Die DSGVO und Ihre Auswirkungen auf Ihr Unternehmen
(Unstrukturierte Daten im Unternehmen und deren Risiken)

I. Die DSGVO – wichtige Zahlen und Fakten und ausgewählte Anforderungen

I. 1. Zahlen und Fakten

Die DSGVO EU Datenschutz Grundverordnung oder auch GDPR European General Data Protection ist am 27.04.2016 als direkt anwendbares Recht in Kraft getreten.
Bis zum 25.05.2018 wurde eine Übergangsfrist für die Verordnung (679EU http://eur-lex.europa.eu) vereinbart um den Unternehmen Zeit zu geben, sich auf das neue Regelwerk einzustellen. Ferner um im Gültigkeitsraum EU und EWR den nationalen Gesetzgebern an einigen Stellen der Verordnung -sog. Öffnungsklauseln- die Möglichkeit zu geben die Regelungen der Verordnung zu konkretisieren und zu ergänzen. In Deutschland ist die Verabschiedung eines entsprechenden Gesetzes für Frühsommer 2017 geplant. Da die meisten Regelungen für die Unternehmen in der Verordnung abschließend geregelt sind, kann die Anpassung der Unternehmensprozesse bereits jetzt begonnen werden.

Der Anwendungsbereich (Artikel 3.) der Verordnung wird auf alle ganz oder teilweise automatisierten wie auch nichtautomatisierte Datenverarbeitung ausgeweitet, welche EU-Bürger betrifft und personenbezogene Daten selbiger verarbeitet.
Darunter fallen unter anderem auch Trackingdaten das Internetverhalten diesen Personenkreis betreffend. Analog gilt die Anwendung bei Warenangeboten in Online-Shops und Suchdiensten, welche personenbezogene Daten von EU Bürgern erheben. Dieser Sachverhalt ist losgelöst davon zu sehen ob eine Zahlung zu leisten ist oder nicht. Der Aufenthalt in der EU ist für die Anwendung ausreichend, was z.B. auch Touristen oder Fremdarbeiter in den Schutz der DSGVO einbezieht, wenn in Deutschland ansässige Firmen Ihre Daten verarbeiten.

I.2. Ausgewählte Anforderungen

I.2.1. Anforderungen an das Datenmanagement

Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht.

Artikel 5. - Grundsätze für die Verarbeitung personenbezogener Daten

Unternehmen im Geltungsbereich der DSGVO sind rechenschaftspflichtig über die Einhaltung folgender Punkte. Personenbezogene Daten müssen:

a) auf rechtmäßige Weise, nach Treu und Glauben und für die betroffene Person nachvollziehbar (Transparenz)
b) für einen eindeutigen und legitimen Zweck erhoben (Zweckbindung)
c) dem Zweck angemessen und beschränkt (Datenminimierung)
d) sachlich richtig und auf dem neuesten Stand (Richtigkeit)
e) in einer die Identifizierung der betroffenen Person nur so lange ermöglichenden Form gespeichert werden, wie für die Verarbeitung bzw. ein

f) öffentliches Interesse an der Archivierung besteht. (Speicherbegrenzung) ggf. besteht die Möglichkeit der Pseudonymisierung Artikel 5 und /oder Anonymisierung.
g) Ferner müssen diese in einer Weise verarbeitet werden, die eine angemessene Sicherheit einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung wie auch unbeabsichtigtem Verlust, Zerstörung und Schädigung durch geeignete Maßnahmen sicherstellt. (Integrität und Vertraulichkeit)

Artikel 6 /7 - Rechtmäßigkeit und Einwilligung

Von einer rechtmäßigen Datenverarbeitung kann nur gesprochen werden, wenn ein Erfordernis zur Vertragserfüllung, rechtlicher Verpflichtungen, ein lebenswichtiges Interesse, ein öffentlichen Interesse oder eine Einwilligung zur Verarbeitung der personenbezogenen Daten für einen oder mehrere Zwecke gegeben wurde.

