U n t e r n e h m e n s r i c h t l i n i e DSGVO

Inhaltsangabe **Seite**

2. Übersichtlichkeit Ihrer Website in datenschutzrechtlicher Hinsicht, auch zum Thema „one click“ und datenschutzfreundlichen Voreinstellungen

3. Einwilligungserklärung oder berechtigtes Interesse? Zugleich zum besonderen Schutz von Minderjährigen

4. Ausdrückliche Einwilligungserklärung in Sonderfällen

5. Zweckänderung zwischen erstmaliger Erhebung und späterer Nutzung

V. Datenschutz durch Einsatz informativer Mittel / Dokumentation Richtung Behörde

1. Nachweispflichten im Allgemeinen

2. Das sog. Datenverarbeitungsverzeichnis

3. Was tun bei einem sog. Daten-Leck oder sonstigem Datenverlust?

VI. Erleichterungen in Sachen Nachweispflichten durch Zertifizierung und Verbandsarbeit

1. Zertifizierer

2. Aufsichtsbehördlich genehmigte Verbandsregularien

VII. Zusammenarbeit mit Dritten

1. Kooperation mit sog. Auftragsverarbeitern

2. Datengewinnung bei Dritten

3. Weiterleitung an Dritte

4. „Korrektur-Wasserfall“ Richtung Dritter

5. Dritte im Ausland

VIII. Zum Umgang mit spezifischen Kundenrechten („Rechte-Katalog“) in Sachen Datenschutz

1. Rechte im Einzelnen

2. Reaktionsfristen und Dokumentation

3. Aufbewahrungsfristen

4. Im Zweifel: Prüfung durch Rechtsanwalt

IX. Zum Umgang mit nicht automatisierter Datenverarbeitung, Vermeidung von „Parallel-Administrationen“

X. Zum Umgang mit juristischen Personen

XI. Sonderthema Datenschutz gegenüber Mitarbeitern

XII. Sonderthema Datenschutz-Folgenabschätzung

XIII. Ungeklärte Probleme

Insb. Löschungen!

XIV. Aufsichtsbehörde, Monitoring Rechtsentwicklung, Sonstiges

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html;jsessionid=B236788418B2A295D3B20C7DB300D377.1_cid351

I. Allgemeines

Der vornehmliche Zweck dieser Unternehmensrichtlinie besteht darin, deutlich zu machen, wie wir unser Unternehmen und die in selbigem stattfindenden Arbeits- und Verwaltungsvorgänge sowie in allgemeinerem Sinne die hier vorhandene Organisation in rechtlicher Hinsicht in Übereinstimmung bringen mit den aktuellen Anforderungen des Datenschutzrechts. Namentlichen geht es dabei um jene der Datenschutzgrundverordnung (DSGVO), welche ab dem 25.5.2018 in Geltung sein wird.

Im Vergleich mit der bisherigen Rechtslage, die weitgehend durch das Bundesdatenschutzgesetz (BDSG) bestimmt wurde, bringt die DSGVO insbesondere deutlich erweiterte Pflichten gegenüber unseren Kunden mit sich, aber auch gegenüber den Behörden. Besonders hohe Anforderungen gelten bei sensiblen Daten mit hervorgehobenem Persönlichkeitsbezug wie auch bei grenzüberschreitender Datenverarbeitung mit Bezug zu solchen Ländern, die einen Datenschutz auf EU-Niveau nicht gewährleisten.

Letztlich geht es auch der DSGVO darum, einen sinnvollen Kompromiss zu erreichen zwischen Aspekten des Datenschutzes und demjenigen, was von einem Unternehmen, welches sich marktüblich verhält, insoweit unter Mitwägung des entsprechenden Aufwandes wie seiner geschäftlichen Belange redlicherweise erwartet werden kann.

Unter dem Strich ist effektiver Datenschutz ein Zusammenwirken technischer wie personaler Faktoren, gepaart mit einem kritischen Bewusstsein für die Belange desjenigen, der modernen Datenverarbeitungsmaßnahmen ausgesetzt ist. Zentrale Grundsätze der DSGVO, insbesondere Verfolgung und Festlegung zulässiger Zwecke, Datenminimierung, Speicher(zeit)begrenzung, Integrität und Vertraulichkeit, müssen dabei in unsere unternehmerische Sphäre „übersetzt“ und in der täglichen Routine „gelebt“ werden. Nur so wird die Chance gewahrt, sich sowohl rechtskonform gegenüber dem Betroffenen (z.B. Kunde, Lieferant, sonstige Dritte) zu verhalten als auch einen eventuellen behördlichen Audit beanstandungsfrei (und damit zugleich bußgeldfrei) überstehen zu können.

