Wie gut sind Ihre Datenschutzmaßnahmen?

In einer kurzen Präsentation möchte ich Ihnen das Thema „Datenschutz“ ein wenig näher bringen.

Ein paar Hintergrundinformationen:
Datenschutz gibt es schon lange. Sehr lange!
Das Hessische Datenschutzgesetz trat 1970 In Kraft und gilt als das erste Datenschutzgesetz überhaupt und weltweit.
Die erste Version des Bundesdatenschutzgesetzes (BDSG) in Deutschland wurde 1977 verabschiedet.
Und 1983 wurde „Das Recht auf informationelle Selbst-bestimmung“ in das Deutsche Grundgesetz übernommen.

Seit 2018 gibt es die DSGVO, die europaweit gilt, ergänzt vom neuen Bundesdatenschutzgesetz (BDSG-neu) und für jeden Unternehmen, Verein, jeder Praxis, Kanzlei und öffentlicher Stelle genau festlegt, wie mit persönlichen Daten zu verfahren ist.

Aber was sind denn überhaupt „persönliche Daten“?

Ganz einfach:
Alles, was in irgendeiner Form Rückschlüsse auf eine Person zulässt. Sowohl digital, als auch analog.
Natürlich sind das in erster Linie Name und Adresse, sowie Geburtsdatum.
Aber auch Telefonnummern, Kontoverbindungen, Steuernummern, KFZ-Kennzeichen, Verträge, Kreditkarteninformationen, Vereins- und Religionszugehörigkeit, Bilder, und noch einiges mehr gehören zu den persönlichen Daten.

Und Sie als „Verantwortlicher“ eines Unternehmens oder ähnlichem sind dafür zuständig, alle Maßnahmen zu treffen, um die persönlichen Daten Ihrer Mitarbeiter, Kunden, Partner und so weiter wirkungsvoll zu schützen.

Sind Sie dem gewachsen? Ja? Nein? Sie sind sich unsicher?

Dann wiederhole ich einmal die Frage „Wie gut sind eigentlich Ihre Datenschutzmaßnahmen?“

Und hier mal ein paar Antworten, die ich standardmäßig auf diese Frage erhalte:

„Ich shredder alle alten Papiere.“

„Meine Mitarbeiter wissen, dass sie keine Interna verraten dürfen.“

„Ich verarbeite gar keine persönlichen Daten.“

„Darum kümmert sich mein IT-Dienstleister.“

„Ich muss mich gar nicht darum kümmern, weil wir weniger als zwanzig Mitarbeiter sind.“

„Alles gut, ich habe eine Datenschutzerklärung auf meiner Webseite.“

„Mir passiert schon nichts.“

Klären wir doch erstmal die Frage „Was ist eigenlich genau unter >Datenschutz< zu verstehen?“

Das Grundgesetz der Bundesrepublik Deutschland (GG) regelt in Artikel 2, Absatz 1 in Verbindung mit Artikel 1, Absatz 1 das Recht auf informationelle Selbstbestimmung.
Dies bedeutet, dass jeder das Recht hat, über die Preisgabe und Verwendung seiner personenbezogenen Daten selbst zu bestimmen.
Dieses Recht ist Teil des allgemeinen Persönlichkeitsrechts und schützt die Person vor den Risiken automatisierter Daten-verarbeitung.

Und um dieses Recht wahrnehmen zu können, muss die Person unter anderem ja auch wissen, wo von wem welche Daten hinterlegt wurden und wofür sie genutzt werden.

Damit nicht jede Behörde, jeder Verein oder jedes Unternehmen für sich selbst entscheidet, wie dieses Gesetz umzusetzen ist, gibt es die „DSGVO“, die Datenschutzgrund-verordnung.

In dieser Verordnung ist genau geregelt, wie mit persönlichen Daten umgegangen werden **muss**.
(Dazu später mehr)

Jetzt ist schon klar, dass >Datenschutz< nicht gleich >Datensicherheit< ist.

Und somit ist nicht Ihr IT-Dienstleister für den Datenschutz zuständig, sondern nur für einen kleinen Teil davon, der Datensicherheit der persönlichen Daten, die Sie verarbeiten.

Aber wer ist denn jetzt für den Datenschutz verantwortlich?
Ganz klar: „**SIE**“!
Die Geschäftsführung, der Inhaber.
(Auch das ist in der DSGVO klar bestimmt)

Natürlich können Sie Mitarbeiter oder externe Dienstleister verpflichten, sich um Ihren Datenschutz zu kümmern.

Aber verantwortlich sind und bleiben nur SIE!

Und SIE zahlen auch die nicht unerheblichen Strafen bei Datenschutzverstößen und Datenschutzverletzungen.
(Auch dazu später mehr)

Aber für was genau hat der Gesetzgeber Sie denn jetzt verantwortlich gemacht?

Sie sind verantwortlich für die Einhaltung der DSGVO, die den Umgang mit persönlichen Daten wie folgt beschreibt:

Jeder Verantwortliche muss die Einhaltung der im Artikel 5 DSGVO aufgeführten Rechtsgrundsätze (Rechtmäßigkeit der Verarbeitung nach Treu und Glauben, Transparenz, Zweck-bindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität, Vertraulichkeit und Rechenschaftspflicht) gewährleisten.