Die Einwilligung muss in leicht verständlicher Sprache und von anderen Sachverhalten losgelöst erbeten und auf Verlangen nachgewiesen werden. Die Einwilligung kann jederzeit eingeschränkt oder ganz wiederrufen werden. Dies muss gleichsam Einfach wie die Erteilung erfolgen können. Bei Zweckänderung der Datenverarbeitung ist das Unionsrecht bzw. das nationale Recht welchem der für diese Daten Verantwortliche unterliegt maßgebend. Die beabsichtigte Weiterverarbeitung geht einher mit einer Prüfung ob der neue Zweck in Verbindung mit dem Erhebungszweck steht.
Der Verantwortliche für diese Daten hat die Rechtmäßigkeit und mögliche Folgen für die betroffene Person im Einzelfall zu prüfen und ggf. behördliche Hilfe vor der Verarbeitung in Anspruch zu nehmen. Es müssen der betroffenen Person geeignete Garantien, wozu Verschlüsslung oder Pseudonymisierung gehören kann gegeben werden.

Artikel 12 – 14 - Datenerhebung

Es sind geeignete Maßnahmen zu treffen um betroffenen Personen alle Informationen und Mitteilungen die sich auf die Verarbeitung beziehen in verständlicher und leicht zugänglicher Form und einer klaren, einfachen Sprache zu übermitteln. Im Zuge der Erhebung besteht Informationspflicht zu allen relevanten Punkten im Zusammenhang mit der Erhebung.

Diese sind unter anderem:
- Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten (wenn vorhanden)
- Zweck der Erhebung und Rechtsgrundlage
- Die Absicht Daten an ein Drittland bzw. weitere Organisation zu geben
- Dauer der Speicherung und ggf. die Kriterien hierfür
- Hinweis auf das Beschwerderecht bei einer Aufsichtsbehörde
- Ob die Bereitstellung der personenbezogenen Daten gesetzlich vorgeschrieben ist
- Ob ein Verfahren wie Profiling zur Anwendung kommen soll mit den Auswirkungen

- Hinweis auf das Recht auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Widerspruchsrecht gegen die Verarbeitung, Recht auf Datenübertragbarkeit oder Löschung.
- Wird eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu welchem diese erhoben wurden angestrebt, sind vor dieser alle maßgeblichen Informationen zu diesem Zweck und die zutreffenden, vorstehenden Informationen durch den Verantwortlichen zur Verfügung zu stellen.

Der Verantwortliche hat den betroffenen Personen die Ausübung Ihrer Rechte zu erleichtern. Der Verantwortliche hat der betroffenen Person in der Frist eines Monates nach Eingang des Antrages mit der Möglichkeit der Verlängerung auf max. drei Monate die im Antrag geforderten Informationen zur Verfügung zu stellen. Diese Informationen werden unentgeltlich zur Verfügung gestellt. Wird der Verantwortliche ohne ausreichend Begründung nicht tätig, muss Er die betroffene Person über Ihr Recht der Beschwerde bei der Aufsichtsbehörde unverzüglich unterrichten.

Folgende Rechte stehen dem betroffenen Personenkreis zur Verfügung:

Artikel 15 - Auskunftsrecht der betroffenen Person
Die betroffene Person hat das Recht eine Bestätigung über die Verarbeitung personenbezogener Daten zu verlangen. Diese Information soll u.a. enthalten:
Den Zweck, ev. Kategorien der Daten, Empfänger und Nutzer der Daten inkl. Land, geplante Speicherdauer und eine Kopie der Daten welche Gegenstand der Verarbeitung sind.

Artikel 16 - Recht auf Berichtigung
Die betroffene Person hat das Recht auf unverzügliche Berichtigung sie betreffender unrichtiger Daten. Analog gilt gleiches für die Vervollständigung unvollständiger Daten.

