Checkliste Datenschutz – Einführung

Die Checkliste dient der Sensibilisierung für den Datenschutz und beinhaltet eine Zusammenfassung der notwendigen Schritte, um den Datenschutz im Betrieb sicherzustellen und zu dokumentieren.

Vorrangig ist bis zum 25.05.2018 sicherzustellen, dass die formalen Voraussetzungen des neuen Datenschutzgesetzes (BDSG) und der Datenschutzgrundverordnung(DSGVO), die nach außen sichtbar sind, bspw. Datenschutzhinweis, Meldung des Datenschutzbeauftragten, Einwilligungshinweise eingehalten werden. Hier steht vor allem zu befürchten, dass Wettbewerbszentralen und Anwälte bei Fehlen offenkundig notwendiger Angaben Abmahnverfahren in Gang bringen.

Intern hat der Betriebsinhaber/ Geschäftsführer, der datenrechtlich als Verantwortlicher bezeichnet wird, ein **Datenschutzkonzept** – bestehend aus einem Verarbeitungsverzeichnis und der Niederlegung der technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes – zu erstellen.

Viele Einzelfragen lassen sich im Laufe der Erstellung des betrieblichen Datenschutzkonzeptes im Einzelfall und praktisch lösen. Nicht jeder in den Mustern aufgezählte Gesichtspunkt ist für die Einhaltung der Schutzvorschriften elementar, bspw. ist der Einbau einbruchsicherer Türen oder eines Servertresorraumes sicher wünschenswert, aber keine Verpflichtung, die unbedingt einzuhalten ist.

Gem. § 24 DSGVO ist der Verantwortliche verpflichtet, den Datenschutz im Rahmen des Gebotenen und Möglichen umzusetzen. Dieser Rahmen ist von Betrieb zu Betrieb verschieden, entsprechend unterschiedlich sind die Anforderungen an den zu betreibenden Aufwand.

Die herausgegebenen Muster und Formulierungshinweise sind allgemeine Empfehlungen und sind unter Umständen unter Einschluss der IT- Services des Betriebes individuell anzupassen.

Die Checkliste geht von den formal notwendigen Bestandteilen über die einzeln wichtigen Bestandteile des Datenschutzes hin zu allgemeinen Hinweisen.

I. Datenschutzbeauftragter erforderlich?

- Unter den folgenden Voraussetzungen eine Formvorschrift, die durch jeden Betrieb zu beachten ist:

- Bei mehr als 9 datenverarbeitungstauglichen Arbeitsplätzen, Mobile Geräte bei im Ausseneinsatz tätigen Mitarbeiter zählen mit

- Bearbeitung besonders geschützter Daten im erheblichen Umfang (bspw. Gesundheitsdaten)

- intern: Mitarbeiter, Schulung, Kündigungsschutz, Kosten

- extern: Preis beachten

II. Bestandteile des konkreten Datenschutzes

Verarbeitungsverzeichnis erstellen. Organigramm über die Verantwortlichkeiten und den Datenfluss im Unternehmen erstellen. (Muster abarbeiten)

= erster wichtiger Teil des Datenschutzkonzepts, die Verantwortlichkeiten und Wege der Daten zu erfassen und zu dokumentieren.

Technische und organisatorische Maßnahmen dokumentieren. (Muster abarbeiten).

= zweiter wichtiger Teil ist die Erfassung und Dokumentation der tatsächlich vorhandenen Abläufe.

Beides zusammen ergibt ein hinreichend verlässliches Datenschutzkonzept.

Erfassung und gegebenenfalls Erneuerung der nach außen sichtbaren Komponenten des Datenschutzes (Einwilligungen, Signaturen, Hinweise, Pflichtangaben). (Muster und technische Notwendigkeiten einfügen)

Datenschutzmitteilungen und Verpflichtungen der Mitarbeiter (Muster vorlegen und unterschreiben lassen)

Sonderanforderungen an Telearbeit, Mobile Datenverarbeitung, Video- und GPS – Einsatz(Muster beachten)

III. Datenfluss im Unternehmen

1. Kundendaten

Aufnahme der Daten

Telefonisch, persönlich, digital, außer Haus - Datenschutzhinweise, Einwilligungen sind notwendig.