Rechtmäßigkeit:
Die Verarbeitung personenbezogener Daten muss auf einer Rechtsgrundlage beruhen, wie z.B. einer Einwilligung, einem Vertrag, einer gesetzlichen Verpflichtung oder einem öffentlichen Interesse. (Nicht nur „einfach so“)

Transparenz:
Die Betroffenen müssen über die Verarbeitung ihrer Daten informiert werden, z.B. über den Zweck der Verarbeitung, die Art der Daten und die Speicherdauer.

Zweckbindung:
Die Daten dürfen nur für den Zweck verarbeitet werden, für den sie erhoben wurden, und nicht für andere, nicht kompatible Zwecke.

Datenminimierung:
Es dürfen nur so viele Daten verarbeitet werden, wie für den jeweiligen Zweck unbedingt erforderlich sind.

Richtigkeit:
Die Daten müssen richtig und immer auf dem neuesten Stand sein.

Speicherbegrenzung:
Die Daten dürfen nur so lange gespeichert werden, wie es für den Zweck der Verarbeitung erforderlich ist. Und nicht länger!

Integrität und Vertraulichkeit:
Die Daten müssen sicher und geschützt vor unbefugtem Zugriff und Weitergabe sein. (Datensicherheit)

Rechenschaftspflicht:
Die Verantwortlichen müssen nachweisen können, dass sie die DSGVO einhalten. (Vorgeschriebene Dokumentationen)

Die DSGVO legt auch fest, dass die Verarbeitung von Daten auf bestimmten Rechtsgrundlagen erfolgen muss, wie z.B. Einwilligung, Vertrag, Rechtsgrundlage, oder öffentliche Interessen.

Aber von wessen Daten sprechen wir hier eigentlich?

Kurze Antwort: „Von jedem!“

Ausführliche Antwort:

Oftmals glauben die Verantwortlichen, dass die DSGVO sich nur auf die personenbezogenen Daten von Kunden bezieht.

Aber das ist absolut falsch:
Auch die Daten, die Sie von Mitarbeitern, ehemaligen Mitarbeitern, Bewerbern, Subunternehmen, Freelancern, Partnern usw. erfasst haben, fallen unter die DSGVO!

Und für jeden einzelnen gelten andere Bedingungen.

Auf der nächsten Seite führe ich ein paar Schlagworte auf und bitte Sie, mal nachzudenken, welche davon Ihnen bekannt vorkommen.

- Datenschutz- und Geheimhaltungsverpflichtung "Freelancer"
- Einwilligung in die Veröffentlichung von Foto- und Videoaufnahmen
- Verpflichtung zur Vertraulichkeit
- Datenschutzhinweise für Beschäftigte
- Leitlinie zu Datenschutz & Informationssicherheit
- Richtlinie zum Datenschutz (für Beschäftigte)
- Richtlinie für mobiles Arbeiten und Home-Office
- Videoüberwachung - Dokumentation
- Technische und organisatorische Maßnahmen (ToM)
- Verzeichnis der Verarbeitungstätigkeiten
- Datenschutzhinweise für Internetpräsenz
- Vertrag zur Auftragsverarbeitung

Kommen wir jetzt mal dazu, uns zu überlegen, ob Ihnen überhaupt etwas passieren kann.

Salopp ausgedrückt:
Wenn Sie meinen „Mir passiert schon nichts“, bleibt mir nur, Ihnen viel Glück zu wünschen.

Allein im Jahr 2020 kam es zu über 700.000 Angriffen auf kleine Unternehmen, die einen Gesamtschaden von 2,8 Milliarden US-Dollar verursachten.
Fast 40 % der kleinen Unternehmen gaben an, dass sie durch einen Angriff wichtige Daten verloren haben.

„Cybersecurity Ventures“ prognostiziert, dass bis 2031 alle 2 Sekunden ein Ransomware-Angriff einen Verbraucher oder ein Unternehmen treffen wird, was 43.200 Angriffen pro Tag entspricht. Im Jahr 2021 war es noch alle 11 Sekunden so, was etwa 7.850 Angriffen pro Tag entspricht.

Allerdings entsteht den Unternehmen der größte, bzw. häufigste Schaden noch nicht einmal durch Datenschutzverletzungen, sondern durch gemeldete Datenschutzverstöße.

Was ist jetzt der Unterschied zwischen einer „Datenschutzverletzung“ und einem „Datenschutzverstoß“?

Bei einer Datenschutzverletzung sprechen wir davon, dass …

… persönliche Daten entweder nicht mehr verfügbar sind (kompletter Zusammenbruch der Speicherung oder Ramsonsoftwareangriff),

… oder persönliche Daten in „fremde Hände“ gefallen sind (Weitergabe, Hackerangriff, unberechtigter Zugriff, etc.)