Artikel 17 - Recht auf Löschung („Recht auf Vergessenwerden“)
Die betroffene Person hat das Recht zu verlangen, dass sie betreffende Daten unverzüglich gelöscht werden, sofern einer der folgenden Gründe vorliegt:

- Die Daten sind für den Erhebungszweck nicht mehr nötig
- Wiederruf der Einwilligung bei Fehlen einer anderweitigen Rechtsgrundlage
- Wiederspruch gegen die Verarbeitung ohne das vorrangige berechtigte Gründe für diese vorliegen.
- Die Daten wurden unrechtmäßig verarbeitet
- Die Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben
- Die Löschung dient der Erfüllung einer rechtlichen Verpflichtung

Die Löschung kann auch bei Veröffentlichung der Daten unter Berücksichtigung der verfügbaren Technologie die Ergreifung geeigneter Maßnahmen zur Löschung aller Links zu diesen personenbezogenen Daten oder Kopien verlangt werden.

Ausnahmen sind nur im rechtlichen und öffentlichen Interesse angesiedelt.

Artikel 18 - Recht auf Einschränkung der Verarbeitung
Die betroffene Person hat das Recht die Einschränkung der Verarbeitung zu verlangen, wenn
eine der nachstehenden Voraussetzungen gegeben ist:

- Die Richtigkeit der Daten wird bestritten – für die Dauer der Prüfung
- Die Verarbeitung ist unrechtmäßig, die Daten sollen aber nicht gelöscht werden
- Die Daten für den Zweck der Verarbeitung nicht länger benötigt werden, die betroffene Person diese aber zur Geltendmachung, Ausübung o-ä. von Rechtsansprüchen benötigt

Wurde die Verarbeitung erfolgreich eingeschränkt, dürfen die personenbezogenen Daten zwar gespeichert, aber nur mit Einwilligung der betreffenden Person verarbeitet werden.

Artikel 20 - Recht auf Datenübertragbarkeit

Die betroffene Person hat das Recht, Ihre personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.
Sie darf diese Daten einem anderen Verantwortlichen übermitteln.
Sie kann diese Übertragung auch als direkte Übertragung erwirken.

Hierzu ist anzumerken, dass nur die der Person zugehörige Daten – nicht aber die Daten welche andere Personen auf z.B. Ihrer Social-Media Seite eingestellt haben übertragen werden. Dies würde die Rechte und Freiheiten der anderen Person(en) beeinträchtigen.

Artikel 33 und 34 - Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und die betroffenen Personen

Wer kennt sie nicht? Meldungen wie dieser Tage wieder: Yahoo 500 Millionen Konten gehackt. Immer neue Meldungen schrecken die Verbraucher auf. Das Besondere daran ist der Umstand wie lange die Vorfälle bereits zurückliegen, aber jetzt erst zugegeben wurden.

Mit dieser Praxis macht die DSGVO Schluss:
Im Fall einer Verletzung des Schutzes personenbezogener Daten hat der Verantwortliche unverzüglich und möglichst binnen 72 Stunden nach Kenntnis der Verletzung die zuständige Aufsichtsbehörde zu informieren. Einzige Ausnahme: Wenn die Verletzung nach genauer Abwägung nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
Erfolgt die Meldung nicht in der vorgeschriebenen Zeit, ist eine Begründung beizufügen.

Gemeldet werden muss:

- Die Art der Verletzung des Schutzes der personenbezogenen Daten
- Die Kategorie der Daten
- Die ungefähre Anzahl der betroffenen Datensätze

- Die Kontaktdaten des Datenschutzbeauftragten bzw. Kontaktperson
- Eine Beschreibung der zu erwartenden Folgen durch die Verletzung
- Eine Beschreibung der vorgeschlagenen/ ergriffenen Maßnahmen zur Behebung,
  wie auch der Abmilderung der möglichen nachteiligen Auswirkungen

Alle Schritte und Maßnahmen sind verbindlich für die Aufsichtsbehörde zu dokumentieren.

