DIE DSGVO TRITT AM 25.05.2018 IN KRAFT

Was bedeutet das für mein Unternehmen?

Infoveranstaltung Riscreen GmbH am 17.05.2018

Die Riscreen GmbH

Gegründet 2014

Beratung zur Compliance-Themen (Datenschutz und Geldwäscheprävention)

Wir bieten Beratung, Umsetzung und Outsourcing

Wir entwickeln eine Compliance Management Software

Wir sind TÜV zertifiziert und bei Behörden in dieser Funktion angezeigt

Die Riscreen GmbH

Medizintechnik

Software

Pharma

Bank

Medien

Industrie

Beratung

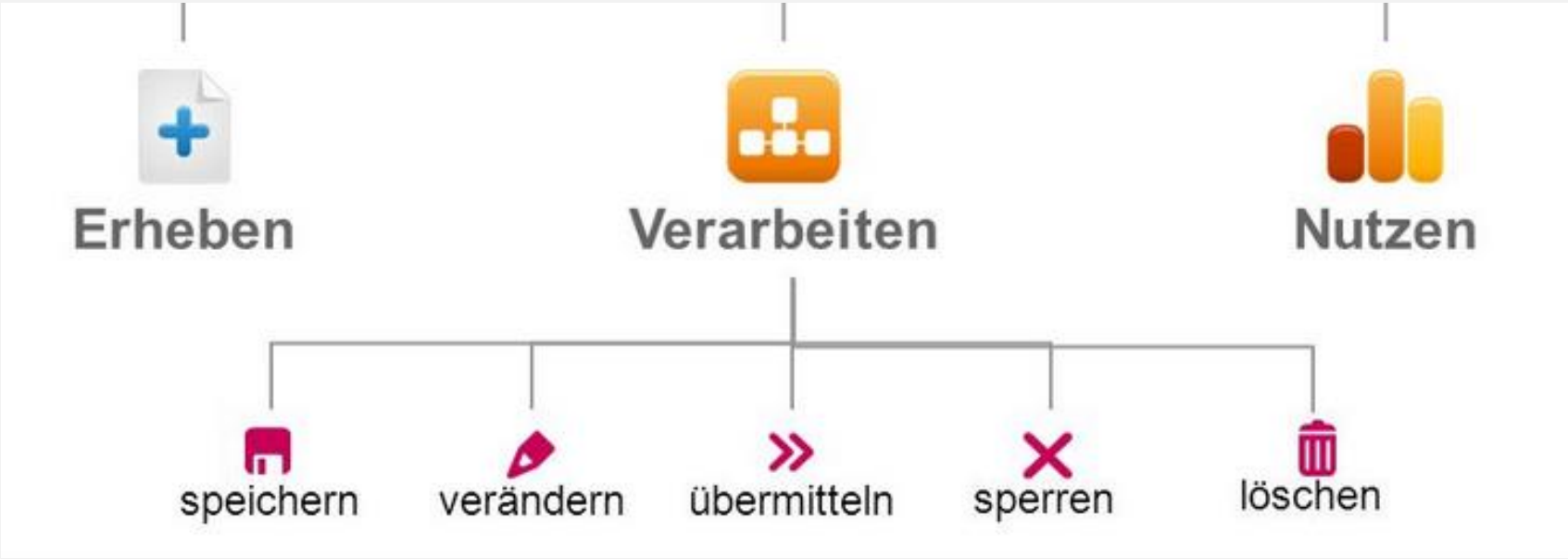
Vereine

Warum Datenschutz – Warum DSGVO?

So wie Sie nicht wollen, dass Daten über Sie Unbefugten zur Kenntnis gelangen, müssen Sie auch dafür sorgen, dass Sie die Daten anderer vertraulich behandeln!

Grundrecht auf informationelle Selbstbestimmung: (Volkszählungsurteil von 1983)

Grundlegendes– Wann gilt die DS Gesetzgebung?



https://edps.europa.eu/sites/edp/files/factsheet_1_de.png

Grundlegendes– Datenschutz und Datensicherheit?

