handwerk. magazin

www.handwerk-magazin.de

Anleitung:

10 PUNKTE DSGVO-ANLEITUNG FÜR UNTERNEHMEN

Autor: Christian Heutger, IT-Sicherheitsexperte

IMMER AUF DER SICHEREN SEITE

DSGVO-ANLEITUNG FÜR UNTERNEHMEN

Ab 25. Mai 2018 muss die EU-Datenschutz-Grundverordnung (DSGVO) in Unternehmen umgesetzt sein. Die IT-Sicherheitsexperten der PSW GROUP haben eine Liste mit den wichtigsten Aufgaben für Unternehmen zusammengestellt.

DATENINVENTUR DURCHFÜHREN

Im Fokus der DSGVO stehen das Prinzip der Datensparsamkeit und die strategische Datenerhebung. Für Unternehmen heißt es also: weg von der Datensammelwut hin zur bedarfsgerechten Erhebung von Daten. Um dieses Ziel zu erreichen und einen Überblick über die vorhandenen, bereits verarbeiteten Daten zu schaffen, eignet sich eine Dateninventur. Dabei treten in der Regel immense Datenberge zum Vorschein; über Jahre hinweg produziert von Mitarbeitern, Kunden, Lieferanten, Partnern und Dienstleistern.

Sämtliche Daten, die im Unternehmen verarbeitet werden, sollten dabei gesichtet werden. Erst mit diesem Überblick kann es an die eigentliche Umsetzung der Regeln der DSGVO gehen. Positiver Nebeneffekt: Unternehmen verschaffen sich einerseits Wissen über sämtliche Datenprozesse und erhalten den Ausgangspunkt, um das sogenannte „Verfahrensverzeichnis“ einzurichten.

In diesen Unternehmensprozessen fallen Daten an und sollten deshalb durchleuchtet werden:

- Verarbeiten von Kundendaten (Vertrags-, Kontakt-, Zahlungsdaten, Kaufhistorie, Bonitätsprüfungen, etc.)
- Cookies und Social Plugins
- Newsletter-Versand
- Analyse- sowie Trackingtools
- Datenverarbeitungsprozesse, die extern geregelt werden
- Finanzen und steuerrechtliche Daten (Rechnungsstellungen, Lohnbuchhaltung, etc.)
- Personaldaten (Arbeitszeiterfassungen und -verträge, Bewerbungsmanagement, etc.)
- Einkauf sowie Vertrieb (Lieferantenkontakte, etc.)
- Buchhaltung
- externe Dienstleister

VERFAHRENSVERZEICHNIS ERSTELLEN

Das Verfahrensverzeichnis ist Pflicht für Unternehmen – die nationalen Aufsichtsbehörden haben das Recht, dieses einzusehen, um die Einhaltung des Datenschutzes zu überprüfen. Versäumnisse können mit hohen Bußgeldern belegt werden.

Im Verfahrensverzeichnis werden sämtliche Datenverarbeitungsprozesse des Unternehmens katalogisiert. Die Pflichtangaben sind:

- Namen und Kontaktdaten des für die Verarbeitung Verantwortlichen sowie die des Datenschutzbeauftragten
- Zwecke der jeweiligen Datenverarbeitung
- Kategorien der Empfänger, denen personenbezogene Daten offengelegt wurden oder noch werden

- Beschreibung der Kategorien betroffener Personen und Kategorien personenbezogener Daten
- Rechtsgrundlagen der Datenverarbeitung
- Angabe der vorgesehenen Löschfristen
- allgemeine Beschreibung technischer und organisatorischer Datenschutzmaßnahmen
- sofern im Einzelfall vorhanden: die Verwendung von Profiling sowie Kategorien von Übermittlungen personenbezogener Daten an Drittstaaten bzw. Unternehmen in Drittstaaten.

COMPLIANCE SCHAFFEN

Die Umsetzung der Datenschutz-Grundverordnung setzt voraus, dass sich sämtliche Mitarbeiter im Unternehmen – insbesondere Entscheidungsträger und IT-Verantwortliche, aber auch das Web-und Social Media-Team – in die Thematik Datenschutz einarbeiten.

Es muss sichergestellt werden, dass ausschließlich Daten erhoben, gespeichert und weiterverarbeitet werden, die für Geschäftsprozesse notwendig sind. Ist geklärt, welcher Mitarbeiter mit welchen Daten im Unternehmen umgehen darf? Kompetenzen dürfen dabei keinesfalls überschritten werden: Nur wer für die Bearbeitung der Daten zuständig ist, darf auch mit ihnen umgehen. Eine Datenspeicherung auf Vorrat darf nicht mehr stattfinden. Ist die Website datenschutzfreundlich gestaltet? Dazu gehört unter anderem auf vorangehakte Checkboxen oder ähnliches verzichten.

DATENSCHUTZ-INFORMATIONEN AKTUALISIEREN

Die meisten Datenschutzerklärungen müssen mit der DSGVO neu aufgesetzt werden und deutlich ausführlicher ausfallen, als das derzeit der Fall ist. Zudem muss über die Verarbeitung personenbezogener Daten informiert werden – und zwar vollständig und verständlich. Die folgenden Inhalte müssen deshalb in der Datenschutzerklärung enthalten sein:

- Name/ Firma und Adresse
- Kontaktangaben, beispielsweise E-Mail-Adresse
- E-Mail-Adresse des Datenschutzbeauftragten, wenn vorhanden
- Welche Daten für welche Zwecke verarbeitet werden. Heißt konkret: Angaben zu einzelnen Verarbeitungstätigkeiten, wenn Nutzer davon betroffen sind. So muss beispielsweise auch die Weiterleitung der Adresse an das Logistikunternehmen benannt werden, wenn Waren versendet werden.
- Werden Daten auf Basis berechtigter Interessen wie Werbemaßnahmen verwendet, müssen diese Interessen benannt werden. Im Falle von Marketingmaßnahmen wären dies etwa „wirtschaftliche Interessen“.
- Es müssen die Rechtsgrundlagen der Datenverarbeitung genannt werden.
- Der Zeitpunkt der Löschung personenbezogener Daten muss angegeben werden.
- Teilt der Nutzer die Daten nicht selbst mit, muss die Datenquelle benannt werden.