Geht mit der Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen einher, so sind die betroffenen Personen unverzüglich durch den Verantwortlichen zu informieren.
Diese hat in klarer Sprache die Verletzung, zusätzliche Informationen der Meldung an die Aufsichtsbehörde und Empfehlungen zu beinhalten.
Die Benachrichtigung der betroffenen Personen kann unterbleiben, wenn Sicherheitsvorkehrungen getroffen und auf die betroffenen personenbezogenen Daten angewendet wurden. Diese müssen Personen ohne Befugnis vom Zugriff auf die personenbezogenen Daten ausschließen. Das hohe Risiko darf nach Ergreifen der Maßnahmen nicht länger bestehen. Ist die Benachrichtigung nur durch einen unverhältnismäßigen Aufwand möglich, hat eine öffentliche Bekanntmachung oder ähnlich gelagerte Maßnahme zu erfolgen welche die Betroffenen vergleichbar wirksam informiert. Sollte noch keine Information der betroffenen Personen seitens des Verantwortlichen erfolgt sein, kann dies durch die Aufsichtsbehörde verlangt werden.

Artikel 82 - Haftung und Recht auf Schadensersatz

Jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadensersatz gegen den Verantwortlichen bzw. Auftragsverarbeiter seiner personenbezogenen Daten.

Jeder an der Verarbeitung personenbezogener Daten beteiligte Verantwortliche haftet für Schäden die aus einer nicht mit der Verordnung konformen Verarbeitung entstehen. Für die Haftungsfrage ist der Nachweis ob der Verantwortliche oder Auftragsverarbeiter für den Umstand, durch den der Schaden eingetreten ist, verantwortlich zeichnet von zentraler Bedeutung. Der Nachweis das keinerlei Verantwortung für den Schadensumstand vorliegt wirkt entlastend.
Im Fall das mehrere Verantwortliche oder Auftragsverarbeiter an ein und derselben Verarbeitung beteiligt sind, haftet jeder Verantwortliche oder Auftragsverarbeiter für den gesamten Schaden. Hat ein Verantwortlicher umfänglich Schadensersatz geleistet, kann er diesen anteilig von den an derselben Verarbeitung Beteiligten zurückfordern. Der Gerichtsstand für Verfahren zur Inanspruchnahme des Rechtes auf Schadensersatz befindet sich am für die genannten Rechtsvorschriften zuständigen Gericht des Mitgliedstaats.

Artikel 83 - Allgemeine Bedingungen für die Verhängung von Geldbußen

Die Aufsichtsbehörden verfügen über ein breites Spektrum an Möglichkeiten zur Durchsetzung der DSGVO. Diese wären z.B.:

- Unangekündigte Überprüfungen auch bei zertifizierten Unternehmen
- Abgabe eines Hinweises auf Versäumnisse
- Abgabe einer Warnung bei problematischen Umständen die zu einem Verstoß gegen die DSGVO führen können
- Verwarnung wenn durch Verarbeitungsvorgänge gegen die DSGVO verstoßen wird
- Die Verantwortlichen anzuweisen Abhilfe zu schaffen:
    - Anträgen von betroffenen Personen auf Ausübung ihnen zustehender Rechte zu entsprechen.
    - Verarbeitungsvorgänge ggf. auf festgelegte Weise innerhalb einer festgelegten Frist in Einklang mit der Verordnung zu bringen
    - Die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen zu benachrichtigen
- Eine vorübergehende oder endgültige Beschränkung der Verarbeitung bis hin zu einem Verbot zu verhängen
- Eine Zertifizierung zu widerrufen bzw. die Zertifizierungsstelle anzuweisen dies zu tun
- Eine Geldbuße zu verhängen, auch zusätzlich zu oder anstelle der vorstehend genannten Maßnahmen, je nach Sachlage des Einzelfalls

Für die Verhängung von Bußgelder gilt, dass die jeweilige Aufsichtsbehörde sicher zu stellen hat, dass die Verhängung für Verstöße gegen die DSGVO in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