Der Datenschutz:

Beschreibt den Schutz der Daten von natürlichen Personen

Die Datensicherheit

Beschreibt die Maßnahmen die vorgenommen werden um (personenbezogene-) Daten vor unberechtigtem Zugriff zu schützen

Datensicherung und technisch-organisatorische Maßnahmen (TOMs):

Sind ein wesentlicher Bestandteil um überhaupt Datensicherheit gewährleisten zu können. Das Gesetz gibt vor, dass personenbezogene Daten angemessen zu sichern, verwahren und zu verarbeiten sind. Die Maßnahmen um dies zu gewährleisten sind unter anderem eine den aktuellen Standards entsprechendes Datensicherheitskonzept

Grundlegendes - Personenbezogene Daten

Was sind personenbezogene Daten?

allgemeine Personendaten (Name, Geburtsdatum und Alter, Geburtsort, Anschrift, E-Mail-Adresse, Telefonnummer)

Besitzmerkmale (Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, **Kfz-Kennzeichen, Zulassungsdaten)**

Kennnummern (bei der Krankenversicherung, **Personalausweisnummer, Matrikelnummer)**

Physische Merkmale (Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße usf.)

Bankdaten (Kontonummern, Kreditinformationen, Kontostände)

Kundendaten (Bestellungen, Adressdaten, Kontodaten)

Online-Daten (IP-Adresse, Standortdaten)

Werturteile (Schul- und Arbeitszeugnisse)

Grundregeln des Datenschutzes

Verbot mit Erlaubnisvorbehalt /
Rechtmäßigkeit

Transparente Verarbeitung

Zweckbindung

Datenminimierung

Richtigkeit

Definierte Löschpflichten

Datensicherheit

Rechenschaftspflicht

Grundlegendes - Erheben personenbezogener Daten

Verbot mit Erlaubnisvorbehalt / Rechtmäßigkeit

Grundsatz:

- Personenbezogene Daten dürfen **GAR NICHT** erhoben, verarbeitet oder genutzt werden!

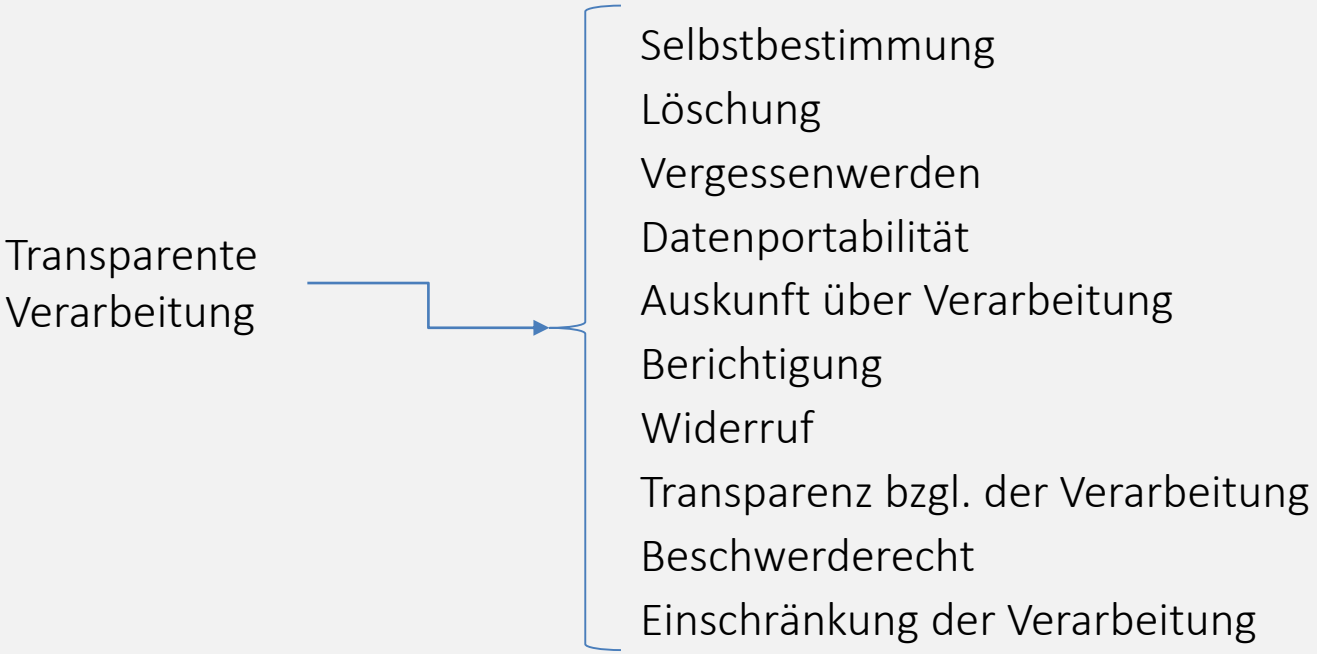
Ausnahmsweise ist die Verarbeitung erlaubt wenn:

