How-To Datenschutz-konzept

Leitfaden

S-COP GmbH

Rathausplatz 5
83684 Tegernsee

Vorwort

Ein ausreichend ausformuliertes Datenschutzkonzept bewahrt ein Unternehmen vor unnötigen Bußgeldern durch die Aufsichtsbehörde.

Darin werden die von der verantwortlichen Stelle (Ihr Unternehmen) erhobenen und automatisiert verarbeiteten personenbezogenen Daten kategorisiert, die Geschäftsvorgänge dokumentiert und in den jeweiligen technischen und organisatorischen Maßnahmen das beherrschende Datenschutzrisiko bewertet.

Unser Leitfaden soll Ihnen vermitteln, wie wir **Ihr Datenschutzkonzept** aufbauen würden und welche datenschutzrechtlichen Entscheidungen zu treffen sind. Als Ergebnis Ihres Verfahrensverzeichnisses und Beschreibung der datenschutzrechtlich notwendigen Angaben sollte eine klare, transparente und einfach zu verstehende Betrachtung des Datenschutzrisikos aus Ihrer Sicht (als die verantwortliche Stelle) möglich sein.

Auf den folgenden Seiten stellen wir Ihnen anhand praxisnaher Beispiele die wesentlichen Elemente dar, hinterfragen bestehende Gegebenheiten und ermöglichen Ihnen damit eine Sicht durch die Datenschutzbrille.

„Risikobetrachtung durch Interessensabwägung.“

Mit der selbsterklärenden Darstellung und plausiblen Strukturierung wollen wir Ihnen die Möglichkeit geben, Ihr Datenschutzniveau selbstkritisch hinterfragen und das **Datenschutzrisiko** selbstverantwortlich bewerten zu können.

Inhaltlich entscheidend ist neben einer gültigen Rechtsgrundlage zur Erhebung und Verarbeitung personenbezogener Daten jedoch nicht nur die strukturierte Dokumentation in Form eines Verfahrensverzeichnisses, sondern maßgeblich ist auch eine situationsadäquate **Interessensabwägung** aus Sicht aller Betroffenen.

Datenschutzkonzept

Datenschutzrechtlich notwendige Angaben

- ✓ Name und Anschrift der verantwortlichen Stelle
- ✓ Datenschutzverantwortlicher im Unternehmen
- ✓ Datenschutzbeauftragter
- ✓ Zweck der Datenerhebung, -verarbeitung oder -nutzung
- ✓ Organisation und Umsetzung des Datenschutzes
- ✓ Grundlagen der datenschutzrechtlichen Risikobetrachtung
- ✓ Wahrnehmung und Umsetzung der Rechte der Betroffenen
- ✓ Beschreibung und Bewertung des Datenschutzrisikos

Verfahrensverzeichnis

Art. 30 DSGVO Verzeichnis von Verarbeitungstätigkeiten

Was sind Verarbeitungstätigkeiten?
Unter diesem Begriff versteht man alle Vorgänge im Unternehmen, die personenbezogene Daten verarbeiten, wie z. Bsp. im Innenverhältnis bei der Lohnabrechnung oder Einzelverbindungsnachweise der Telefonie und im Außenverhältnis der grundsätzliche Umgang mit Kunden- und Lieferatendaten.

Im Verfahrensverzeichnis müssen nun alle Verarbeitungstätigkeiten, Datenkategorien und Gruppen der Betroffenen aufgelistet werden, um die Erhebung und automatisierte Verarbeitung personenbezogener Daten datenschutzkonform zu dokumentieren.

Ausreichend ausformuliert beantwortet das Verfahrensverzeichnis folgende Fragen aus Sicht der verantwortlichen Stelle:

- ▹ Um welche Kategorien personenbezogener Daten handelt es sich?
- ▹ Welche automatisierten Verfahren werden genutzt?
- ▹ Wie werden die Daten verarbeitet bzw. gelöscht?
- ▹ Welche Datenschutzmaßnahmen schützen die Verarbeitungsvorgänge?
- ▹ Welche Hard- und Software wird eingesetzt, welche technischen Datenschnittstellen gibt es?

Hierfür notwendige Angaben:

- ✓ Rechtsgrundlage
- ✓ Betroffene Personengruppen und Datenkategorien
- ✓ Kategorien von Empfängern
- ✓ Fristen für die Löschung der Daten
- ✓ Datenübermittlung und insbesondere an Drittstaaten

Technische & organisatorische Maßnahmen

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO & Reporting

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technisch

▹ Wie schütze ich mich vor unbefugtem Zutritt?