Wenn im Folgenden von Daten die Rede ist, sind damit personenbezogene Daten im Sinne der DSGVO gemeint.

II. Datenschutz durch Einsatz technischer Mittel

1. Grundsätze

Ein erheblicher Beitrag für einen rechtskonformen Datenschutz liegt darin, als Unternehmen in technischer Hinsicht gut aufgestellt zu sein. Dazu gehört zum einen die inhaltliche Ausgestaltung technischer Verfahren, zum anderen die Unterlegung solcher Verfahren mit einem gewissen Level an Hard- und Software.

(a) Gestaltung von Eingabemasken und anderer Datenabfrageroutinen vor dem Hintergrund von Datenminimierungsanforderungen

Generell dürfen nur jene Daten erhoben werden, welche für Zwecke der Führung unseres Unternehmens nach gutem Marktstandard erforderlich sind. Darin stecken zwei Voraussetzungen: wir müssen ein legitimes Anliegen verfolgen, und um dies in vernünftiger / sinnvoller Weise umzusetzen, können wir auf die Gewinnung bestimmter Daten im diesem Zusammenhang nicht verzichten. Ein Beispiel hierzu: ein Unternehmen U verkauft Maschinen an die Holzwirtschaft, wobei es sich um sehr unterschiedliche Maschinen handelt, je nachdem, ob damit mit einem Nadel- oder Laubwald gearbeitet werden soll. Werden vom Käufer nun nach der Art „seines“ Waldes Daten erhoben /

abgefragt, so ist dies legitim, auch wenn daraus gewisse Rückschlüsse auf seine finanzielle Situation möglich sein könnten, etwa weil Laubwald wertvoller sein könnte als Nadelwald. Um ihm jedoch die „richtigen“ Maschinen anbieten / liefern zu können, ist diese Angabe unentbehrlich und die Erhebung daher zulässig. Etwas anderes wäre es, wenn U – welches noch ein Tochterunternehmen T besitzt, welches mit Jagdsportartikeln handelt – beim Käufer abfragen würde, ob dieser auch Jäger ist, weil diese Angabe für das Geschäft des U irrelevant ist. Unzulässig wäre es hier insbesondere, das eine mit dem anderen in zwingender Weise zu verknüpfen, also dem Käufer nur dann Waldmaschinen zu liefern, wenn er zugleich die Angabe zur Jägereigenschaft machte. Wollte man letzteres per se in Erfahrung bringen, um eventuell auch der Tochtergesellschaft weiteres Geschäft zu „besorgen“, sollte insoweit mit ausdrücklichen Einwilligungslösungen gearbeitet werden (siehe dazu unten Abschnitt IV Nr. 3).

KONKRET müssen wir (letztlich fortlaufend) eine betriebsinterne Analyse dazu zu erstellen, welche Daten wir für unsere Geschäftszwecke wirklich (zwingend) benötigen, und welche eher einen „nice to have“-Charakter haben. Nur erstere sollten in unseren Standard-Eingabemasken (etwa einem Bestellschein, gleich ob online oder vor Ort ausgefüllt) oder (sonstigen) routinemäßigen Kontaktaufnahmen zwischen Kunden (bzw. anderen Parteien wie z.B. Lieferanten) und uns abgefragt werden. Daten jenseits von Kundenstammdaten, essentieller Bestellscheininformationen etc. wären demgegenüber ggfs. im Wege ausdrücklicher Einwilligungen einzuholen. Diese separate Erfassung hätte überdies den Vorteil, dass man damit spätere Löschungen o.ä. erleichtern würde. Dem Kunden stehen nämlich je nach „Notwendigkeitsgrad“ der jeweiligen Daten unterschiedlich intensive (Löschungs-)Rechte zu (so dürfen Daten für Zwecke der Direktwerbung bereits unmittelbar nach Widerspruch nicht mehr verwendet werden), so dass wir dann nach Lage des Falles den einen Datensatz (notwendige Daten) ohne weiteres stehen lassen könnten und nur den anderen („nice to have“) zu löschen hätten.

(b) Gestaltung von Einwilligungserklärungen und deren automatisierter Dokumentation, auch zum Thema „double opt-in“

Die DSGVO stellt keine Detailanforderungen an Einwilligungserklärungen, es gelten jedoch die allgemeinen Grundsätze, wonach eine solche Erklärung zumindest deutlich, leicht verständlich und transparent zu sein hat. In selbiger sollte daher zum Ausdruck kommen, welche Daten wir sammeln, wie und warum das geschieht, wie wir mit diesen Daten umgehen, ggfs. auch unter Einschaltung Dritter, und welche Rechte dem Kunden insoweit jedenfalls dem Grunde nach zustehen. Auch die Einwilligung für den Erhalt von Newslettern und oder weiteren Angeboten ist diesen Grundsätzen zu enterziehen.