- Eine Rechtsgrundlage für die Verarbeitung existiert (z.B. aus dem Telemediengesetz, dem Sozialgesetzbuch, der Gewerbeordnung, etc.) – Spezialgesetze
- Die Verarbeitung durch das Bundesdatenschutzgesetz erlaubt wird
- Der Betroffene einwilligt

Besonderheit **Einwilligung:**

- Einwilligungen sind **Zweckgebunden**
- D.h. jede **Einwilligung** kann **nur für einen Zweck** gelten
- Die Einwilligung muß „positiv“ sein

Grundregeln des Datenschutzes



Die betroffene Person muss wissen, **wer welche Daten für welchen Zweck** verarbeitet. Daher gibt es umfangreiche **Betroffenenrechte** (z. B. Informationspflichten, Auskunftsrechte, Recht auf Berichtigung der Daten, Widerspruchsrecht). Der Zweck muss darüber hinaus legitim, das heißt rechtmäßig sein. **Betroffenenrechte sind immer auch Pflichten der Verantwortlichen Stelle und der Empfänger**, d.h. Letztere müssen die **Sicherstellung der Rechte durch technische und organisatorische Maßnahmen** gewährleisten

Schutz

Grundregeln des Datenschutzes

Zweckbindung

Personenbezogene Daten dürfen immer **nur für einen zulässigen Zweck gespeichert und verarbeitet** werden, über welchen die Betroffenen grundsätzlich zu informieren ist. Daten dürfen nur zweckbezogen an Dritte weitergegeben werden Wenn die Daten für mehrere Zwecke erhoben werden, sind **alle Zwecke** aufzuführen!

Nachträgliche Zweckänderungen sind nur in eng begrenzten Ausnahmefällen möglich.
Sollen Daten an Dritte weitergegeben werden, muss der Betroffene darüber aufgeklärt werden, insbesondere wenn Daten in ein Land außerhalb der europäischen Union weitergeleitet werden.

Grundregeln des Datenschutzes

Datenminimierung

Es dürfen nur die personenbezogenen Daten erhoben und verarbeitet werden, die **für die Zweckerreichung notwendig** sind.

Je mehr Daten man über Personen speichert, desto größer ist die Gefahr, dass die Betroffenen dadurch einen Nachteil haben können. Bei jeder Datenspeicherung muss man sich in die Lage der Betroffenen versetzten und überlegen, ob man selbst möchte, dass jemand anders solche Daten über einen selbst speichert. Speziell aus dem Kommunikationsverhalten sowie dem Surf-Verhalten lassen sich schnell Profile über Menschen erstellen, die eventuell richtig, vielleicht aber auch falsch sind.

Um die Datenminimierung wirksam umzusetzen und das Risiko z.B. durch Hacker zu senken, können auch Anonymisierungs- und Pseudonymisierungsverfahren eingesetzt werden.

Grundregeln des Datenschutzes

Datenminimierung

Bei **Pseudonymisierung** werden personenbezogene Daten durch Zufallscodes ersetzt. Generell muss dazu ein zentrales System eingerichtet werden, das personenbezogene Daten verarbeitet und diese in Codes konvertiert. Für einige Prozesse benötigt man jedoch die Originaldaten. Mithilfe einer Master-Tabelle lassen sich die Codes den ursprünglichen Kennungen zuordnen. So können Mitarbeiter mit pseudonymisierten Dateien arbeiten, die keine Rückschlüsse auf die Identität der betroffenen Personen zulassen.