Organisatorisch

▹ Gibt es eine Rezeption?

▹ Wer erlaubt Personen den Zutritt?

▹ Wer verwaltet die Schließanlage?

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (u.a. Computer, Tablets, Smartphones) von Unbefugten genutzt werden können.

Technisch

▹ Werden zentral überwachter Malware-Schutz und Firewall-Lösungen im lokalem Netzwerk verwendet?

▹ Sind wirklich alle datenverarbeitenden Geräte gleichermaßen vor unbefugtem Zugang geschützt?

Organisatorisch

▹ Wer kontrolliert und prüft die Wirksamkeit der technischen Maßnahmen?

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technisch

▹ Sind alle Benutzer, gemäß der von Ihnen verarbeitenden Datenkategorien eindeutig identifizierbar?

▹ Werden beim Einsatz von Verschlüsselung zuverlässige Zertifikate genutzt?

▹ Wie stelle ich sicher, dass zu löschende Daten auch wirklich gelöscht oder Datenträger entsprechend vernichtet sind?

Organisatorisch

▹ Werden diese Zugriffe regelmäßig auf Gültigkeit geprüft und ggf. die notwendigen Zugriffsrechte entzogen?

▹ Sind externe Dienstleister datenschutzkonform beauftragt?

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technisch

▹ Wird die Lohnbuchhaltung vom Waren-Wirtschaftssystem durch eigenständige Datenverarbeitungssysteme getrennt?

Organisatorisch

▹ Wer prüft die Datenzugriffsrechte und reguliert das Berechtigungskonzept?

▹ Wird das 4-Augen-Prinzip zwischen Rechtevergabe und Rechtekontrolle umgesetzt?

1.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen keinen Personenbezug mehr aufweisen. Die spezifischen Daten sind betroffenen Personen nicht mehr zuzuordnen, sofern die zur Entschlüsselung zusätzlich benötigten Informationen gesondert aufbewahrt werden und durch entsprechende technische und organisatorische Maßnahmen geschützt sind.

Technisch

▹ Werden E-Mail-Adressen verwendet, die einen Rückschluss auf den Namen des Mitarbeiters erlauben?

▹ Wird im CRM-System zwischen privaten und betrieblichen Kontaktinformationen meiner Geschäftspartner ausreichend unterschieden und entsprechend chiffriert?

Organisatorisch

▹ Sind alle Nutzer mit entsprechenden Zugriffsrechten über die Vorgehensweise zur Ver- und Entschlüsselung dieser personenbezogener Daten ausreichend informiert?

2. Integrität Art. 32 Abs. 1 lit. b DSGVO

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technisch

▹ Werden schützenswerte E-Mails verschlüsselt?

▹ Wird bei einer Fernwartung auf ausreichende Sicherheit geachtet?

Organisatorisch

▹ Wie wird die sichere Weitergabe personenbezogener Daten geprüft?

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.

Technisch

▹ Werden bei der Datenerhebung, -veränderung oder -löschung Protokolldateien erzeugt und revisionssicher aufbewahrt?

Organisatorisch

▹ Sind die Zuständigkeiten für die unterschiedlichen Verarbeitungsvorgänge klar geregelt?

3. Verfügbarkeit und Belastbarkeit Art. 32 Abs. 1 lit. b DSGVO

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technisch

▹ Werden die Daten regelmäßig gesichert?

▹ Wird die Datensicherung regelmäßig auf deren Integrität überprüft?

Organisatorisch

▹ Sind die Schutzmaßnahmen zum unterbrechungsfreien Betrieb der EDV dokumentiert?

▹ Wer prüft die Datensicherung und Datenwiederherstellung?

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO

4.1. Datenschutz-Management

Technisch

▹ Gibt es eine softwaregestützte Lösung zur Erstellung und Pflege des Datenschutzkonzeptes?

▹ Wie wird die Datenschutzfolgenabschätzung, falls notwendig, durchgeführt?

▹ Wie können Betroffene ihr Recht auf Auskunft wahrnehmen?

Organisatorisch

▹ Wurde ein Datenschutzbeauftragter bestellt?

▹ Sind die Mitarbeiter und der für den Datenschutz Verantwortliche ausreichend geschult?