… oder persönliche Daten unberechtigt verändert wurden (Hackerangriff, Fahrlässigkeit von Mitarbeitern)

Eine verantwortungsvoll geführte IT-Administration kann das Risiko einer Datenschutzverletzung deutlich minimieren. Wenn der Verantwortliche darüber hinaus die Vorschriften der DSGVO eingehalten hat, kann man davon ausgehen, dass sich der Schaden begrenzen lassen kann.

Ein Datenschutzverstoß allerdings liegt schon in dem Moment vor, in dem Sie gegen eine Vorschrift der DSGVO verstoßen.

Und 90% der gemeldeten Datenschutzverstöße gehen auf Meldungen von unzufriedenen Mitarbeitern, Ex-Mitarbeitern oder Mitbewerbern zurück!

So würde es z. B. schon reichen, wenn Sie einen Mitarbeiter entlassen und dieser der zuständigen Stelle meldet, dass er niemals Informationen darüber erhalten hat, was mit seinen persönlichen Daten passiert. (Speicherort, Speicherdauer, etc.)

Und solche Datenschutzverstöße können richtig ins Geld gehen.

Ein Beispiel:
Für das Nichtaushändigen oder das Nichtzurverfügungstellen der „Datenschutzhinweise für Beschäftigte“ droht bei einem Vorjahresumsatz von unter 1.000.000,- € ein Bußgeld von mindestens 3.000,- € und höchstens 11.700,- €.

Pro Fall!

Von der betroffenen Person kann unter Umständen zusätzlich eine Schadensersatzforderung gestellt werden, auch wenn kein materieller Schaden entstanden ist!

Und da es nach einer Meldung einer betroffenen Person immer zu Prüfungen seitens des Gesetzgebers kommt, kann Ihr finanzieller Schaden noch erheblich höher ausfallen.

Und somit komme ich wieder auf meine Frage nach **IHREM** Datenschutz und den Antworten, die ich so oft erhalte, zurück.

„Ich shredder alle alten Papiere.“ **Und das soll reichen?**

„Meine Mitarbeiter wissen, dass sie keine Interna verraten dürfen.“ **Haben Sie das rechtskonform schriftlich?**

„Ich verarbeite gar keine persönlichen Daten.“ **Doch!**

„Darum kümmert sich mein IT-Dienstleister.“ **Nein, das kann er gar nicht!**

„Ich muss mich gar nicht darum kümmern, weil wir weniger als zwanzig Mitarbeiter sind.“ **Doch, denn das ist keine Frage der Anzahl der Mitarbeiter!**

„Alles gut, ich habe eine Datenschutzerklärung auf meiner Webseite.“ **Diese gilt nur für Ihre Internetseite!**

„Mir passiert schon nichts.“ **Dann viel Glück!**

Und damit sind wir fast am Ende der kleinen Präsentation angelangt.

Ich hoffe, ich konnte Ihnen einen kleinen Überblick darüber verschaffen, wie wichtig Datenschutzmaßnahmen auch in Ihrem Unternehmen sind.

Wenn Sie jetzt der Meinung sind, dass Datenschutz richtig und wichtig ist, weil jeder Mensch das Recht hat, zu wissen, was mit seinen Daten geschieht und dass mit diesen Daten sorgfältig umgegangen werden muss, würde mich das sehr freuen.

Denn das ist der Grund, warum ich mich für den Datenschutz einsetze.

Auch mich ärgern die vielen Werbemails, Anrufe von obskuren Unternehmen und dergleichen.
Und diese resultieren ausschließlich aus einem zu sorglosen Umgang mit persönlichen Daten.

Und zuletzt: Was können SIE jetzt tun?

Gehen Sie in sich.

Überlegen Sie sich für ihr Unternehmen, wieweit Sie die Vorgaben der DSGVO umsetzen oder ob da Verbesserungs-potenzial besteht.

Und wenn, ob Sie das selbst „stemmen“ möchten und ob Sie die finanziellen und personellen Ressourcen dafür haben.

Oder ob Sie sich professionelle Hilfe in Form eines externen Datenschutzbeauftragten ins Boot holen möchten.

Ein interner oder externer Datenschutzbeauftragter ist übrigens gesetzlich vorgeschrieben, wenn in Ihrem Betrieb mehr als zwanzig Personen dauerhaft mit der Verarbeitung personen-bezogener Daten beschäftigt sind; und/oder wenn Sie besondere Kategorien personenbezogener Daten verarbeiten.

Ich danke Ihnen für Ihre Aufmerksamkeit und stehe Ihnen natürlich für weitere Fragen gerne zur Verfügung.

IT-Beratung Frank Berger / Berliner Str. 29 / 53919 Weilerswist
www.IT-Beratung-Berger.de / IT-Beratung@EdvBerger.com
+49 (0)174 / 3 65 65 31

Qualifikationen:

TÜV-zertifizierter Datenschutzbeauftragter

TÜV-zertifizierter IT-Security-Beauftragter

Zertifizierte Fachkraft laut §15 HinSchG

Weitere Leistungen:

E-Rechnung / Internet / HinSchG / BFSG / Cyberversicherung