SICON®

IT-SICHERHEIT · CONSULTING · DATENSCHUTZ

Datenschutzmanagement nach DSGVO

LEITFADEN

Inhaltsverzeichnis

Durch die Digitalisierung ist die Menge digitaler Informationen, die erfasst und gespeichert werden, exponentiell gewachsen. Gleichzeitig steigt der Missbrauch von Daten durch Unternehmen und Regierungen. Die Datenschutz-Grundverordnung (DS-GVO) soll diesem Umstand Rechnung tragen und unsere personenbezogenen Daten schützen.

Sie zielt darauf ab den Datenschutz europaweit zu harmonisieren und die informationelle Selbstbestimmung von Einzelpersonen zu gewähren. Dabei drohen bei Missachtung der Vorschriften empfindliche Geldbußen von bis zu 4% des weltweiten Umsatzes des Vorjahres.

Wen verpflichtete die DS-GVO?

Die DS-GVO verpflichtet Verantwortliche und Auftragsverarbeiter dazu die Verarbeitungsvorgänge und die hierfür eingesetzte Technik im Hinblick auf die Gewährleistung des grundrechtlichen Schutzes der Rechte der Betroffenen auszugestalten. Insofern betrifft die DS-GVO alle Organisationen.

Ein Verantwortlicher ist die Person oder Firma, die den Zweck und die Art und Weise bestimmt, für die personenbezogene Daten verwendet werden. Der Verantwortliche ist für die Einhaltung der Grundsätze der Verarbeitung nach Art. 5 Abs. 1, 24 DSGVO verantwortlich und muss deren Einhaltung nachweisen können.

Ein Auftragsverarbeiter ist jeder, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, beispielsweise IT-Dienstleister, Datenanalyse-Dienste, die Daten auf einem Server bereitstellen oder speichern. Der Auftragsverarbeiter muss die Rechtmäßigkeit der Verarbeitung dem Verantwortlichen gegenüber nachweisen können.

Schutz persönlicher Daten

Alle Unternehmen verarbeiten Daten wie IP-Adressen, Protokoll- oder Zahlungsdaten. Nur wenige Organisationen steuern diese Daten auf konsistente Art und Weise.

Dementgegen stehen Interessen der Verbraucher. Diese sind zwar besorgt über die Verwendung und den Missbrauch persönlicher Daten, stimmen aber paradoxerweise häufig der Teilung ihrer Daten zu, um auf neue digitale Dienste zugreifen zu können.

Durch die DS-GVO sind Unternehmen verpflichtet die Verarbeitung personenbezogener Daten besser zu organisieren und Anforderungen zum Schutz personenbezogener Daten umzusetzen, wie beispielsweise das Recht auf Vergessenwerden, Datenportabilität, obligatorische Benachrichtigung bei der Verletzung des Schutzes personenbezogener Daten, einschließlich der Daten die außerhalb Europas übertragen werden. Es sind Geldbußen von bis zu 4% des weltweiten Jahresumsatzes möglich.

Was sind die Nutzen eines Datenschutz-Management-Systems?

Die DS-GVO entwickelte sich aus einem mangelnden Vertrauen von Verbrauchern und Aufsichtsbehörden in Unternehmen, die immer größere Datenmengen sammeln und nutzen.

Ein systematischer Ansatz zum Schutz personenbezogener Daten liefert Verantwortlichen ein Werkzeug, um den Nachweis zu erbringen, dass personenbezogene Daten nach den Vorgaben der DS-GVO verarbeitet werden und damit langfristig Erfolg zu haben.

Das Datenschutz-Management-System (DMS) bietet einen Rahmen für die Planung und Implementierung von Richtlinien und Prozessen zur Einhaltung gesetzlicher Anforderungen. Es werden Werkzeuge und Maßnahmen herangezogen um bei jeder einzelnen Verarbeitung zu prüfen, ob das rechtlich geforderte SOLL von Maßnahmen mit dem vor Ort vorhandenen IST von Maßnahmen übereinstimmt. Verstöße gegen den Schutz personenbezogener Daten können verhindert oder abgemildert werden. Es wird ein Verständnis dafür geschaffen, in welcher Form Verstöße gegen den Schutz personenbezogener Daten auftreten und was dagegen getan werden kann. Sie werden auf den Umgang mit Datenschutzverstöße vorbereitet, indem das Personal geschult wird und Verfahren zur Schadensbegrenzung sowie zur Information von betroffenen Personen, Behörden, Kunden und Mitarbeitern entwickelt werden.

Damit Unternehmen das Vertrauen ihrer Kunden, Mitarbeiter und anderer Interessengruppen gewinnen und halten können, müssen sie digitale Verantwortung beweisen: Verantwortliche versichern Kunden, dass ihre persönlichen Daten sicher sind. Auftragsverarbeiter zeigen Glaubwürdigkeit gegenüber Verantwortlichen.

Die Sicherheit der Daten wird durch die Auswahl technisch-organisatorischer Maßnahmen erreicht und stetig unter Berücksichtigung des Stands der Technik optimiert. Diese Maßnahmen müssen angemessen und geeignet sein, die Risiken für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen soweit einzudämmen, dass ein dem Risiko angemessenes Schutzniveau gewährleistet wird.

Die lückenlose Dokumentation des DMS sorgt für die geforderte Transparenz der Datenverarbeitungen, das Vertrauen interessierter Parteien und unterstützt den Verantwortlichen dabei seiner Rechenschaftspflicht nachzukommen.

Gerne unterstützen wir Sie auch bei Zertifizierungen. Diese fördern das Vertrauen in die Verwendung von Big Data in Ihrem Unternehmen und helfen Ihnen, die Möglichkeiten der digitalen Transformation zu nutzen.