Im Fall der Verhängung einer Geldbuße und deren Betrag wird in jedem Einzelfall folgendes berücksichtigt:

- Art, Schwere und Dauer des Verstoßes in Verbindung des Zweck der betreffenden Verarbeitung, wie auch der Anzahl der betroffenen Personen und des Ausmaßes des von diesen erlittenen Schadens
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
- Alle vom Verantwortlichen getroffenen Maßnahmen zur Schadensminderung
- Grad der Verantwortung des Verantwortlichen unter Berücksichtigung der durch diese getroffenen technischen und organisatorischen Maßnahmen
- Historie an Verstößen des Verantwortlichen
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde bei der Abhilfe
- Art und Kategorie der betroffenen Daten
- Art und Weise, wie der Verstoß der Aufsichtsbehörde zur Kenntnis gelangt ist
- Einhaltung von früher gegen den Verantwortlichen verhängte Maßnahmen
- Einhaltung von genehmigten Verhaltensregeln oder Zertifizierungsverfahren
- Alle weiteren erschwerenden oder mildernden Umstände im jeweiligen Fall wie eventuell erlangte finanzielle Vorteile oder vermiedene Verluste

Bei Verstößen gegen u.a. nachfolgende Bestimmungen werden Geldbußen bis zu 10.000.000 EUR oder im Fall eines Unternehmens von bis zu 2% seines gesamten

weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahr verhängt, je nachdem welcher Betrag höher ist.

- **Allgemeine Pflichten:**
  Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft (Artikel 8), Verarbeitung, für die eine Identifizierung der betroffenen Personen nicht erforderlich ist (Artikel 11), Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25), Gemeinsam für die Verarbeitung Verantwortliche (Artikel 26), Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern (Artikel 27), Auftragsverarbeiter (Artikel 28), Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters (Artikel 29), Verzeichnis von Verarbeitungstätigkeiten (Artikel 30), Zusammenarbeit mit der Aufsichtsbehörde (Artikel 31)

- **Sicherheit personenbezogener Daten:**
  Sicherheit der Verarbeitung (Artikel 32), Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Artikel 33), Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Artikel 34)
- **Datenschutz-Folgeabschätzung und vorherige Konsultation (Artikel 35 u. 36)**
- **Datenschutzbeauftragter:**
  Benennung eines Datenschutzbeauftragten (Artikel 37), Stellung des Datenschutzbeauftragten (Artikel 38), Aufgaben des Datenschutzbeauftragten (Artikel 39)
- **Verhaltensregeln und Zertifizierung:**
  Zertifizierung (Artikel 42), Zertifizierungsstellen (Artikel 43), Überwachung der genehmigten Verhaltensregeln (Artikel 41.Abs. 4)

Bei Verstößen gegen u.a. nachfolgende Bestimmungen werden Geldbußen bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahr verhängt, je nachdem welcher Betrag höher ist.

- **Grundsätze:**
  Grundsätze für die Verarbeitung personenbezogener Daten (Artikel 5), Rechtmäßigkeit der Verarbeitung (Artikel 6), Bedingungen für die Einwilligung (Artikel 7), Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 9)
- **Rechte der betroffenen Person – Transparenz, Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten:**
  Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person (Artikel 12), Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Artikel 13), Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Artikel 14), Auskunftsrecht der betroffenen Person
  (Artikel 15)

- **Berichtigung und Löschung:**
  Recht auf Berichtigung, Recht auf Löschung ("Recht auf Vergessenwerden"), Recht auf Einschränkung der Verarbeitung, Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit (Artikel 16-20)
- **Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall:**
  Widerspruchsrecht (Artikel 21), Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (Artikel 22)
- **Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen:**
  Allgemeine Grundsätze der Datenübermittlung, Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses, Datenübermittlung vorbehaltlich geeigneter Garantien, Verbindliche interne Datenschutzvorschriften, Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung, Ausnahmen für bestimmte Fälle (Artikel 44-49)

Gerne steht Ihnen die CCF AG für weiterführende Gespräche zum Thema und Ihrer ganz persönlichen Sachlage zur Verfügung. Beachte Sie aber bitte: Wir leisten weder juristische Beratung, noch haben unsere Ausführungen zur DSGVO einen verbindlichen Charakter. Diese dienen ausschließlich dem Zweck eines ersten Verständnisses der Thematik als Basis für die Betrachtung nachstehender Lösungsansätze.