Bei **Anonymisierung** wird der Code als „Schlüssel“ zum personenbezogenen Datum „weggeworfen“, der Personenbezug kann nicht mehr hergestellt werden

Grundregeln des Datenschutzes

Richtigkeit

Personenbezogene Daten müssen richtig erfasst und über den erforderlichen Verarbeitungszeitraum richtig gehalten werden, anderenfalls sind sie zu löschen. Betroffene Personen haben das Recht auf Richtigstellung.

Löschpflichten

Daten mit Personenbezug müssen beispielsweise nach Wegfall des Zwecks der Verarbeitung und dem Ablauf notwendiger Aufbewahrungsfristen **gelöscht werden**. Es ist nicht zulässig, personenbezogene Daten zeitlich unbefristet aufzubewahren.

Dieser Grundsatz lässt sich am einfachsten durch ein Löschkonzept realisieren. Hierbei werden die unterschiedlichen Datenkategorien klassifiziert und die Löschfristen pro Kategorie festgelegt. Datensätze müssen dann nach Ablauf der Fristen aus dem IT System gelöscht werden.

Grundregeln des Datenschutzes

Sicherheit

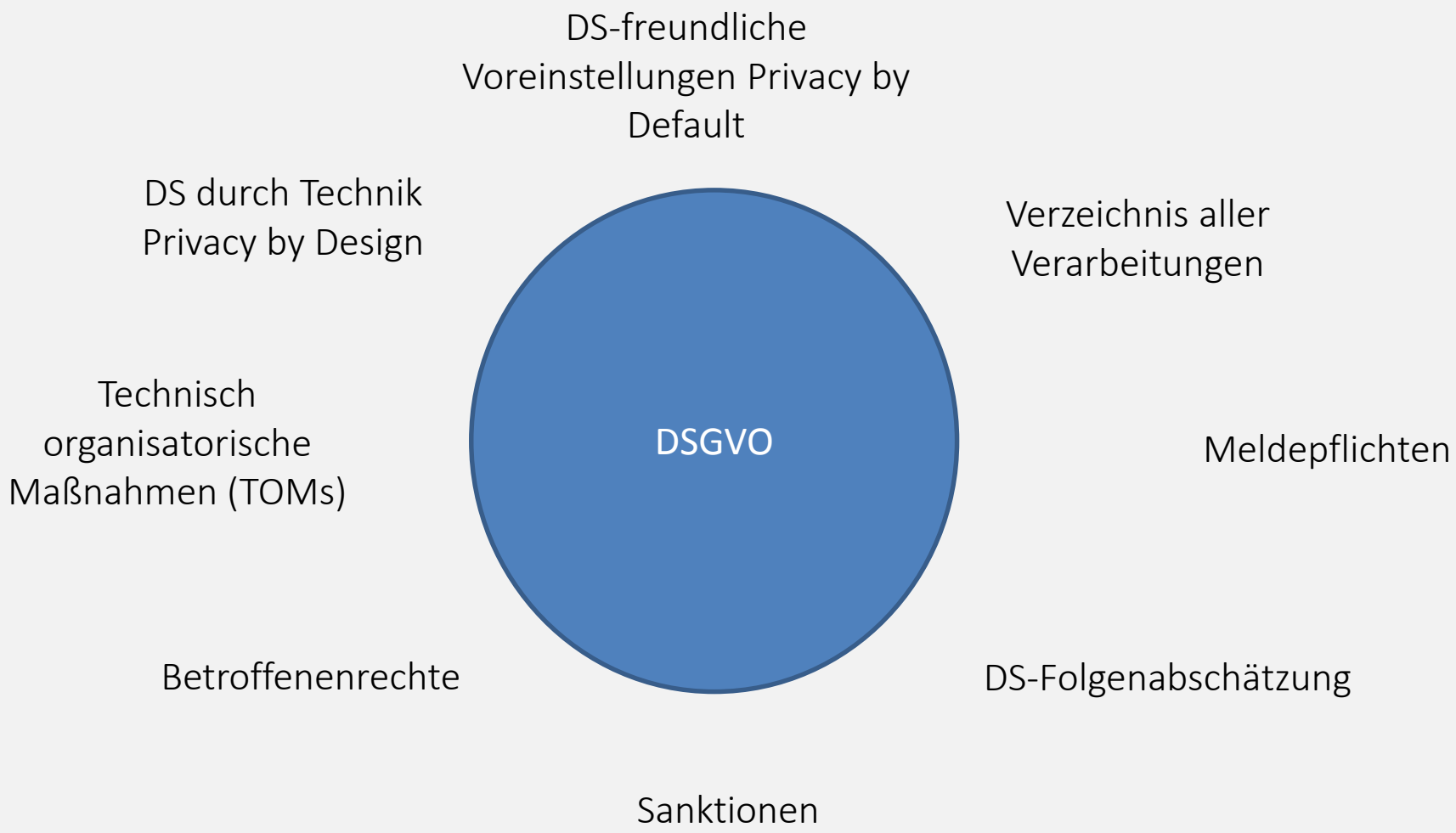
Die Sicherheit der Daten muss durch geeignete **technische und organisatorische Maßnahmen** gewährleistet werden. Wichtige Ziele sind u.a. der Schutz vor unberechtigtem Zugriff, Datenverlust und Manipulation.
Die Datenschutzgrundverordnung verknüpft sehr stark den Datenschutz mit der Technik. Die IT-Verfahren aber auch die Prozesse im Unternehmen müssen somit schon von Anfang an darauf ausgerichtet sein, möglichst wenig personenbezogene Daten verarbeiten zu können (**privacy by design**).
Auch bei der Datensicherheit spielen Verschlüsselungsverfahren, sowie **Anonymisierung und Pseudonymisierung** wieder eine Rolle