Konkret:

Telefonisch: Bestätigen per E-Mail, schriftlich oder Fax mit Datenschutzhinweis

Persönlich, außer Haus: Hinweis unterschreiben lassen

Digital: per E-Mail: Bestätigung mit Verlinkung zum Datenschutzhinweis

per Login: Datenschutzhinweis obligatorisch anklicken lassen

Notreparaturen, -aufträge, Geschäftsführung ohne Auftrag, Gefahrenabwehr beruhen zumeist auf gesetzlichen (Sicherheits-) Vorschriften, die die Datenbearbeitung rechtfertigen.

Die Verwendung zu Vertragszwecken ist grundsätzlich zulässig, die freiwillig gegebenen Daten berechtigen zur vertragsnotwendigen Verwendung. Die aktive Einwilligung bleibt ein Problem, soweit kein mit ihr verbundener Auftrag unterschrieben wird.

Datenschutzhinweise auf die Datenverwendung und die Rechte der betroffenen Personen sind zu erstellen, einzupflegen und vorzuhalten.

Speicherung

Mitteilung an die betroffene Person im Datenschutzhinweis, notwendig für Wartungen, Garantieleistungen etc. Unzugänglichkeit und Sicherheit in der Speicherung. Dokumentation durch bspw. IT Plan.

Verwendung gegenüber Dritten

Keine Datenweitergabe an Dritte ohne konkrete Einwilligung. Im Einzelfall kann dies zu Vertragszwecken notwendig sein. Garantieleistungen der Hersteller. Weitergabe an Abrechnungszentren. Schadensregulierung mit Versicherungen. Soweit dies zur Erfüllung notwendig ist muss dies im Datenschutzhinweis enthalten sein, soweit eine

konkrete Einwilligung nicht vorliegt. Mit dem Empfänger der Daten müssen Datenschutzabkommen geschlossen sein.

Die Bewerbung eigener Produkte und Dienstleistungen muss genehmigt werden.

Die Weitergabe der Daten an nicht benannte Dritte ist absolut unzulässig.

Löschung

Prinzip der Datenminimierung, nichts länger als es muss. Datenschutzhinweis muss das Recht auf Löschung und die beabsichtigte Aufbewahrung der Daten beinhalten. Beantragt die betroffene Person ist ihm die Datenlöschung ggf. über den Datenschutzbeauftragten zu bestätigten, oder mitzuteilen, was einer Löschung entgegensteht(gesetzliche Aufbewahrungspflichten).

2. Mitarbeiterdaten

Erhebung/ Verwendung

Es sind alle zur Durchführung des Arbeitsvertrages notwendigen Daten zu erheben. Unabhängig von den einzelnen Verschweigensrechten sind dies die üblichen Personendaten, aber auch das Vorliegen von Führerscheinen, Führungszeugnissen, besonderen Befähigungen, soweit der Mitarbeiter dies mitteilt Schwerbinderungen, Personenstandsdaten, Bankdaten etc. Alle Mitarbeiter haben ein Datenschutzmerkblatt und eine Datenschutzerklärung zu unterschreiben. Diese ist der Personalakte beizufügen, oder getrennt für den Datenschutz gesammelt aufzubewahren. Es ist gegebenenfalls auf die Datenweitergabe(DATEV, Krankenkassen, Finanzamt, Lohnbüro, eventuell Vertragspartner(Kontrollen Mindestarbeitsbedingungen) etc.) hinzuweisen und eine Einwilligung erklären zu lassen.

Die Weitergabe außerhalb der der Erfüllung gesetzlicher und arbeitsvertraglicher Verpflichtung ist unzulässig.

Speicherung

Die Mitarbeiterdaten sind gesondert zu speichern, zu sichern und nur von den Mitarbeitern einzusehen, die damit unmittelbar zu tun haben.

Löschung

Nach Beendigung des Arbeitsverhältnisses sind alle Daten zu löschen, die nicht weiter aufgrund gesetzlicher Vorschriften aufzubewahren sind. Der Mitarbeiter hat entsprechende Auskunfts- und Löschungsansprüche.

3. Vertragspartner

Mit IT- Unternehmen, Versicherungen, Dauer- und Großkunden, allen Vertragspartnern gegenüber denen personenbezogene Daten, sei es von Kunden, sei es von Mitarbeitern preisgegeben werden, müssen Datenschutzvereinbarungen in schriftlicher Form abgeschlossen sein. Zumeist werden die Vertragspartner selbst die Vereinbarungen vorlegen.