II. Betrachtung der Problemfelder zur Umsetzung der Verordnung

II.1 Datenwachstum und Datenzusammensetzung

Die Datenmenge weltweit steigt rund alle zehn Jahre um den Faktor siebzehn an. An Berechnungen wie diese von der renommierten amerikanischen Berkeley-Universität haben wir uns längst gewöhnt. Eine Verdopplung der Datenmenge alle zwei bis drei Jahre scheint hinnehmbar und in Zeiten des andauernden Preisverfalls bei Speichermedien kaufmännisch akzeptabel. Ist das wirklich so?

Neu ist in diesem Zusammenhang die Erkenntnis erster Unternehmen, lange Zeit die Auswirkungen und Gefahren aus diesem Fakt schlichtweg ignoriert zu haben. Unstrukturierte Daten stehen an erster Stelle der Ursachen für den immer schnelleren Anstieg von Unternehmensdaten. In den meisten Unternehmen liegt der prozentuale Anteil strukturierter Daten in Datenbanken resultierend aus den im Unternehmen eingesetzten Applikationen unter 50%. Der Rest verteilt sich auf Office-Daten, Mail, PDF, Audio, Video, Zeichnungen um nur einige zu nennen. Eine von Veritas bei Vanson Browne als unabhängiges Forschungsunternehmen in Auftrag gegebene Studie belegt eindeutig, wie sich die „Datenberge“ deutscher Unternehmen im Schnitt zusammensetzen:

- 15% der Daten sind als bekannte unternehmenskritische Daten klassifiziert.
- 19% der Daten gelten als Redundante, veraltete und triviale Daten (ROT Data). Diese Daten sind klassifiziert, besitzen aber i.d.R. keinen geschäftlichen Nutzen.

- 66% der Daten gelten als sogenannte Dark Data. Bei diesen Daten ist keine Klassifizierung vorhanden. Es kann sich um unternehmenskritische aber auch um ROT Daten handeln. (Quelle: Veritas, „Der Databerg Report 2016“)

ROT und Dark Data sind hinsichtlich rechtlicher Relevanz an erster Stelle zu sehen. Vereinbarungen, Geschäftsberichte und ähnliche Dokumente werden per E-Mail ausgetauscht. Verträge, Angebote, techn. und kaufm. Details werden als Text- oder PDF Dateien abgelegt. Tabellenblätter, Zeichnungen und zum Beispiel digitale Bewerbungen finden sich an diversen Speicherorten und in diversen Dateiformaten.

Die rechtlichen Risiken für die Unternehmen und deren leitende Angestellte steigen mit jeder Datei ohne klare Zuordnung. Neben der Gefahr der digitalen Amnesie (Diese liegt vor, wenn ein Unternehmen Daten oder Informationen nicht in einer angemessenen Zeit auffinden kann), droht die Unfähigkeit gesetzliche Vorschriften angemessen umzusetzen.

Gesetzliche Vorschriften angefangen vom US-amerikanischen Sarbanes-Oxley-Act, das deutsche Steuerrecht bis hin zum Handelsrecht (HGB), dem Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG) um nur ein paar zu nennen, stellen für sich gesehen bereits vielfältige Anforderungen an das Unternehmen.

