

Datenschutz-Due-Diligence-Prüfung bei Dritten

I. Verarbeitet Ihr Unternehmen personenbezogene Daten im Auftrag von DS Smith?*

Bitte geben Sie den Standortnamen von DS Smith an:

Ja

Nein

II. Angaben zur Verarbeitung personenbezogener Daten (Füllen Sie diesen Abschnitt nur aus, wenn die Antwort auf Frage I „Ja“ lautet)

1. Werden Sie zur Erbringung dieser Dienstleistungen auf Dritte zurückgreifen?

Ja

Nein

2. Werden die personenbezogenen Daten im Zusammenhang mit DS Smith in verschiedene Länder übertragen oder von dort aus abgerufen (einschließlich über Unterauftragsverarbeiter)?

Ja

Nein

3. Werden Sie personenbezogene Daten verarbeiten, die einen der folgenden Punkte betreffen?

(Wählen Sie alle zutreffenden Optionen aus)

a) Automatisierte Entscheidungsfindung mit rechtlichen oder ähnlichen Auswirkungen

Automatisierte Entscheidungsfindung bedeutet die Fähigkeit, Entscheidungen mit technologischen Mitteln ohne menschliches Zutun zu treffen. Beispiele hierfür sind automatisierte Verarbeitungen, die zu einer Entscheidung führen, die einer Person den Zugang zu einem bestimmten Produkt oder einer bestimmten Dienstleistung verwehrt.

b) Profiling

Unter Profiling versteht man eine Tätigkeit, die auf die Verwendung personenbezogener Daten abzielt, um bestimmte persönliche Aspekte einer Person zu bewerten, Aspekte hinsichtlich der Arbeitsleistung, der wirtschaftlichen Situation, der Gesundheit, der persönlichen Vorlieben, der Interessen, der Zuverlässigkeit, des Verhaltens, des Aufenthaltsorts oder der Bewegungen dieser Person zu analysieren oder vorherzusagen. Dazu gehört beispielsweise die Erstellung von Marketingprofilen darüber, wie jemand mit einer Website interagiert.

c) Systematische Überwachung von Personen

Die systematische Überwachung umfasst Aktivitäten wie den Einsatz von Videoüberwachungssystemen in öffentlichen Räumen und jede andere regelmäßige Beobachtung öffentlich zugänglicher Bereiche, da Einzelpersonen sich der Überwachung nicht entziehen können. Dazu gehört auch die Überwachung von Mitarbeiterarbeitsplätzen und der Internetnutzung am Arbeitsplatz sowie die Überwachung der Nutzung bestimmter Dienste, wie beispielsweise die Erfassung des Fahrverhaltens.

d) Zusammenführung personenbezogener Daten

Die Zusammenführung oder Verknüpfung personenbezogener Daten aus zwei oder mehr (i) Verarbeitungsvorgängen, die ursprünglich für unterschiedliche Zwecke durchgeführt wurden, und (ii) Datenunternehmen (von denen mindestens eines Teil des Unternehmens ist) in einer Weise, die über die zumutbaren Erwartungen der betroffenen Person hinausgeht. Beispiele hierfür sind die Zusammenführung von durch Cookies erhobenen Daten mit Informationen aus Bewerbungen oder die Verknüpfung von Daten aus verschiedenen Quellen.

e) Verarbeitung sensibler personenbezogener Daten

Zu den sensiblen personenbezogenen Daten können Finanzdaten, Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, zur Identifizierung einer Person verwendete biometrische Daten, Gesundheitsdaten sowie Daten über das Sexualleben oder die sexuelle Orientierung einer Person gehören. Beispiele hierfür sind die Verarbeitung von Bildern zur Hautanalyse, Informationen, die zur Berücksichtigung einer Behinderung eines Mitarbeiters erforderlich sind, oder die Überprüfung des Strafregisters von Bewerbern.

f) Verarbeitung personenbezogener Daten in großem Umfang

Um festzustellen, ob ein Lieferant eine große Menge personenbezogener Daten verarbeitet, könnten die folgenden Faktoren berücksichtigt werden: (i) die Anzahl der betroffenen Personen – entweder als konkrete Zahl oder als Anteil an der relevanten Grundgesamtheit (beispielsweise personenbezogene Daten aller Mitarbeiter des Unternehmens, die Dienstleistungen des Lieferanten in Anspruch nehmen); (ii) das Volumen der personenbezogenen Daten und/oder die Bandbreite der verschiedenen Kategorien von personenbezogenen Daten, die verarbeitet werden; (iii) die Dauer oder Dauerhaftigkeit der Dienstleistungen, die mit der Verarbeitung personenbezogener Daten verbunden sind; (iv) die geografische Reichweite der erbrachten Dienstleistungen.

