Datenschutz

Mandanteninformation

Datenschutz D1/2024

Mandanteninformation Datenschutz D1/2024

Inhalt

1. DSGVO-Compliance im KI-Zeitalter

Tipps für einen sicheren Einsatz im Unternehmen

In unserer digitalisierten Welt gewinnt der Einsatz von künstlicher Intelligenz (KI) in Unternehmen immer mehr an Bedeutung. Der Einsatz von KI kann dabei zu einer enormen Effizienzsteigerung und Zeitersparnis führen. Dabei sollte jedoch der Datenschutz nicht vergessen werden. Der nachfolgende Beitrag gibt Ihnen einen Überblick, was beim Einsatz von KI datenschutzrechtlich zu beachten ist.

1.1 Was ist künstliche Intelligenz?

Eine genaue Definition von künstlicher Intelligenz ist nicht einfach, da bereits der Begriff der "Intelligenz" schwer einzuordnen ist. Allgemein lässt sich sagen, dass KI als Teilbereich der Informatik ein Oberbegriff für viele verschiedene Technologien ist. Beispiele hierfür sind Systeme, die lernfähig sind, Muster erkennen oder komplett neue Informationen generieren können. Zwei Programme, die künstliche Intelligenz einsetzen, sind **ChatGPT** und **Microsoft Copilot**. ChatGPT ist ein Chatbot, der mit Hilfe von KI mit Nutzern über Bilder und Texte kommunizieren kann. Microsoft Copilot basiert auf ChatGPT und ist eine intelligente Assistenzfunktion für Microsoft 365-Anwendungen bzw. Windows.

1.2 Welche Rolle spielt Datenschutz bei der Nutzung von KI?

Die Datenschutz-Grundverordnung (DSGVO) beschäftigt sich mit dem Schutz personenbezogener Daten. Hierzu zählen z. B. Name, E-Mail-Adresse, Telefonnummer oder die IP-Adresse. Beim Einsatz von KI im beruflichen Kontext besteht die Möglichkeit, dass entsprechende Systeme mit personenbezogenen Daten in Kontakt kommen.

1.3 Was ist datenschutzrechtlich zu beachten, wenn Sie KI in Ihrem Unternehmen einsetzen?

Wenn Sie in Ihrem Unternehmen KI einsetzen wollen, sollten Sie aus Datenschutzsicht insbesondere die nachfolgenden Punkte berücksichtigen:

Abschluss eines Auftragsverarbeitungsvertrags (AVV)

Beim Einsatz von KI-Lösungen externer Anbieter, ist regelmäßig der Abschluss eines Auftragsverarbeitungsvertrags erforderlich. Dadurch wird gewährleistet, dass der Dienstleister die Datenschutzstandards der DSGVO einhält. Viele dieser Unternehmen bieten heutzutage vorgefertigte Verträge an, die Sie oftmals von der Webseite herunterladen können oder auf Anfrage erhalten.

Wichtig: bevor Sie den Vertrag unterzeichnen, sollte dieser immer von Ihrem Datenschutzbeauftragten oder einem Rechtsanwalt geprüft werden.

Durchführung einer Datenschutz-Folgenabschätzung (DSFA)

Eine Datenschutz-Folgenabschätzung (DSFA) ist immer dann erforderlich, wenn Sie Datenverarbeitungen vornehmen, die ein hohes Risiko für betroffene Personen darstellen. Insbesondere der Einsatz neuer Technologien wie KI kann - je nach Anwendung - ein entsprechendes Risikopotenzial aufweisen. So führen die deutschen Aufsichtsbehörden z. B. den Einsatz künstlicher Intelligenz im Bereich des Kundensupports als ein Beispiel an, für das die Durchführung einer DSFA regelmäßig erforderlich ist. Eine DSFA ist ein Verfahren, mit dessen Hilfe Datenschutzrisiken beim Einsatz von KI identifiziert, bewertet und - bei Bedarf - durch entsprechende Schutzmaßnahmen reduziert werden können.

Wichtig: wenn Sie verpflichtet sind, eine DSFA durchzuführen, schreibt das Gesetz unabhängig von Ihrer Mitarbeiterzahl die Benennung eines Datenschutzbeauftragten vor. Dieser unterstützt Sie bei der späteren Durchführung einer DSFA.

