.

Wir wollen somit gewährleisten, dass alle Beschäftigten im Unternehmen der Zielsetzung der Geschäftsführung folgen und jegliche Form von Daten und Informationen im Unternehmen, ob personenbezogen oder unternehmensrelevant, mit der entsprechenden Sorgfalt und einem ausreichendem Schutz- und Sicherheitsbewusstsein behandeln.

## Verantwortlichkeiten

Grundsätzlich ist für die Einhaltung des Datenschutzes das gesamte Unternehmen und in Vertretung die Geschäftsleitung verantwortlich. Diese ist verpflichtet, Maßnahmen und Schutzmechanismen so zu etablieren, dass das Risiko einer Datenschutzverletzung bei der Verarbeitung von personenbezogenen Daten im Unternehmen minimiert ist.

Daneben ist jeder Mitarbeiter, welcher personenbezogene Daten verarbeitet ebenfalls verantwortlich sensibel mit den Daten umzugehen, Richtlinien und Arbeitsanweisungen umzusetzen und aktiv zum Schutz der personenbezogenen Daten beizutragen.

Bei dem Schutz von personenbezogenen Daten geht es um den Schutz der Grundrechte einer Person. Daher können bei fahrlässigen oder vorsätzlichen Verstößen, welche die Rechte von Personen einschränken, auch arbeitsrechtliche oder strafrechtliche Schritte eingeleitet werden.

Die Gesamtverantwortung obliegt immer der Geschäftsleitung.

Zur Unterstützung dazu ist der gesetzlich notwendige Datenschutzbeauftragte extern bestellt worden.

## Datenschutzbeauftragter

Der Datenschutzbeauftragte unseres Unternehmens implementiert und betreut hierfür ein ganzheitliches Datenschutzmanagement, welches sämtliche Anforderungen der EU-DSGVO abdeckt und somit die Wahrung der Vertraulichkeit aller Daten und Informationen in unserem Unternehmen optimal vorantreibt. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen.

Ansprechpartner für den Datenschutz im Unternehmen ist:

vimopro GmbH  
Warenburgstr. 8  
78050 Villingen-Schwenningen

[datenschutz@kundoxt.com](mailto:datenschutz@kundoxt.com)  
Telefon: +49 7721 69811 51

Verpflichtend ist daher der Datenschutzbeauftragte frühzeitig in alle Fragen einzubinden, welche mit dem Schutz personenbezogener Daten zusammenhängen. Ein Unternehmen ist gesetzlich verpflichtet, Ressourcen und Zugänge zur Erfüllung der Aufgabe bereitzustellen. (Art. 38 DSGVO) Gleichzeitig unterliegen der Datenschutzbeauftragte und seine Erfüllungsgehilfen einer besonderen Verschwiegenheitspflicht über Dinge, die ihnen im Rahmen ihrer Tätigkeit bekannt werden.

Der Datenschutzbeauftragte ist nur verpflichtet der Geschäftsleitung im Unternehmen zu berichten.

Betroffene Personen, egal ob Mitarbeiter, Bewerber oder externe Ansprechpartner, dürfen sich jederzeit mit Fragen zu der Verarbeitung ihrer Daten oder zur Wahrnehmung ihrer Rechte an den Datenschutzbeauftragten wenden.

Zu den Aufgaben des Datenschutzbeauftragten gehören (Art. 39 DSGVO):

- Die Unterrichtung und Beratung des Verantwortlichen und seiner Beschäftigten hinsichtlich ihrer Pflichten nach der DSGVO und dem BDSG
- Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategie des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter und der Überprüfung dessen.
- Beratung – auf Anfrage – im Zusammenhang mit Datenschutz-Folgenabschätzungen und Überwachung ihrer Durchführung
- Zusammenarbeit mit der Aufsichtsbehörde
- Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängender Fragen und der Konsultation dieser nach Art. 36 DSGVO, sowie ggf. Beratung zu allen sonstigen Fragen.

Bei der Beratung und Aufgabenerfüllung muss immer das mit der Verarbeitung verbundene Risiko in Art, Umfang, Umstände und Zweck der Verarbeitung berücksichtigt werden.

## Geltungsbereich

Diese Leitlinie gilt für alle personenbezogenen Daten in unserem Unternehmen und findet in allen Bereichen, in denen datenschutzrelevante Informationen verarbeitet werden Anwendung.

## Bedeutung des Datenschutzes

Insofern wir als Unternehmen innerhalb der EU agieren, sind wir verpflichtet, die DSGVO einzuhalten. Zum Teil können auch die Mitgliedsstaaten der EU die gesetzlichen Regelungen darauf über so genannte „Öffnungsklauseln“ erweitern. In Deutschland ist dies bspw. durch das BDSG gegeben.