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Technisch

▹ Gibt es eine automatisierte Benachrichtigung bei einer Malware-Infektion?

▹ Kann ein verloren gegangenes Smartphone jederzeit gelöscht werden?

Organisatorisch

▹ Wie werden datenschutzrelevante Sicherheitsvorfälle im Unternehmen dokumentiert?

▹ Wer koordiniert die Kommunikation zwischen der verantwortlichen Stelle, den Betroffenen und der Aufsichtsbehörde?

4.3. Datenschutzfreundliche Voreinstellungen

Privacy by design / Privacy by default

Technisch

▹ Wird selbst erstellte bzw. veränderte Software zur Erhebung und Verarbeitung personenbezogener Daten im Unternehmen eingesetzt?

Organisatorisch

▹ Gibt es klar beschriebene Richtlinien für die Erstellung und Veränderung von Software zur Verarbeitung personenbezogener Daten?

4.4. Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technisch

▹ Werden bei der Erhebung und Verarbeitung personenbezogener Daten nur festangestellte Mitarbeiter eingesetzt?

Organisatorisch

▹ Ist jeder interne und externe Nutzer bei der Erhebung, Verarbeitung oder Löschung personenbezogener Daten namentlich bekannt?

▹ Sind diese Vorgänge ausreichend vertraglich vereinbart?

5. Rechte der betroffenen Personen

Es ist seitens der verantwortlichen Stelle sicherzustellen, dass folgende **Rechtsansprüche der Betroffenen** fristgemäß beantwortet und umgesetzt werden können:

- ▹ Art. 15 DSGVO Recht auf Auskunft
- ▹ Art. 16 DSGVO Recht auf Berichtigung
- ▹ Art. 17 DSGVO Recht auf Löschung („Recht auf Vergessenwerden“)
- ▹ Art. 18 DSGVO Recht auf Einschränkung der Verarbeitung
- ▹ Art. 19 DSGVO Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
- ▹ Art. 20 DSGVO Recht auf Datenübertragbarkeit
- ▹ Art. 21 DSGVO Widerspruchsrecht

Risikobewertung

Interpretation der Wirksamkeit der Umsetzung aller Technischen und Organisatorischen Maßnahmen im Verfahrensverzeichnis.

Bei der Risikobewertung muss anhand der umgesetzten TOM eindeutig und klar beschrieben sein, mit welcher **Eintrittswahrscheinlichkeit** unbefugte Zugriffe auf personenbezogene Daten erfolgen könnten, wie diese Datenschutzverletzungen an die Aufsichtsbehörde und ggf. Betroffenen gemeldet werden und in welcher Granularität sich die verantwortliche Stelle (Ihr Unternehmen) über die Möglichkeiten mangelnder Vorkehrungen bewusst ist.

Interessensabwägung zwischen den betroffenen Personen mit der Rechtsgrundlage der Verarbeitung personenbezogener Daten durch die verantwortliche Stelle.

Eine Interessensabwägung erfolgt grundsätzlich anhand der zugrunde liegenden Rechtsnormen, z. Bsp. das verfassungsmäßig geschützte Recht auf Unversehrbarkeit verbietet automatisch eine Veröffentlichung von Gesundheitsdaten oder diskriminierende Details aus dem Privatleben.
Im handelsüblichen Gewerbebetrieb sind wesentliche Entscheidungskriterien der Interessensabwägung u.a. wie und wann wurden personenbezogene Daten erhoben und zu welchem Zweck verarbeitet.
Gibt es klar geregelte Fristen zur Überprüfung und Löschung, immer bezugnehmend zum Zweck und der Rechtsgrundlage aus Sicht der verantwortlichen Stelle?

Wird im Zuge der Risikobewertung festgestellt, dass eine Datenschutzfolgenabschätzung notwendig wird, ist zwangsläufig ein **Datenschutzbeauftragter** zu bestellen!

KONTAKT

Wir stehen Ihnen gerne jederzeit zur Verfügung, helfen Ihnen bei Ihrem Anliegen gerne weiter und können Ihnen lästige Dokumentationspflichten und Unsicherheiten abnehmen.

Registrieren Sie sich für unseren Newsletter!

S-COP GmbH
Rathausplatz 5
83684 Tegernsee

+49 (0)8022 7058 185
datenschutz@s-cop.bayern
https://www.s-cop.bayern