- Sämtliche Rechte des Nutzers müssen benannt werden. Besondere Aufmerksamkeit erhält das Widerspruchsrecht; dieses muss gesondert aufgeführt werden und erhält idealerweise einen eigenen Unterpunkt.

NEUE BETROFFENENRECHTE WAHREN

Mit der DSGVO wurden neue Betroffenenrechte geschaffen, allen voran das „Recht auf Vergessenwerden“, das Recht auf Datenübertragbarkeit sowie das Auskunftsrecht. Betroffene, insbesondere Kunden und Mitarbeiter, deren persönliche Daten verarbeitet werden, sollen mit der DSGVO besonders geschützt werden. Diese Betroffenenrechte müssen Teil des Unternehmensworkflows werden: Ist es beispielsweise softwareseitig möglich, das Recht auf Datenübertragbarkeit zügig und umfassend geltend machen zu können? Alle Informationen über einen Betroffenen sollten dafür übersichtlich gespeichert sein, um sie ohne großen Aufwand übertragbar zu machen.

Da Betroffene jederzeit Auskunft über ihre gespeicherten Daten, den Zweck der Datenspeicherung und etwaige Datenweitergaben einholen können, sollten solche Auskünfte per Knopfdruck generiert werden können. Idealerweise ist die Unternehmenssoftware so programmiert, dass Auskunftsfunktionen integriert und geeignete Daten gekennzeichnet sind. Übrigens: Eine solche Auskunft muss unverzüglich erfolgen – die Höchstdauer ist mit einem Monat angesetzt. Und egal, wie hoch der Aufwand ist: Es dürfen keine Kosten in Rechnung gestellt werden.

EXTERNE DATEN

Daten werden in der Cloud gespeichert, E-Mail-Kontaktdaten beim Mailing-Dienstleister hinterlegt, das Callcenter verfügt über unternehmensinterne Daten und so weiter: Oftmals werden Daten nicht komplett allein verwaltet, sondern es sind externe Dienstleister eingebunden. Steht überhaupt fest, welche Daten extern lagern und wer außerhalb des Unternehmens Daten verwaltet?

Existierende Auftragsverarbeitungsverträge sollten dringend auf DSGVO-Konformität überprüft und aktualisiert werden. Von besonderem Interesse sind auch Cloud-Daten. Wer Cloud-Anbieter gewählt hat, die außerhalb der EU sitzen, muss selbst sicherstellen, dass die ausgelagerten Daten nach EU-Recht gespeichert und weiterverarbeitet werden.

FEHLENDE EINWILLIGUNGEN EINHOLEN

Mit dem Start der DSGVO benötigen Unternehmen für jede Datenverarbeitung eine Einwilligung. Das schließt das Erheben, Speichern und Nutzen von persönlichen Daten ein. Unternehmen sollten jetzt intern prüfen, wofür sie noch Einwilligungen benötigen und diese schnell einholen. Nicht vergessen werden dürfen dabei Cookies und Newsletter. Auch hier lohnt sich eine softwareseitige Vorbereitung, aus der schnell ersichtlich ist, welcher Betroffene welche Einwilligungen oder Widersprüche eingereicht hat.

DATENSCHUTZBEAUFTRAGTEN BESTIMMEN

Die meisten Unternehmen sind laut DSGVO verpflichtet, einen Datenschutzbeauftragten zu benennen. Nach deutschem Recht müssen alle Unternehmen mit mehr als 10 Mitarbeitern, die mit personenbezogen Daten arbeiten, einen Datenschutzbeauftragten bestellen. Aber auch für alle anderen lohnt es sich, externe Unterstützung zu holen, um regelmäßig über Änderungen in der Datenschutzgesetzgebung informiert zu sein.

DATENSCHUTZVERSTÖSSE MELDEN

Die DSGVO reagiert auf Datenschutzverstöße mit horrenden, existenzvernichtenden Bußgeldern. Es ist deshalb ratsam ein Verfahren zu implementieren, um Verstöße zügig aufdecken, melden und untersuchen zu können. Im Falle eines Datenschutzverstoßes ist der Verantwortliche für den Datenschutz angehalten, unverzüglich, jedoch spätestens 72 Stunden nach Bekanntwerden, Meldung an die zuständige Aufsichtsbehörde zu machen.

ZERTIFIZIERUNGEN PRÜFEN

Wer ideal auf die DSGVO vorbereitet sein und ihre Regelungen souverän umsetzen will, sollte über eine Zertifizierung nachdenken. Während für große Unternehmen die ISO27001 ideal ist, kommt für KMU beispielsweise die ISIS12-Zertifizierung in Frage. Im Rahmen einer Zertifizierung wird das gesamte Unternehmen auf Datenschutz getrimmt.

Autor: Christian Heutger
Als IT-Sicherheitsexperte berät Christian Heutger Unternehmen zu Datenschutz und IT-Security. Er ist Lehrbeauftragter sowie temporär agierender Lehrer und Dozent, u. a. an der FH Fulda. Heutger ist außerdem Geschäftsführer der PSW GROUP (www.psw-group.de), die sich auf SSL- und Internet Security-Produkte spezialisiert hat, der PSW GROUP Training (www.psw-training.de) sowie der PSW GROUP Consulting (www.psw-consulting.de).