Der Datenschutz basiert auf dem Grundrecht einer Person auf informationelle Selbstbestimmung. Wir wahren die Grundrechte aller Menschen und schützen Personen und deren Daten daher so gut wie möglich.

Die Ziele gehen dabei Hand in Hand mit unserer Unternehmensstrategie und den damit verbundenen Risiken. Unsere Tochtergesellschaft KUNDO xT GmbH ist auf die Entwicklung und Produktion von Messwarnsystemen für Gase und Temperaturfühler für die Industrie spezialisiert. Gemäß der wachsenden Nachfrage im Bereich Klimaschutz-Technik liegt unser Hauptaugenmerk auf Kunden aus dem Umweltschutz und der Landwirtschaft. Derzeit bedienen wir Kunden hauptsächlich im europäischen Wirtschaftsraum, planen aber die Erschließung weiterer Märkte in Drittländern außerhalb des EWR.

Gemäß unserer Unternehmensstrategie legen wir dabei besonderen Wert auf den Schutz von Mitarbeiterdaten und der Daten von Ansprechpartnern von Geschäftspartnern. Dabei sind wir auf eine langfristige Bindung der Beschäftigten konzentriert.

Darüber hinaus werden Räumlichkeiten des Gebäudes an externe Parteien vermietet. Da diese auch in verschiedene Sicherheitssysteme eingebunden sind, legen wir auch sehr viel Wert darauf, deren Interessen zu wahren und den Schutz Ihrer Daten sicherzustellen. Gleichzeitig stellt dies auch die Herausforderung dar, Daten getrennt voneinander zu halten.

Grundsätzlich werden bei von folgenden Personengruppen personenbezogene Daten verarbeitet:

- Mitarbeiter
- Praktikanten
- Auszubildende
- Rentner
- Aushilfskräfte (Leiharbeiter, Zeitarbeiter)
- Bewerber
- Mieter
- Ansprechpartner von Interessenten
- Ansprechpartner von Lieferanten
- Ansprechpartner von Dienstleister
- Ansprechpartner von Kunden
- Ansprechpartner von Behörden oder öffentlichen Stellen

Deshalb agieren wir proaktiv und gestalten Prozesse und Vorgaben so, dass sie auf Basis des Risikos für den Betroffenen in ausreichender Weise geschützt werden. Datenschutz ist ein fortlaufender Prozess, der ständig neue oder geänderte Anwendungsfälle im Unternehmen hat. Deshalb ist es erforderlich, dass Mitarbeiter die Rahmenbedingungen kennen und anwenden können.

## Datenschutzziele

Unser höchstes Ziel im Datenschutz ist es, konform zur DSGVO und dem BDSG zu arbeiten.

Unsere daraus abgeleiteten Datenschutzziele sind primär die Vermeidung von ungewollten Datenabflüssen und der Erhalt der Vertraulichkeit der Daten.

Uns liegt besonders daran, unsere Mitarbeiter zu schützen, was auch den Schutz der Daten über unsere Mitarbeiter beinhaltet.

Besondere personenbezogene Daten erheben und verarbeiten wir hauptsächlich von Beschäftigten und ggf. Bewerbern.

Wir schützen alle personenbezogenen Daten, doch in den genannten Bereichen sehen wir auch ein besonderes Risiko für den Datenschutz, da hier die meisten personenbezogenen Daten durch uns verarbeitet werden und zeitgleich auch das Risiko am höchsten ist, dass ein Nachteil für die betroffene Person entstehen könnte, wenn in die Vertraulichkeit, Verfügbarkeit oder Integrität der Daten unrechtmäßig eingegriffen wird.

Die Verfügbarkeit von personenbezogenen Daten muss bis zur verpflichtenden Löschung (Zweckwegfall, Ende Archivierungspflicht, ggf. Löschanfrage) bestehen bleiben.

Die Integrität von personenbezogenen Daten beschreibt, dass diese nicht unrechtmäßig, bspw. „aus Versehen“ oder durch Schadsoftware verändert werden.

Die Vertraulichkeit besagt, dass personenbezogene Daten nur durch die Personen eingesehen werden können, welche auch mit ihrer Verarbeitung betraut wurden.

Der Schutz von personenbezogenen Daten ergibt sich aus den folgenden Grundsätzen heraus.