Sensibilisierung von Mitarbeitern

Ihre Mitarbeiter spielen eine Schlüsselrolle beim Einsatz von KI. Durch gezielte und wiederholte Schulungen lernen diese, wie Sie produktiv und gleichzeitig verantwortungsvoll mit KI-Anwendungen im beruflichen Alltag umgehen. Darüber hinaus ist es empfehlenswert, dass Sie Ihren Mitarbeitern zusätzlich einen Leitfaden an die Hand geben, der konkrete Handlungsanweisungen enthält und die wichtigsten Punkte im Umgang mit entsprechenden Systemen zusammenfasst.

1.4 Was sind mögliche Folgen bei einem Verstoß gegen die DSGVO?

Verstöße gegen die DSGVO können hohen Geldbußen oder Schadensersatzansprüche zur Folge haben. Möglich sind auch Reputationsschäden oder ein Vertrauensverlust. Aus diesem Grund sollte der Einsatz von KI im Vorfeld stets sorgfältig geplant und datenschutzrechtlich geprüft werden.

Fazit

Künstliche Intelligenz hält immer mehr Einzug in den beruflichen Alltag und kann zu enormen Effizienz- und Produktivitätssteigerungen führen. Dabei sollte jedoch stets der Datenschutz berücksichtigt werden, um ein unnötiges Risiko zu vermeiden.

Sie planen, KI in Ihrem Unternehmen einzusetzen? Unsere spezialisierten Rechtsanwälte, Datenschutzbeauftragten und IT-Experten unterstützen Sie gerne bei der Umsetzung.

Vereinbaren Sie jetzt ein kostenloses Online-Erstgespräch mit unserem Rechtsanwalt Daniel Lösch.

Hier geht's zur Terminbuchung!

2. Datenschutz im Homeoffice

2.1 Worauf müssen Sie achten?

Im Zuge der zunehmenden Digitalisierung und nicht zuletzt wegen der Corona-Pandemie hat sich die Arbeit außerhalb der betrieblichen Räume - sei es in der Privatwohnung oder unterwegs - etabliert. Diese modernen Arbeitsformen bieten eine Reihe von Vorteilen, von der erhöhten Flexibilität für Mitarbeiter bis hin zur Vermeidung von Fahrtzeiten. Zu beachten ist allerdings, dass Arbeiten außerhalb des Unternehmens erhöhte datenschutzrechtliche Risiken beinhalten können. Der nachfolgende Beitrag gibt Ihnen einen kurzen Überblick, auf was Sie als Arbeitgeber achten sollten:

2.2 Homeoffice, Mobiles Arbeiten und Telearbeit

Die Begriffe Homeoffice, Telearbeit und mobiles Arbeiten werden häufig synonym gebraucht, obwohl es sich um unterschiedliche Arbeitsformen handelt.

Telearbeit ist in der ArbStättV definiert und bezeichnet einen vom Arbeitgeber fest eingerichtete Bildschirmarbeitsplätze im Privatbereich eines Beschäftigten. Dabei sind Arbeitszeit und Dauer der Telearbeit gemeinsam festzulegen und in einer Vereinbarung festzuhalten. Darüber hinaus stellt der Arbeitgeber die Ausstattung mit Mobiliar, Technik und den nötigen Kommunikationseinrichtungen zur Verfügung. Im Rahmen der Telearbeit können Beschäftigte entweder komplett im Privatbereich tätig sein oder einen Teil der Arbeitszeit innerhalb des Unternehmens erbringen. Im letztgenannten Fall spricht man von alternierender Telearbeit.

Mobile Arbeit bedeutet, dass Arbeitnehmer Ihre Arbeitsleistungen mit Hilfe eines mobilen Endgeräts von einem beliebigen Ort aus erbringen. Mobile Endgeräte sind z. B. Laptops, Smartphones oder Tablets. Die Arbeitsleistung kann dabei von unterwegs (Bahnfahrt, bei einem Kunden oder sogar aus dem Ausland) oder zuhause erbracht werden.

Homeoffice ist ein umgangssprachlicher Begriff und wird in der Öffentlichkeit häufig als Synonym für Telearbeit verwendet.

Alle drei Begriffe haben eine Gemeinsamkeit: die Arbeit wird nicht in den betrieblichen Räumlichkeiten des Arbeitgebers erbracht.

2.3 Was ist bei der Arbeit außerhalb der Unternehmensräume datenschutzrechtlich zu beachten?

Wenn Unternehmen personenbezogene Daten verarbeiten (z. B. von Kunden oder Mitarbeitern) haben sie sicherzustellen, dass angemessene technische und organisatorische Maßnahmen ergriffen werden, um diese Daten zu schützen. Beispiele für organisatorische Maßnahmen sind Schulungen der Mitarbeiter im Umgang mit personenbezogenen Daten. Technische Maßnahmen sind z. B. der Einsatz von Antivirenprogrammen, Firewall oder die Durchführung von Backups zur Datensicherung.