Bei all diesen Vorschriften kommt hinzu, dass die am 27.04.2016 als direkt anwendbares Recht verabschiedete und nach einer Übergangsfrist zum 25.05.2018 voll wirksame DSGVO EU- Datenschutz Grundverordnung (GDPR – European General Data Protection) im gleichen Zuge zu beachten ist. Eine gesetzeskonforme Aufbereitung der Unternehmensdaten sollte zudem nicht nur als Erfüllung von Anforderungen gesehen werden. Sie hilft dem betroffenen Unternehmen auch neben den rechtlichen Aspekten auch in folgenden Bereichen:

- Neu- oder Rezertifizierung in Standards wie DIN und ISO
- IT-Governance (Risikomanagement; Compliance….)
- Absicherung der Daten vor internem und externem Datendiebstahl
- Reduzierung der Zeitfenster der Datensicherung und Wiederherstellung
- Reduzierung des Aufwandes der Datenhandhabung und Speicherung
- Durchsetzung von Anordnungen der Unternehmensverwaltung wie Rundschreiben und interne Richtlinien.

Wie sollte sich Ihr Unternehmen diesen vielfältigen Anforderungen stellen und wie können wir als CCF AG Ihnen dabei helfen?

Nun, um es gleich am Anfang zu erwähnen:
Rechtliche Anforderungen, auch die DSGVO sind in Teilen noch nicht wirklich mit praktikablen Handlungsanweisungen ausgestaltet. Eine 100% Lösung wird es aus Gründen stetiger Veränderung nicht geben. Daraus aber eine Verzögerung der

Umsetzung der übrigen Vorschriften herzuleiten, wäre sicher ein riskantes Unterfangen. Vor allem da eine solche Umsetzung ein langwieriger Prozess ist, was oft unterschätzt wird.

Wir können Sie gemeinsam mit unseren Partnern auf dem Weg hin zur Erfüllung der Anforderungen begleiten:

- Eine der Möglichkeiten ist die Verwendung eines prozessorientierten Systems als Gerüst für die Einzellösungen bei der jeder Arbeitsschritt auditierbar, transparent und damit revisionssicher ist.
- Eine weitere Möglichkeit ist die Verwendung optimierter Einzellösungen um die bereits bestehenden Lösungen in Ihrem Unternehmen zu ergänzen. Diese sollten ebenfalls in den einzelnen Schritten dokumentiert und für Zwecke des Nachweises in Audits und Überprüfungen aufbereitet sein.

Nachfolgend geben wir Ihnen einen ersten Abriss über den CCF AG Skill Set und freuen uns bereits jetzt auf vertiefende Gespräche mit Ihnen.

III. 1. Aufarbeitung der Unternehmensdaten

Am Anfang steht die Schaffung von Transparenz, die gezielte Datenbereinigung, Klassifizierung und Verlagerung von Daten.

Um diese und weitere Aufgaben eines „Information Management“ optimal umsetzen zu können, sollten aus unserer Sicht folgende Punkte erfüllt sein:

- Es sollte eine verbindliche Policy geben in welcher zum Beispiel geregelt ist wann welche Daten gelöscht werden.
- Es sollte ein Klassifizierungsframework geben nach welchem die Daten eingestuft werden.
- Es sollte einen Verantwortlichen für diese Themen geben
- Es sollte eine klar für alle erkennbare Festlegung und Zusage durch die Geschäftsleitung diese Themen betreffend geben

Als vordringlichste Aufgabe ist die Analyse und Klassifizierung der unter ROT und Dark Data fallenden Daten zu sehen.
Lösungen wie Data Insight von Veritas zur 2D und 3D Analyse der vorhandenen Daten helfen bei der Datenminimierung, dem Auffinden von Daten und Zugriffen.
Durch den Einsatz der Darstellung von Daten unter verschiedenen Parametern zum Beispiel:
Datenstruktur nach dem letzten Verwendungsdatum und im Anschluss zum Beispiel
Mit einem Alter >3 Jahre und aufgegliedert nach Datentyp um nur ein paar Möglichkeiten zu nennen. Damit lassen sich Problemdaten, unternehmenskritische Daten und Massendaten beispielsweise zur Anonymisierung und Verwendung bei Unternehmensauswertung unterscheiden und entsprechend zuordnen.