KONKRET haben wir von unserer Anwaltskanzlei den Entwurf einer Einwilligungserklärung erhalten, bezogen auf den typischen Geschäftsvorfall. Insoweit brauchen wir uns also inhaltlich nicht weiter um diese zu kümmern. „Verfahrenstechnisch“ sollten wir die Einwilligung jedoch, zumindest für den Bereich des Onlinegeschäfts, im Wege eines sog. „double opt-in“ absichern, d.h. unser Kunde bestätigt uns die Einwilligung (z.B. mittels „clicks“ auf einen an dessen Email-Adresse übersandten Links) noch einmal. Dies hat zugleich den Vorteil, dass wir dann von jedem Kunden ein einheitliches Dokument – nämlich die Bestätigungs-Email – als Einwilligungs-Nachweis archivieren können und so unserer Nachweispflicht in erleichterter Weise nachkommen können. Alternativ soll die Bestätigung der Optionsauswahl in der Eingabemaske so gespeichert werden, dass bei Übersendung des Kontaktformulars vermerkt ist, wann der Betroffene seine Einwilligungserklärung erteilt hat. Die in der Praxis bis heute recht häufig anzutreffende Variante, in welcher die Einwilligung nicht archiviert wird, sondern der Bestellvorgang nur so gestaltet wird, dass es aus technischen Gründen nicht „weitergehen“ kann, wenn nicht an der richtigen Stelle ein Kreuz gesetzt wird, reicht nach den Maßstäben der DSGVO nicht (mehr) aus.

(c) Einrichtung von automatischen „Wiedervorlagen“ (zur Löschung oder Einschränkung) innerhalb bestimmter Fristen nach erstmaliger Anlegung eines Datenbestandes

Datenerhebung und Datenlöschung hängen eng miteinander zusammen, man könnte auch sagen: dem Kunden ist es überhaupt nur zuzumuten, dass seine Daten gespeichert werden, wenn ihm gleichzeitig die konkrete Perspektive geboten wird, dass selbige innerhalb absehbarer Zeit auch wieder gelöscht oder jedenfalls im Prinzip nicht mehr genutzt werden (können). Es ist also immer daran zu denken, dass ein Kunde, dem ein Löschungsanspruch vielleicht erst in gewisser Zeit zusteht, ggfs. heute schon eine (sog.) Einschränkung der Daten verlangen kann (vgl. dazu ausführlich weiter unten Abschnitt VIII.). Auch ohne Initiative seitens des Kunden (der also z.B. einen Löschungsanspruch gelten machen würde) sind wir jedoch verpflichtet, gespeicherte Daten turnusmäßig daraufhin zu überprüfen, ob die weitere Aufbewahrung noch durch tatsächliche unternehmerische Zwecke (sog. berechtigte Interessen) unsererseits legitimiert ist. Solche berechtigten Interessen können vielfältiger Art sein, allerdings bestehen selbige – mit umgekehrten Vorzeichen – regelmäßig auch auf Kundenseite. Das Prüfmoment (nach Turnus) dient also insbesondere dazu, festzustellen, wessen Interessen in Bezug auf den konkreten Fall überwiegen. Um dabei wenigstens eine grobe Marschroute aufzuzeigen: je länger Daten schon gespeichert sind, je weniger intensiv der Kundenkontakt, je unwichtiger diese für Ihr Unternehmen sind und je unsicherer die Perspektive auf eine Belebung der geschäftlichen Beziehung, desto eher wird der Löschungsanspruch des betroffenen Kunden unser Interesse an einer Fortsetzung der Speicherung überwiegen. Es ist aber stets eine Einzelfallentscheidung zu treffen, wenn auch intern noch Kriterien entwickelt werden können, welche der Vereinheitlichung solcher Entscheidungen dienen.