4. Internet

Website

Datenschutzhinweis auf alle Erhebung, Verwendung von Daten und der Einhaltung der DSGVO und des BDSG. Nutzung der Daten geschäftlicher Kontakten im Konzern und/oder zu Folgegeschäften.

Der Hinweis muss von jeder Seite, wie auch das Impressum zu erreichen sein.

Besondere Einwilligungen und Hinweise in gesicherten und Registrierungsbereichen.

Werbung und Newsletterbestellung gesondert. Bei Werbung und Newsletter auf Ein-Klick- Abbestellung hinweisen.

Auf Tracking- und Cookienutzung hinweisen.

E-Mail

Verschlüsselung nur bei gesetzlicher Vorschrift oder vertraglicher Vereinbarung.

Verlinkung auf den Datenschutzbeauftragten. Sicherer ist die Hinzufügung des Datenschutzhinweises in die Signatur.

Signaturhinweise auf geschäftlichen Mailverkehr und die Behandlung der Kontaktdaten für zukünftige Verwendung und Löschensverpflichtung bei Falschsendung.

E-Mail Textsignatur

Bestimmte Pflichtangaben müssen nicht nur im Impressum auf der Webseite, sondern auch in der E-Mail-Signatur aufgeführt werden. Dies gilt für geschäftsbezogene E-Mails von Aktiengesellschaften, GmbHs, KGs und die OHG sowie alle anderen Kaufleute, die E-Mails zur Abwicklung ihrer Geschäfte nutzen. Ein in der E-Mail-Signatur vorhandener Hyperlink auf die in der Homepage abrufbaren Unternehmensinformationen ist für die Erfüllung der handelsrechtlichen Pflichtangaben grundsätzlich nicht ausreichend. Die Angaben müssen im Textformat erscheinen, nicht als Bild oder Logo.

Werden diese gesetzlichen Vorgaben, die nunmehr durch das EHUG explizit auch auf E-Mails Anwendung finden, nicht eingehalten, drohen Zwangsgelder in Höhe von bis zu EUR 5.000,-. Daneben können ggf. Wettbewerber oder Interessenverbände einen solchen Gesetzesverstoß abmahnen.

Die Pflichtinformationen sind je nach Unternehmensform etwas unterschiedlich, hier ein Beispiel für die Pflichtangaben einer GmbH:

· Firmenbezeichnung wie im Handelsregister, Rechtsformzusatz "GmbH",
· Ort der Handelsniederlassung,
· zuständiges Registergericht, Handelsregisternummer,
· Familienname und mindestens ein ausgeschriebener Vorname jedes Geschäftsführers.

Die E-Mail Signatur muss in jeder geschäftlichen E-Mail vorhanden sein, unabhängig davon, von welchem Gerät die E-Mails versendet werden. In der Praxis kommt es immer wieder vor, dass die E-Mails von mobilen Geräten, z.B. Smartphones oder Tablets, keine gültige E-Mail Signatur enthalten.

E-Mail-Accounts nur betrieblich nutzen.

Sicherung der E-Mails dokumentieren.

Vertretungen und Weiterleitungen dokumentieren.

IV. Allgemeines

Mitarbeiterschulung in regelmäßigen Abständen (Datenschutzbeauftragter).

Schutz sichtbarer Daten. Schreibtische bei Arbeitsende sichern.

Keine unkuvertierten Schreiben im internen Betriebsablauf.

Passwortverwaltung, - hinterlegung organisieren und dokumentieren.

Kundenverkehr von den Arbeitsplätzen fernhalten.

Datenschutzdokumentation gesondert sichern, gleich ob digital oder stofflich. Ein Griff zum Nachweis.

Die Nutzung von Rechner und Internet soll unter Berücksichtigung der Gleichbehandlung geregelt sein.

Der Rechner des Betriebsinhabers sollte frei von privatem Datenaufkommen sein.

Die Einhaltung des Datenschutzes im Betrieb ist zu beachten, ebenso wie die Nutzungsumfänge von Rechnern und Datenträgern sowie der Software.

Besondere Bedeutung hat die Dokumentation für den Fall, dass tatsächliche Beschwerden oder Nachfragen erfolgen, sollte nachgewiesen werden können, dass der Datenschutz im Betrieb Beachtung findet und dies schnell nachgewiesen werden kann.