g) Verarbeitung personenbezogener Daten schutzbedürftiger Personen

Eine Person gilt als „schutzbedürftig“, wenn in ihrer Beziehung zum Unternehmen ein erhebliches Ungleichgewicht hinsichtlich der Kontrolle oder des Verständnisses der Beziehung besteht. Beispiele hierfür sind Kinder und ältere Menschen; wahrscheinlich fallen auch Mitarbeiter darunter.

h) Einsatz neuer Technologien bei der Erbringung von Dienstleistungen

Beispiele hierfür sind Technologien wie Fingerabdruck- oder Gesichtserkennungsscanner, als diese ursprünglich zu Sicherheitszwecken auf den Markt gebracht wurden. Es ist wichtig zu bedenken, dass neue Technologien im Laufe der Zeit zur gängigen Praxis werden können. Eine Möglichkeit, diese Unterscheidung zu treffen, besteht darin, zu beurteilen, ob die Nutzung durch das Unternehmen als Nutzung durch einen „First Adopter“ oder einen „Early Adopter“ angesehen werden würde.

- i) **Dienstleistungen, die dazu führen, dass Personen daran gehindert werden, ein Recht auszuüben, eine Dienstleistung in Anspruch zu nehmen oder einen Vertrag abzuschließen**
Dies kann die Verarbeitung von Daten umfassen, bei der Bewerber anhand ihrer Qualifikationen geprüft, bestimmte Kandidaten, die bestimmte Kriterien nicht erfüllen, abgelehnt oder die Leistung von Mitarbeitern anhand der erfassten Arbeitsstunden analysiert wird, woraus sich dann ihr Anspruch auf Jahresurlaub ergibt.

- j) **Verwendung von Cookies oder ähnlichen Tracking-Technologien**
Dies kann Anbieter umfassen, die Cookies, Pixel, Tags, Geräte-Fingerprinting oder ähnliche Tracking-Tools auf Websites, Portalen oder Anwendungen einsetzen, die sie in unserem Auftrag betreiben. Beispielsweise ein Anbieter, der ein kundenorientiertes Portal betreibt, das Analyse-Cookies zur Erfassung des Besucherverhaltens nutzt, oder eine Marketingplattform, die Retargeting-Pixel auf unseren Webseiten platziert, um personalisierte Werbung anzuzeigen.

4. Garantieren Sie, dass Sie über folgende Maßnahmen verfügen:

- a) Verfahren eingerichtet haben, die DS Smith dabei unterstützen, Anfragen von betroffenen Personen (z.B. Auskunft, Löschung, Berichtigung, Widerspruch) innerhalb der gesetzlichen Fristen zu bearbeiten?

Ja Nein

- b) über ein dokumentiertes Verfahren zur Meldung von Datenschutzverletzungen verfügen, das eine rechtzeitige Benachrichtigung der Kunden gewährleistet?

Ja Nein

5. Haben Sie in den letzten zwei (2) Jahren Folgendes erlebt:

- a) Sicherheitsvorfälle oder Datenschutzverletzungen, die zu einer Meldung an eine Datenschutzbehörde oder betroffene Personen geführt haben

oder

- b) jeder Sicherheitsvorfall bzw. jede Sicherheitsverletzung, die zu einer Aufforderung, einer Untersuchung oder einem Durchsetzungsverfahren seitens der Datenschutzbehörde führt.

Ja Nein

6. Verfügen Sie über ein dokumentiertes Verfahren zur Meldung von Datenschutzverletzungen, das eine rechtzeitige Benachrichtigung der Kunden gewährleistet?

Ja Nein

7. Waren Sie in den letzten zwei (2) Jahren Gegenstand von Anordnungen, Ermittlungen oder Durchsetzungsverfahren einer Datenschutzbehörde?

