DATENSCHUTZ LEICHT GEMACHT: EINE ORIENTIERUNGSHILFE VON NETZLINK

INHALT

EINLEITUNG

UNSER VERSTÄNDNIS:
DATENSCHUTZ & IT-SECURITY ALS FESTE EINHEIT

UNSERE EXPERTISE

HERAUSFORDERUNGEN BEIM DATENSCHUTZ

WORAUS ES ANKOMMT:
GRUNDSÄTZLICHE REGELUNGEN ZUM DATENSCHUTZ

FAZIT

BESUCHEN SIE UNS

IMPRESSUM

EINLEITUNG

„Ehrlich gesagt habe ich kein Problem damit, wenn meine persönlichen Daten im Internet stehen, ich habe ja nichts zu verbergen…“ – haben Sie nicht? Ihr Name, Ihre E-Mail-Adresse oder Ihre Kreditkartennummer sind nur einige wenige Beispiele für sensible Daten, die eindeutig Ihrer Person zuzuordnen sind. Diese Informationen sind sehr begehrt, denn es lassen sich aus ihnen Rückschlüsse über Ihr Kaufverhalten, Ihre Interessen, Ihre Lebensweise oder Ihren Arbeitgeber ziehen. Sie werden beispielsweise für die Marktforschung, personalisiertes Marketing oder gezielte Angriffe auf Unternehmen genutzt. Die Verarbeitung Ihrer Daten ist jedoch nur dann zulässig, wenn Sie selbst dazu eingewilligt haben. Gelangen Ihre persönlichen Daten ohne Ihre Zustimmung in die falschen Hände, sind die Folgen durch möglichen Missbrauch schwerwiegend: In Ihrem Namen könnten beispielsweise Verträge abgeschlossen, Produkte gekauft oder sonstige Banking-Geschäfte durchgeführt werden.

Der Schutz von personenbezogenen Daten stellt in Europa und Deutschland ein hohes Gut dar. Durch das Recht auf informationelle Selbstbestimmung hat jeder Mensch grundsätzlich die Freiheit, selbst zu entscheiden, welche Informationen preisgegeben werden und auf welche Weise diese verwendet werden dürfen. In der Folge muss sich jede Organisation, die personenbezogene Daten verarbeitet, ausführlich mit dem Thema Datenschutz auseinandersetzen. Vom Start-Up bis zum Konzern, vom Frisörsalon bis zum Krankenhaus mit KRITIS-Infrastruktur – die Thematik ist für alle von höchster Relevanz.

UNSER VERSTÄNDNIS: DATENSCHUTZ & IT-SECURITY ALS FESTE EINHEIT

Um effektiven Datenschutz zu gewährleisten, ist dieser stets in Verbindung mit IT-Security zu betrachten. Wir bei Netzlink verfolgen für ein ganzheitliches Datenschutzkonzept einen interdisziplinäreren Ansatz, bei dem beide Aspekte Hand in Hand gehen. Auf diese Weise lassen sich datenschutzrechtliche Vorgaben sowohl aus organisatorischer Perspektive als auch aus technologischer Sicht umsetzen.

Die Beziehung zwischen Datenschutz und IT-Security lässt sich wie folgt veranschaulichen: IT-Security hilft dabei, Datenschutz bei elektronischen Daten durch technologische Maßnahmen zu gewährleisten. So führt beispielsweise die Abwehr von Cyber-Attacken auf ein Unternehmen dazu, dass Datendiebstahl oder auch die Veränderung von personenbezogenen Daten verhindert und somit der Schutz der Daten sichergestellt wird.

UNSERE EXPERTISE

Im Rahmen des vom Bundesministerium für Gesundheit (BMG) geförderten Projekts SORMAS (Surveillance Outbreak Response Management and Analysis System) verantwortet Netzlink unter anderem das Arbeitspaket für Datenschutz und IT-Sicherheit. Die Anwendung zum Kontaktpersonenmanagement für den öffentlichen Gesundheitsdienst dient der Eindämmung der Corona-Pandemie. Durch dieses Projekt konnten wir unsere umfassende Expertise im Bereich Datenschutz und IT-Security, insbesondere für das Gesundheitswesen, weiter ausbauen und stehen unseren Kunden mit Rat und Tat zur Seite.

Für alle Fragen rund um den Datenschutz wenden Sie sich jederzeit an unser Netzlink-Expertenteam. Gemeinsam erarbeiten wir mit Ihnen eine passende Datenschutz-Strategie!

HERAUSFORDERUNGEN BEIM DATENSCHUTZ

Beim Thema Datenschutz sehen sich Organisationen zahlreichen Herausforderungen und Fragen gegenüber. Die Kenntnis darüber, welche „Baustellen" bei der Umsetzung auftreten können, hilft bei der Bewältigung dieser.

Welche datenschutzrechtlichen Vorgaben gelten für mein Unternehmen?