Grundregeln des Datenschutzes

Rechenschaftspflicht

Der Verantwortliche für die Datenverarbeitung ist für die Einhaltung der neuen Pflichten aus der Datenschutzgrundverordnung verantwortlich.
Er muss daher auf Anfrage von Betroffenen aber auch ggü. Behörden nachweisen, dass er seine Pflichten erfüllt hat.
Es handelt sich dabei, anders als im alten Bundesdatenschutzgesetz um eine **Beweislastregel** – das betroffene Unternehmen muss ggf. belegen, dass sie sämtliche Vorgaben des Datenschutzrechts eingehalten hat.

DSGVO Schwerpunktthemen



Was bedeutet das für Vereine?

Mitgliederverwaltung

Betrieb der Webseite des Sportvereins (über Hosting-Paket eines externen Dienstleisters)

Veröffentlichung von Mitgliederfotos auf der eigenen Webseite

Beitragsverwaltung

Lohnabrechnung (über einen externen Dienstleister)

Quelle: https://www.lda.bayern.de

Was bedeutet das für Vereine?

	Ja	Nein
Muss ein DSB vom Verein benannt werden?		X
Ist ein Verarbeitungsverzeichnis erforderlich?	X	
Ist eine DS Verpflichtung für Beschäftigte durchzuführen?	X	
Bestehen irgendwelche Informationspflichten?	X	
Gibt es eine Anforderung zur Datenlöschung?	X	

Quelle: https://www.lda.bayern.de

Was bedeutet das für Vereine?

	Ja	Nein
Müssen die Daten besonders gesichert werden?		X
Ist ein Vertrag zur Auftragsverarbeitung notwendig?	X	
Müssen bestimmte Vorfälle gemeldet werden?	X	
Muss eine DSFA vom Verein durchgeführt werden?		X
Besteht eine Ausschilderungspflicht bezüglich VÜ?	X	

Quelle: https://www.lda.bayern.de

Was bedeutet das für Beherbergungsbetriebe?