Ja Nein

III. Benachrichtigung über Änderungen bei der Verarbeitung personenbezogener Daten

Der Lieferant hat den Käufer unverzüglich schriftlich, ohne unnötige Verzögerung und in jedem Fall innerhalb der in der geltenden Datenverarbeitungsvereinbarung festgelegten Frist über jede tatsächliche oder vernünftigerweise zu erwartende wesentliche Änderung im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Lieferanten oder einen vom Lieferanten im Zusammenhang mit der Erfüllung dieser Vereinbarung beauftragten Unterauftragsverarbeiter zu informieren.

Diese Mitteilungspflicht gilt insbesondere in den folgenden Fällen:

1. Wenn der Anbieter oder ein Unterauftragsverarbeiter mit der Verarbeitung personenbezogener Daten beginnt, die er zuvor nicht verarbeitet hat oder die nicht zum ursprünglichen Verarbeitungsumfang gehörten.
2. Wenn der Lieferant oder ein Unterauftragsverarbeiter die Art, den Umfang oder den Zweck der Verarbeitung personenbezogener Daten gegenüber den ursprünglich vereinbarten Bedingungen wesentlich ändert.

3. Wenn sich der Standort der personenbezogenen Daten ändert, sodass diese nun in einem anderen Land verarbeitet, gespeichert oder abgerufen werden.
4. Wenn sich wesentliche Änderungen im Geschäftsbetrieb des Anbieters oder eines Unterauftragsverarbeiters ergeben, wie z. B. Änderungen der Eigentumsverhältnisse, der Organisationsstruktur oder der Sicherheitsvorkehrungen.
5. Wenn der Anbieter oder ein Unterauftragsverarbeiter im Zusammenhang mit der Verarbeitung personenbezogener Daten gemäß dieser Vereinbarung automatisierte Verarbeitungsverfahren, Profiling oder künstliche Intelligenz einführt oder deren Nutzung wesentlich ändert.

Diese Benachrichtigungspflicht gilt kumulativ zu den Benachrichtigungspflichten gemäß dem Abschnitt „AI-Risiko-Due-Diligence“ dieses Formulars, der geltenden Datenverarbeitungsvereinbarung oder sonstigen vertraglichen Verpflichtungen zwischen den Parteien und ersetzt oder beschränkt diese nicht.

IV. Unterzeichnung

Ort / Datum:

.....

Name des Unternehmens und des Mitarbeiters:

.....

.....

Unterschrift

**Beispiele für personenbezogene Daten:*

- Geschäftliche Kontaktdaten (z. B. Name, geschäftliche E-Mail-Adresse)
- Identifikationsdaten, einschließlich Online-Identifikatoren (z. B. Name, Adresse, Telefonnummer, Benutzernamen, E-Mail-Adressen, Social-Media-Handles, Anmeldedaten, Sozialversicherungsnummer, Steueridentifikationsnummer, Fahrzeugidentifikationsnummer, Kfz-Kennzeichen, Reisepassnummer)
- Biografische Daten (z. B. Geburtsdatum, Alter, Geschlecht, Familienstand, Geburtsort, Bildungsnachweise)
- Finanzdaten (z. B. Bankkontonummer, Kreditkartennummer, Bonität, Einkommen)
- Angaben zur Beschäftigung (z. B. Berufsbezeichnung, Gehalt, beruflicher Werdegang, Notfallkontakte)
- Bilder und Videos (z. B. Fotos, Aufnahmen von Überwachungskameras)
- Standortdaten (z. B. GPS-Daten, Daten von Mobilgeräten)
- Geräteinformationen (z. B. IP-Adresse, Browsertyp, Betriebssystem, MAC-Adresse des Geräts und Online-Browserverlauf)
- Online-Tracking-Daten (z. B. Cookies, Tracking-Pixel, Web-Beacons)
- Verhaltensdaten (z. B. Kaufhistorie, Clickstream-Daten)
- Audioaufzeichnungen (z. B. Voicemails, Aufzeichnungen von Telefongesprächen)
- Metadaten (z. B. Datums- und Zeitstempel, Dateieigenschaften)
- Daten aus sozialen Netzwerken (z. B. Beiträge, Likes, Shares)
- Ethnische Zugehörigkeit / rassische Herkunft Gesundheitsdaten / medizinische Informationen / Informationen zu Behinderungen Biometrische / genetische Informationen Vorstrafen / Straftaten Gewerkschaftszugehörigkeit Politische Meinung, religiöse oder philosophische Ansichten Sexuelle Orientierung / Sexualleben