Grundlegend für den Datenschutz in Deutschland ist die DSGVO (Datenschutz-Grundverordnung). Sie wurde im Jahr 2016 eingeführt und gilt seit 2018 in Europa als verpflichtend. Daneben bestehen noch weitere Verordnungen und Gesetze für den Datenschutz, wie zum Beispiel das Bundesdatenschutzgesetz (BDSG) oder bereichspezifische Gesetze wie das Telemediengesetz. Jede Organisation ist in der Verantwortung, abhängig von der Art der verarbeiteten Daten, dem Zweck und den zutreffenden Bundes- und Länderbestimmungen die für sie relevanten Vorgaben zu identifizieren und umzusetzen.

Wie bleibe ich in Sachen Datenschutz auf dem neuesten Stand?

Die rechtlichen Vorgaben zum Datenschutz unterlagen besonders in den ersten Jahren seit Einführung der DSGVO zahlreichen Konkretisierungen. Zudem kommen regelmäßig neue ergänzende Gesetze und Verordnungen hinzu, die spezifische Bereiche detaillierter regeln. Bei Veränderungen stets up-to-date zu bleiben und diese für das eigene Unternehmen passgenau zu integrieren, ist für die Gewährleistung des Datenschutzes zentral. Dafür ist es hilfreich, aktuelle Stellungnahmen von Aufsichtsbehörden und Gerichten zu verschiedenen datenschutzrelevanten Fällen zu verfolgen.

Worauf ist bei der Erstellung des Datenschutzkonzept zu achten?

Im Datenschutzkonzept erfolgt die detaillierte Beschreibung technischer und organisatorischer Maßnahmen und Vorgaben, um personenbezogene Daten zu schützen beziehungsweise die Rechtmäßigkeit der Verarbeitung zu belegen. Dazu gehört unter anderem eine Beschreibung der Art und des Zwecks der verarbeiteten Daten. Für die Übersicht der Datenverarbeitungen in einem Unternehmen ist gemäß DSGVO ein Verzeichnis von Verarbeitungstätigkeiten (VVT) mit allen wesentlichen Angaben zur Datenverarbeitung zu führen. Es bildet die Grundlagendokumentation und ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Die Entwicklung von Maßnahmen und die Dokumentation des Datenschutzes kann, je nach Tätigkeit und Art der verarbeiteten Daten, sehr umfangreich sein. Generell ist es sinnvoll zu wissen, auf welche Aspekte Aufsichtsbehörden im Falle einer Überprüfung besonderen Wert legen und diese gesondert herauszuarbeiten.

Was erwartet mich bei der Umsetzung von Datenschutzvorgaben in meinem Unternehmen?

Die Vorgaben an den Datenschutz sind in der DSGVO in ihren einzelnen Anwendungsfällen und Ausprägungen nicht immer eindeutig beschrieben. Die personenbezogenen Daten im Unternehmen sind, den datenschutzrechtlichen Vorgaben gemäß, bestmöglich und nachvollziehbar zu verarbeiten. Dies impliziert einen gewissen Auslegungsspielraum, innerhalb dessen das eigene Vorgehen zu begründen ist. Die rechtlichen Vorgaben müssen auf die eigene Situation, in Einklang mit den individuellen Gegebenheiten im Unternehmen, angewendet werden.

WORAUF ES ANKOMMT: GRUNDSÄTZLICHE REGELUNGEN ZUM DATENSCHUTZ

Unabhängig der verschiedenen, individuellen Vorgaben zum Datenschutz regelt die DSGVO allgemein geltende Bestimmungen zum Schutz personenbezogener Daten in Art. 5 („Grundsätze für die Verarbeitung personenbezogener Daten“)[1]. Diese stellen die Grundlagen des Datenschutzes in Deutschland dar.

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz:** Die Forderung nach rechtmäßiger, bestmöglicher und nachvollziehbarer Verarbeitung personenbezogener Daten beschreibt das Kernanliegen des Datenschutzes.
- **Zweckbindung:** Personenbezogene Daten dürfen nur zu einem bestimmten, festgelegten Zweck verarbeitet werden.
- **Datenminimierung:** Organisationen dürfen nur die Daten erheben, die für den jeweiligen Zweck erforderlich sind.
- **Richtigkeit:** Es ist darauf zu achten, dass die personenbezogenen Daten im Besitz eines Unternehmens aktuell und korrekt sind.
- **Speicherbegrenzung:** Eine unbefristete Aufbewahrung personenbezogener Daten ist unzulässig. Löschfristen dienen dazu, dass diese nicht auf unbestimmte Zeit archiviert und verwendet, sondern nach Erfüllung ihres Zwecks ordnungsgemäß vernichtet werden.
- **Integrität und Vertraulichkeit:** Personenbezogene Daten sind vor Diebstahl oder auch Beschädigung zu schützen. Zu diesem Zweck kommen unter anderem IT-Security-Maßnahmen zum Einsatz: Die Absicherung von Netzwerken durch verschlüsselte Datenübertragung, technische Zugangsbeschränkungen oder der Schutz vor Phishing-Angriffen reduzieren mögliche Einfallstore für Angreifer.
- **Rechenschaftspflicht:** Organisationen sind für die Einhaltung des Datenschutzes verantwortlich. Gegenüber Aufsichtsbehörden müssen sie in der Lage sein, ihr Datenschutzvorgehen nachzuweisen.