Betrieb der Webseite

Marketing

Gästeverwaltung

Finanzbuchhaltung

Lohnabrechnung

Personalverwaltung

Quelle: https://www.lda.bayern.de

Was bedeutet das für Beherbergungsbetriebe?

	Ja	Nein
Muss ein DSB vom Betrieb benannt werden?		X
Ist ein Verarbeitungsverzeichnis erforderlich?	X	
Ist eine DS Verpflichtung für Beschäftigte durchzuführen?	X	
Bestehen irgendwelche Informationspflichten?	X	
Gibt es eine Anforderung zur Datenlöschung?	X	

Quelle: https://www.lda.bayern.de

Was bedeutet das für Beherbergungsbetriebe?

	Ja	Nein
Müssen die Daten besonders gesichert werden?		X
Ist ein Vertrag zur Auftragsverarbeitung notwendig?	X	
Müssen bestimmte Vorfälle gemeldet werden?	X	
Muss eine DSFA vom Betrieb durchgeführt werden?		X
Besteht eine Ausschilderungspflicht bezüglich VÜ?	X	

Quelle: https://www.lda.bayern.de

Was bedeutet das für den Handel?

Abwicklung von EC und Kreditkartenzahlungen über einen Dienstleister

Werbemaßnahmen zur Kundengewinnung und -bindung mittels gelegentlichen Werbebriefaktionen

Betrieb der Webseite

Marketing

Kundenkartenverwaltung

Personalverwaltung

Lohnabrechnung

Quelle: https://www.lda.bayern.de

Was bedeutet das für den Handel?

	Ja	Nein
Muss ein DSB vom Betrieb benannt werden?		X
Ist ein Verarbeitungsverzeichnis erforderlich?	X	
Ist eine DS Verpflichtung für Beschäftigte durchzuführen?	X	
Bestehen irgendwelche Informationspflichten?	X	
Gibt es eine Anforderung zur Datenlöschung?	X	

Quelle: https://www.lda.bayern.de

Was bedeutet das für den Handel?

	Ja	Nein
Müssen die Daten besonders gesichert werden?		X
Ist ein Vertrag zur Auftragsverarbeitung notwendig?	X	
Müssen bestimmte Vorfälle gemeldet werden?	X	
Muss eine DSFA vom Betrieb durchgeführt werden?		X
Besteht eine Ausschilderungspflicht bezüglich VÜ?	X	

Quelle: https://www.lda.bayern.de

Was bedeutet das für Berater?

Kundendaten

Werbemaßnahmen zur Kundengewinnung und -bindung mittels gelegentlicher Werbebriefaktionen

Betrieb der Webseite

Personalverwaltung

Lohnabrechnung

Quelle: https://www.lda.bayern.de

Was bedeutet das für Berater?

	Ja	Nein
Muss ein DSB vom Betrieb benannt werden?		X
Ist ein Verarbeitungsverzeichnis erforderlich?	X	
Ist eine DS Verpflichtung für Beschäftigte durchzuführen?	X	
Bestehen irgendwelche Informationspflichten?	X	
Gibt es eine Anforderung zur Datenlöschung?	X	

Quelle: https://www.lda.bayern.de

Was bedeutet das für Berater?

	Ja	Nein
Müssen die Daten besonders gesichert werden?		X
Ist ein Vertrag zur Auftragsverarbeitung notwendig?	X	
Müssen bestimmte Vorfälle gemeldet werden?	X	
Muss eine DSFA vom Betrieb durchgeführt werden?		X
Besteht eine Ausschilderungspflicht bezüglich VÜ?	X	

Quelle: https://www.lda.bayern.de

Was bedeutet das für Unternehmer im Gesundheitswesen?

Betrieb der Webseite

Patientenverwaltung

Abrechnung

Terminverwaltung

Personalverwaltung

Lohnabrechnung

Quelle: https://www.lda.bayern.de

Was bedeutet das für Unternehmer im Gesundheitswesen?