III. 2. Datenhandhabung im Unternehmen - Berechtigungsmanagement

Berechtigungen werden in weiten Teilen eines Unternehmens als Aufwertung der eigenen Person und des Ansehens gewertet. Es wundert daher nicht, dass es kaum zur freiwilligen Abgabe selbiger kommt.

Dieses Verhalten in Verbindung mit nicht gelöschten, inflationär vererbten und allgemein erteilten Zugriffsberechtigungen stellt neben den rechtlichen Aspekten eine massive Gefahr für das Unternehmen dar.

Probleme in diesem Umfeld sind unter anderem:

- Datendiebstahl durch Mitarbeiter
- Ransomware bei einem Mitarbeiter mit Auswirkung auf alle Daten auf welche Er Zugriff hat
- Unberechtigte administrative Zugriffe auf Daten (z.B. GL und Personalstamm) sind so gut wie nicht zu erkennen. Dies stellt die Administration unter Umständen unter einen Generalverdacht.
- Mitarbeiter sollten nur die sie betreffenden Daten für die tägliche Arbeit sehen können
- Daten werden fehlerbedingt verlagert und nicht wieder aufgefunden
- Berechtigungen sind meist nur schwerfällig überprüfbar und administrierbar
- Anfragen, Genehmigungen und Änderungen werden nicht dokumentiert
- Eine nachträgliche Dokumentation u.a. für ein DIN /ISO Audit ist kaum möglich und
  hält meist einer Überprüfung nicht stand
- Berechtigungsklassifizierung
- Berechtigungen werden kumulativ vergeben statt angepasst
- Berechtigungen werden mangels Übersichten nicht durch Fachverantwortliche überprüft
- Prozesssicherheit und Prüfbarkeit der Berechtigungen für rechtliche Anforderungen
  und Schutz unternehmenskritischer Daten

Die vorstehende Aufzählung ist nicht als abschließend zu sehen.

Wir als CCF AG helfen Ihnen gerne, die geeignete Lösung zu finden und unterstützen Sie bei der Umsetzung.
Rechtliche Erfordernisse lassen keinen Spielraum. Es besteht aber die Möglichkeit, durch eine entsprechende Auswahl und Planung einen sehr hohen Zusatznutzen zu generieren ohne zusätzliche Kosten zu verursachen. Ein Imageschaden durch Datendiebstahl oder der Verlust von Zertifikaten ist ungleich teurer und wird in seinen Auswirkungen unterschätzt.

III. 3. Sicherung der Unternehmensdaten – Sicherung und Wiederherstellung von Daten

Auf den ersten Blick erscheint dieses Thema keinen so richtigen Bezug zur GS-DVO zu haben.
Dennoch sind die vorhandenen Lösungen in der nahen Zukunft von den Regelungen betroffen.
Der Gesetzgeber hat noch keine klare Anwendungsvorschrift u.a. hinsichtlich des „Recht auf Vergessens“ und den Umgang der betroffenen Daten auf Datensicherungsmedien erlassen.
Hier könnte es zu Erfordernissen einer mehrstufigen Lösung, aber auch unterschiedlichen Aufbewahrungsstrategien kommen.

Ein Vorteil aus Punkt III. 1. kommt hier bereits voll zum Tragen:

- Die verringerte Datenmenge führt zu kürzeren Backup Zeiten und ermöglicht so auch die wichtigen Tests eines Restores, welcher meist aus Zeitgründen ausgelassen wird.
- Die klassifizierten Daten können in optimaler und auf die Inhalte bezogenen Weise gesichert, geschützt und vorgehalten werden.

Es lohnt sich für Sie, bestehende Lösungen mit uns zu besprechen und sich mit unserer Hilfe für zukünftige Anforderungen fit zu machen.
Wir freuen uns auf Ihren Anruf!

Mit freundlichen Grüßen