Wenn Mitarbeiter außerhalb der betrieblichen Räumlichkeiten arbeiten, steigt das Datenschutzrisiko. Arbeitgeber haben diesen Umstand zu berücksichtigen und die bereits vorhandenen technischen und organisatorischen Maßnahmen anzupassen oder zu erweitern. Es ist empfehlenswert, **konkrete Regelungen** zu treffen, auf was Mitarbeiter bei der Arbeit außerhalb des Betriebs zu achten haben. Beispiele hierfür sind:

- Der Einsatz eines VPN oder einer sicheren W-LAN bei der Verbindung mit dem Firmennetzwerk
- Die Nutzung eines abgetrennten Arbeitszimmers - soweit möglich
- Das Verbot der Nutzung privater Hardware
- Die Vermeidung beruflicher Gespräche und Meetings in öffentlichen Bereichen (z. B. in der Bahn)
- Die sichere Verwahrung und Entsorgung von betrieblichen Unterlagen, die personenbezogene Daten enthalten

Neben diesen Beispielen gibt es eine Reihe weiterer Maßnahmen. Diese sind je nach Einzelfall zu bestimmen und umzusetzen. Darüber hinaus ist es sinnvoll, **Mitarbeiter regelmäßig zu schulen** und dort das Thema Datenschutz und Homeoffice ebenfalls aufzunehmen. Ein weiterer wichtiger Baustein ist die Regelung der Nutzung des **betrieblichen Internet- und E-Mail-Accounts**.

Wenn Sie als Unternehmen personenbezogene Daten für andere Unternehmen als Dienstleister verarbeiten (sog. Auftragsverarbeitung), dann sollten Sie zudem darauf achten, dass im Auftragsverarbeitungsvertrag keine Untersagung von Arbeit außerhalb der Geschäftsräume enthalten ist. Wenn eine entsprechende Klausel vereinbart worden ist und Ihre Mitarbeiter dennoch außerhalb Ihres Betriebs tätig sind, verstoßen Sie möglicherweise gegen den Vertrag. In einem solchen Fall ist es sinnvoll, mit dem Auftraggeber in Kontakt zu treten und eine Streichung oder Abänderung der Klausel zu vereinbaren.

Fazit

Wenn Ihre Arbeitnehmer außerhalb der betrieblichen Räumlichkeiten tätig sind, können sich erhöhte Datenschutzrisiken ergeben. Durch geeignete Maßnahmen lassen sich diese Risiken minimieren. Wichtige Bausteine sind dabei regelmäßige Mitarbeiterschulungen, die Festlegung klarer Regelungen, auf was Mitarbeiter achten müssen sowie eine Bestimmung hinsichtlich der Nutzung des betrieblichen Internets und E-Mail-Postfachs. Neben dem Datenschutzrecht ist dabei auch darauf zu achten, dass die Arbeit außerhalb der betrieblichen Räumlichkeiten arbeitsrechtlich geregelt ist.

Bitte sprechen Sie uns an!

Sie wissen nicht genau worauf Sie beim Thema Homeoffice in Bezug auf Datenschutz achten müssen? Unsere spezialisierten Rechtsanwälte, Datenschutzbeauftragten und IT-Experten unterstützen Sie gerne.

Vereinbaren Sie jetzt ein kostenloses Online-Erstgespräch mit unserem Rechtsanwalt Daniel Lösch.

Hier geht's zur Terminbuchung!

Ihre Ansprechpartner:

Homed David Stingl
Associate Partner

+49 9441 2970-0
Homed.Stingl@mtg-group.de

staatl. gepr. Betriebswirt (IHK)
Marc Utry
Datenschutzbeauftragter DSB-TÜV

+49 9441 2970-0
Marc.Utry@mtg-group.de

Lydia Danzer
Rechtsanwältin
Datenschutzbeauftragte nach DSC-Standard

- Datenschutzrecht
- Vertretung von Unternehmen als Datenschutzbeauftragte
- Datenschutzrechtliche Beratung

+49 9441 2970-0
Lydia.Danzer@mtg-group.de

Master of Laws (LL.M.)
Daniel Lösch
Rechtsanwalt

- Datenschutzrecht

+49 941 208645-0
Daniel.Loesch@mtg-group.de

Wirtschaftsprüfung, Steuerberatung und Rechtsberatung aus einer Hand!

Kontaktieren Sie uns!
Wir beraten Sie gerne!
info@mtg-group.de
www.mtg-group.de

MTG Wirtschaftskanzlei