	Ja	Nein
Muss ein DSB vom Betrieb benannt werden?		X
Ist ein Verarbeitungsverzeichnis erforderlich?	X	
Ist eine DS Verpflichtung für Beschäftigte durchzuführen?	X	
Bestehen irgendwelche Informationspflichten?	X	
Gibt es eine Anforderung zur Datenlöschung?	X	

Quelle: https://www.lda.bayern.de

Was bedeutet das für Unternehmer im Gesundheitswesen?

	Ja	Nein
Müssen die Daten besonders gesichert werden?		X
Ist ein Vertrag zur Auftragsverarbeitung notwendig?		X
Müssen bestimmte Vorfälle gemeldet werden?	X	
Muss eine DSFA vom Betrieb durchgeführt werden?		X
Besteht eine Ausschilderungspflicht bezüglich VÜ?	X	

Quelle: https://www.lda.bayern.de

Und morgen auf der Arbeit
Alltagssituationen und Datenschutz

Zum Sensibilisieren für Sie!

Alltagssituationen Vertrieb

Situation:

Während eines Kundentelefonats das kurz vor Dienstschluss stattfand haben Sie Name und Inhalte des Telefonats schriftlich auf in einem Notizblock aufgenommen. Da Sie es eilig haben, lassen Sie alles an Ihrem Arbeitsplatz liegen und fahren nach Hause.

Ist diese Vorgehensweise korrekt?

Antwort: Nein, hier müssen Sie die Clean Desk Policy berücksichtigen

Alltagssituationen Marketing

Situation:

Sie wollen Kunden und Interessenten zum Besuch Ihres Standes auf einer Messe auffordern. Welche Interessenten und Kundendaten dürfen Sie für Marketingzwecke unter welchen Umständen verwenden?

Dürfen Sie explizit Interessenten einladen, die Sie sich „nur“ für ihren Newsletter angemeldet haben?

Antwort: Nein, da die E-Mail Einwilligung zweckgebunden ist, benötigen Sie für jeden Zweck eine separate Einwilligung.

Alltagssituationen Marketing

Situation:

Sie möchten ein postalisches Mailing an Ihre Kunden schicken und nutzen zum Druck und Versand einen Dienstleister.

Was ist hierbei zu bedenken?

Antwort: Sie benötigen einen Vertrag zur Auftragsdatenverarbeitung

Alltagssituationen Personal

Situation:

Sie stellen neue Mitarbeiter ein.

Müssen ihre Mitarbeiter eine Datenschutzerklärung unterschreiben?

Antwort: Ja, jeder, der Zugriff zu Datenverarbeitungssystemen erhält, mit den personenbezogene Daten verarbeitet können.

Alltagssituationen Personal

Situation:

Sie sagen einem Bewerber ab.

Was machen Sie mit seinen Unterlagen?

Antwort: Um die Daten speichern zu können müssen Sie die Einwilligung des Bewerbers einholen, ansonsten müssen Sie die Daten zeitnah löschen.

Alltagssituationen IT

Situation:

Sie erhalten eine Anfrage welche Technologien verwendet werden und welche Vorkehrung getroffen wurden um die Software vor unerlaubtem Zugriff zu schützen.

Welche Maßnahmen sollten vorhanden sein?

Antwort:
TOMs u.A.

- Benutzerberechtigungssysteme
- Passwortschutz
- Verschlüsselungstechnologien
- Zutrittsbeschränkungen zu sensiblen Bereichen
- Gesicherte Datenverbindungen (Bspw. VPN)

Alltagssituationen Finanzen

Situation:

Sie verwenden ein externes System zur Verarbeitung ihrer Lohnbuchhaltung über einen Schnittstelle.

Benötigen Sie einen Vertrag zur Auftragsdatenverarbeitung?

Antwort: Ja, sofern Sie Daten übermitteln, damit diese von einer externen Firma für Sie verarbeitet werden.

Vielen Dank!

Sie haben Fragen oder benötigen Unterstützung? Wir unterstützen Sie gern!

Ihr Ansprechpartner:
Magnus v. Kunhardt
Leiter Marketing und Vertrieb

Riscreen GmbH
Hauptplatz 37
85276 Pfaffenhofen
Tel: +49 171 3899982