[1] Quelle: https://dsgvo-gesetz.de/art-5-dsgvo/ - Stand Sep. 2021

Weiterhin gut zu wissen:

Benennung einer/eines Datenschutzbeauftragten: Unter bestimmten Umständen ist die Benennung einer/s Datenschutzbeauftragten verpflichtend. Ihre/seine Aufgabe ist es, im Unternehmen datenschutzrelevante Aspekte aufzuzeigen, Beratung zum Datenschutz zu leisten, Hilfestellung bei der Umsetzung zu geben, die Einhaltung der Vorschriften zu überwachen und mit der Aufsichtsbehörde zusammenzuarbeiten. Die Berufung einer externen Person als Datenschutzbeauftragte/n kann sich als sinnvoll erweisen, da diese einen neutralen Blick von außen einbringen und im Zweifel unbefangen agieren kann.

Auftragsverarbeitungsvertrag (AVV): Erhalten Dritte, beispielsweise externe Dienstleister, Zugriff auf gespeicherte personenbezogene Daten eines Unternehmens und verarbeiten diese weisungsgebunden als Auftragsverarbeiter, ist ein Auftragsverarbeitungsvertrag abzuschließen.

Meldepflicht bei Verletzungen des Datenschutzes: Datenschutzverletzungen sind eigenverantwortlich unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden an die jeweils zuständige Aufsichtsbehörde zu melden.

Informations-, Auskunfts-, Berichtigungs- und Löschpflichten: Unternehmen müssen anfragenden Personen Auskunft über die eigenen gespeicherten Daten geben, fehlerhafte Daten berichtigen und die Daten auf Wunsch löschen, wenn sie keinem Zweck mehr dienen.

FAZIT

Noch viel zu oft wird das Thema Datenschutz eher stiefmütterlich behandelt. Der Grund dafür liegt auf der Hand - für Unternehmen selbst bedeutet es keinen unmittelbaren Mehrwert, sich mit Datenschutz auseinanderzusetzen. Vielmehr bündelt die Beschäftigung mit der Thematik zeitliche und finanzielle Ressourcen. Kommt es jedoch zu einer Überprüfung durch die zuständige Aufsichtsbehörde oder einem Vorfall der Datenschutzverletzung, drohen hohe Bußgeld- bis hin zu Freiheitsstrafen. Unabhängig davon sollten sich Unternehmen jedoch auch im eigenen Interesse um ein wasserdichtes Datenschutzkonzept bemühen: Gelangen zum Beispiel vertrauliche Daten Ihrer Kunden an die Öffentlichkeit, ist mit einem hohen Schaden für die eigene Reputation zu rechnen.

Ein umfassendes Datenschutzkonzept bietet die Grundlage, um Datenschutzvorgaben effektiv umzusetzen. Dafür müssen sich die festgelegten Datenschutzrichtlinien im Unternehmen in bestehende Prozesse einfügen, mitwachsen und stets mitgedacht werden. Damit Datenschutz Teil der Unternehmens-DNA werden kann, sollten sich die Vorgaben auf natürliche Weise in die Unternehmensrealität integrieren, und keinesfalls als störender Faktor gelten. Nur, wenn bereits die Führungsebene im Unternehmen dem Datenschutz eine hohe Bedeutung zumisst und ein datenschutzkonformes Vorgehen fördert, kann sich das Bewusstsein für die Thematik bei allen Kolleginnen und Kollegen etablieren. Zentral sind regelmäßige Datenschutzschulungen für die Mitarbeitenden sowie die frühzeitige Einbindung von Datenschutz und IT-Security in Projekte.

Sie wollen Ihr angestrebtes Datenschutzniveau ohne Umwege erreichen? Wir beraten Sie gern!

BESUCHEN SIE UNS

www.netzlink.com

Social Media

de.linkedin.com/company/netzlink-informationstechnik-gmbh

xing.com/pages/netzlinkinformationstechnikgmbh

twitter.com/netzlink

www.facebook.com/netzlink

IMPRESSUM

Herausgeber:
Netzlink Informationstechnik GmbH
IT-Campus Westbahnhof
Westbahnhof 11
38118 Braunschweig
Telefon: (+49) 0531 707 34 30

Redaktion:
Netzlink Informationstechnik GmbH

Gestaltung:
Netzlink Informationstechnik GmbH

Fotos:
Adobe Stock / NMedia
Unplash / Privecstasy
Unplash / Scott Graham
Pixabay / TheDigitalArtist

Version:
1.0 // 9. September 2021