Die Schutzziele und Anforderungen der DS-GVO

Die Schutzziele oder Gewährleistungsziele der Datenschutz-Grundverordnung zielen auf eine rechtskonforme Verarbeitung personenbezogener Daten und bestehen darin, das Risiko des Eintretens von Abweichungen von einer rechtskonformen Verarbeitung hinreichend zu mindern. Diese Ziele unterstützen die systematische Umsetzung rechtlicher Anforderungen in technische und organisatorische Maßnahmen und können somit als „Optimierungsgebote“ aufgefasst werden. Im Einzelnen sind dies:

- Datenminimierung
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Nichtverkettung
- Transparenz
- Intervenierbarkeit

Hierin finden sich die seit vielen Jahren in der Praxis bewährten Schutzziele der Informationssicherheit nach IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik wieder. Diese dienen vor allem der Absicherung und dem Schutz der Daten einer Organisation.

Der Fokus aus der Sicht des Datenschutzes liegt dabei jedoch nicht auf der Organisation, sondern auf dem Schutz des Betroffenen. Daraus ergeben sich folgende Anforderungen:

- Transparenz für Betroffene von Verarbeitungen personenbezogener Daten
- Zweckbindung einer Verarbeitung personenbezogener Daten - Datenminimierung einer Verarbeitung personenbezogener Daten
- Richtigkeit personenbezogener Daten
- Speicherbegrenzung personenbezogener Daten
- Integrität personenbezogener Daten
- Vertraulichkeit personenbezogener Daten
- Rechenschafts- und Nachweisfähigkeit des Verantwortlichen

Umsetzung und Implementierung der DS-GVO

Die DS-GVO fordert die Unternehmen zur Regelkonformität auf, um nachzuweisen zu können auf welche Art sie Daten verarbeiten und speichern und auf Informationsanfragen reagieren. Um dies zu erreichen, müssen Unternehmen kohärente Prozesse definieren und sicherstellen, dass sie im gesamten Unternehmen einheitlich angewendet werden. Regelmäßige Audits und Sensibilisierungsmaßnahmen helfen dies zu erreichen.

Die DS-GVO ist eine weitreichende Regelung, die einerseits die Datenschutzrechte von Einzelpersonen und andererseits die Pflichten von Unternehmen regelt. Dazu gehört die klare Verantwortung der Unternehmen, die Einwilligung von Personen einzuholen, über die sie Daten erheben. „Daten“ umfasst sowohl personenbezogene Daten, die zur Identifizierung einer Person, wie Name oder IP-Adresse, verwendet werden können als auch sensible personenbezogene Daten wie religiöse und politische Ansichten oder die sexuelle Orientierung. Ein Schlüsselbegriff ist die Verantwortlichkeit.

Organisationen übernehmen die Rechenschaftspflicht für die von ihnen verarbeiteten Daten und müssen die erforderlichen Ressourcen und Fähigkeiten bereitstellen, um einen optimalen Schutz der persönlichen Daten zu gewährleisten. Die Verpflichtungen sind höher für größere Organisationen sowie für Unternehmen, die eine „regelmäßige und systematische Überwachung“ von Einzelpersonen durchführen oder eine Vielzahl sensibler Daten verarbeiten.

Die Verordnung zielt auch darauf ab, die Transparenz zu erhöhen, nachdem es zu einer Reihe von Verstößen gegen die Datenschutzbestimmungen bei Millionen von Internetnutzern gekommen ist. Organisationen, die Opfer von Hackern werden oder sensible Kundendaten verlieren, müssen den Vorfall innerhalb von 72 Stunden bei der Datenschutzbehörde ihres Landes melden.

In der DS-GVO geht es zu einem großen Teil darum, den Verbrauchern die Datenhoheit zurückzugeben. Beispielsweise können Einzelpersonen kostenlos nach persönlichen Informationen fragen, und Unternehmen müssen die Antwort innerhalb eines Monats geben. Die DS-GVO gibt den Verbrauchern auch das Recht auf Löschung ihrer personenbezogenen Daten.

Das Datenschutz-Management-System

Die Implementierung des DMS umfasst die Planung, Einführung, den Betrieb und die regelmäßige Kontrolle der Rechtmäßigkeit der Datenverarbeitung und erfolgt in folgenden Teilschritten:

- Aufnahme der Verarbeitungstätigkeiten mit personenbezogenen Daten
- Dokumentation und Beurteilung der Rechtmäßigkeit personenbezogener Verarbeitungen
- Bewertung des Risiko für die Rechte und Freiheiten betroffener Personen
- Auswahl und Umsetzung technischer und organisatorischer Maßnahmen
- Schaffung von Transparenz für Betroffene
- Kontrolle und Verbessern der Maßnahmen

Zwei wesentliche Ansätze aus der DSGVO sind dabei Datenschutz by design und Datenschutz by default. Datenschutz by design fordert Organisationen auf den Schutz personenbezogener Daten bei der Gestaltung von Produkten und Dienstleistungen zu

berücksichtigen. Datenschutz by default fordert Unternehmen auf über ein Informationssystem zu verfügen, das jederzeit ein hohes Datenschutzniveau gewährleistet. Das Ergebnis ist ein hohes Maß an Datensicherheit sowie die Einhaltung der DS-GVO.

Gerne stehen wir Ihnen für eine persönliche Beratung zur Verfügung

Sie erreichen unsere Teams von Montag bis Freitag zwischen 8 - 17 Uhr

SICON GmbH

- Datenschutz - Datensicherheit -ISMS - ISO 27001 -

06831 - 122 411

info@sicon-it.de