## Grundsätze

Unser Unternehmen ist sich seiner Verantwortung bei der Einhaltung datenschutzrechtlicher Bestimmungen und der Verantwortung bezüglich der Sicherheit der Verarbeitung aller unternehmensrelevanten Informationen bewusst und legt im Rahmen der Verarbeitung jeglicher Daten und Informationen die folgenden Grundsätze fest:

- **Fairness und Rechtmäßigkeit**  
Wir wahren die Betroffenenrechte, indem wir Informationen auf rechtmäßige Weise erheben und verarbeiten.
- **Zweckbindung**  
Wir erheben Informationen lediglich für die vorher eindeutig festgelegten Zwecke und beachten, dass eine nachträgliche Änderung der Zwecke nicht oder nur eingeschränkt zulässig ist.
- **Transparenz**  
Wir informieren die Betroffenen vollumfänglich mit unseren jeweiligen Informationsblättern auf geeignete Weise über den Umgang, die Verwendung und die Empfänger der Daten sowie ihre Rechte als Betroffene im Sinne der EU-DSGVO und wie sie diese umsetzen können.
- **Datensparsamkeit**

Wir erheben in unserem Unternehmen nur die tatsächlich notwendige Menge an Daten, die für die Erfüllung des Zwecks erforderlich ist und speichern keine Daten auf Vorrat, es sei denn, dies ist aufgrund einer Rechtsvorschrift erforderlich.

- **Löschung**  
Sobald die Grundlage für die Speicherung und Aufbewahrung entfällt, z. Bsp. die Vertragsgrundlage oder die gesetzliche Aufbewahrungsfrist, löschen wir die Daten oder anonymisieren Sie soweit, dass eine Zuordnung zu der betroffenen Person technisch nicht mehr möglich ist.
- **Richtigkeit und Aktualität**  
Wir treffen in unserem Unternehmen geeignete Maßnahmen, um die Richtigkeit und Aktualität der Daten zu gewährleisten.
- **Vertraulichkeit und Datensicherheit**  
Wir behandeln alle Daten und Informationen im Unternehmen vertraulich und schützen sie durch geeignete technische und organisatorische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung und Weitergabe, Verlust, Vernichtung und Veränderung.

## Vertraulichkeit der Verarbeitung

Die personenbezogenen Daten sowie die unternehmensrelevanten Informationen unterliegen dem Datengeheimnis bzw. dem Geschäftsgeheimnisgesetz. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Als unbefugt gilt jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein.

Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten und unternehmensrelevanten Informationen erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Mitarbeiter dürfen personenbezogene Daten sowie unternehmensrelevante Informationen nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Vorgesetzte müssen ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses und auf Ihre Verschwiegenheit zu unternehmensrelevanten Informationen unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

## Sicherheit der Verarbeitung

Personenbezogene Daten und unternehmensrelevante Informationen sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der

Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten zu orientieren. Hierfür ist der Datenschutzbeauftragte in geeigneter Form im Vorfeld zu beteiligen. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten und unternehmensrelevanter Informationen müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

## **Kontrolle von Datenschutz und Datensicherheit**

Die Einhaltung der Richtlinien zum Datenschutz, der geltenden Datenschutzgesetze sowie der Datensicherheit im Unternehmen wird mindestens einmal jährlich durch ein internes Datenschutzaudit überprüft. Die Durchführung obliegt dem Datenschutzbeauftragten und dem internen Ansprechpartner für Datenschutzthemen sowie der Geschäftsführung oder beauftragten externen Prüfern. Die Ergebnisse sowie die abgeleiteten Empfehlungen und Maßnahmen der Datenschutzaudits sind zu protokollieren und der Geschäftsführung mitzuteilen.

## **Vorfälle im Bereich Datenschutz und Datensicherheit**

Alle Beschäftigten im Unternehmen sollen unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie, gegen das Datenschutzhandbuch oder gegen weitere bestehende Richtlinien oder andere Vorschriften zum Schutz personenbezogener Daten sowie unternehmensrelevanter Informationen melden. Die jeweiligen Verantwortlichen sind verpflichtet, die Geschäftsführung sowie den Datenschutzbeauftragten umgehend über Datenschutz- und Sicherheitsvorfälle zu unterrichten.

In Fällen von

- » unrechtmäßiger Übermittlung personenbezogener Daten oder unternehmensrelevanter Informationen die dem Geschäftsgeheimnis unterliegen an Dritte,
- » unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten und unternehmensrelevante Informationen, oder
- » bei Verlust personenbezogener Daten oder unternehmensrelevanter Informationen

sind die im Unternehmen vorgesehenen Meldungen unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutz- und Sicherheitsvorfällen erfüllt werden können.

## **Sanktionen**

Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht sowie das Geschäftsgeheimnisgesetz werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

## **Inkrafttreten der Datenschutzleitlinie**

Diese Richtlinie tritt mit Unterschrift der Geschäftsführung in Kraft und wird entsprechend der rechtlichen und technologischen Entwicklung fortlaufend angepasst.





\_\_\_\_\_  
Datum

\_\_\_\_\_  
Unterschrift der Geschäftsführung

\_\_\_\_\_  
Datum

\_\_\_\_\_  
Unterschrift der Geschäftsführung

\_\_\_\_\_  
Datum

\_\_\_\_\_  
Unterschrift der Geschäftsführung

\_\_\_\_\_  
Datum

\_\_\_\_\_  
Unterschrift der Geschäftsführung