KONKRET erachten wir es für sinnvoll, jeden anzulegenden Datenbestand (falls technisch möglich) bereits im Zeitpunkt der Erstspeicherung mit einer Erinnerungsfunktion zu belegen, die dafür sorgt, dass hierfür automatisiert ein Prüfungstermin vergeben wird und der konkrete Datenbestand etwa im Stile eines „pop-up"-Fensters nach standardisiertem Zeitablauf in unserer Administration als zu erledigende Aufgabe erscheint. In diesem Zuge wäre dann zu entscheiden: Weiterspeicherung wie bisher, Einschränkung der Datenspeicherung oder Löschung. Die „Gretchenfrage" hierbei ist natürlich die Dauer solcher Fristen, d.h. der Zeitraum zwischen Erstverarbeitung und Wiedervorlage zur Prüfung des weiteren Schicksals des jeweiligen Datenbestandes. Dies deckt sich mit der Thematik der Aufbewahrungsfristen, die wir weiter unten (Abschnitt VIII. Nr. 3) mit konkreten Handlungsalternativen näher erörtern und daher an dieser Stelle darauf verwiesen wollen. Tendenziell lässt sich sagen, dass eine Frist umso eher als möglicherweise gegen die Prinzipien der DSGVO verstoßend angesehen werden kann, je länger sie dauert, ohne dass zwischenzeitlich Ereignisse eintreten, welche unser (unternehmerisches) Interesse an der Fortsetzung der Speicherung zu aktualisieren imstande wären.

2. Vorhandene und vorzuhaltende (System-)Ressourcen

Die DSGVO stellt keine Detailanforderungen in Bezug auf die von Unternehmensseite einzusetzende Hard- oder Software, um den gesetzlichen Anforderungen gerecht zu werden. Wie auch in anderen Zusammenhängen belässt die DSGVO es dabei, geeignete Maßnahmen (Stichwort: Datenintegrität durch Verschlüsselung) beispielhaft zu benennen und Sachverhalte nach Art eines „je…desto" Verhältnisses zu behandeln: je sensibler bestimmte Daten ihrer Art nach, je höher deren Gefährdung von außen, je größer die Folgen für die Betroffenen im Falle einer Datenpanne, desto sorgfältiger müssen sie vor unbefugtem Zugriff, rechtswidriger Verwendung und Verlust geschützt werden. Um ein bestimmtes Schutzniveau zu gewährleisten, kann dann auch eine Verschlüsselung erforderlich sein.

(a) Unsere EDV-Umgebung

Unsere aktuelle EDV-Umgebung stellt sich in grober Zusammenfassung etwa wie folgt dar:

Wir speichern die Daten auf einem Server in unserem. Der Zugriff auf unser System ist via peer to peer geregelt. Daneben speichern wir analoge Dokumente in den dafür zuständigen Ordnern. Jeder Mitarbeiter hat nur auf die Vorgänge Zugang, die ihn auch betreffen.

Eine Basisanforderung der DSGVO geht dahin, dass auf Unternehmensseite ein belastbares EDV-System zum Einsatz kommt, welches u.a. die Fähigkeit besitzt, Vertraulichkeit, Integrität und Verfügbarkeit von Daten im Zusammenhang mit deren Verarbeitung auf Dauer sicherzustellen.

KONKRET: Unsere IT-Abteilung hat uns mitgeteilt, dass sie unsere EDV-Anlage geprüft und für tauglich befunden hat, die Vorschriften der DSGVO einzuhalten.

(b) Verschlüsselung

Wie bereits angedeutet, erwähnt die DSGVO die Verschlüsselung von Daten als geeignete Maßnahme zur Gewährleistung eines angemessenen Schutzniveaus. Offen bleibt dabei z.B., in welchem Umfang eine solche Verschlüsselung zu erfolgen hat und welche Verschlüsselungstechnik im Einzelnen eingesetzt werden muss.

Anders als auf anderen gewerblichen Betätigungsfelder, etwa in der Gesundheitsbranche, verarbeiten wir üblicherweise keine besonders sensiblen Daten, denen ein besonders umfangreiches Verschlüsselungserfordernis innewohnt. Hinzu kommt, dass in der heutigen Realität der Kommunikation mit einer hohen Diversität an Empfängern ein allgemein akzeptierter Standard zur Entschlüsselung von Dokumenten etc. nicht einmal ansatzweise besteht, dass Empfänger entweder nicht die Ressourcen vorhalten können oder wollen, um mit solchen Dokumenten vernünftig umgehen zu können oder – umgekehrt – nur ihr eigenes Ver- und Entschlüsselungsprogramm verwenden wollen und „fremdverschlüsselte“ Daten folglich ablehnen. Mit dieser (jedenfalls vorläufigen) Realität müssen wir leben. Wir haben uns daher dazu entschlossen, bis auf weiteres nur den Weg der Kommunikation zu verschlüsseln, nicht den Inhalt derselben. Mit anderen Worten: wenn wir eine E-Mail an den Kunden K schicken, wird diese verschlüsselt bis zu jenem Punkt transportiert, ab welchem der Kunde Zugriff auf selbige hat (das kann z.B. die Benutzeroberfläche seines Email-Providers sein). Den Inhalt der Email kann er dann dort direkt (ohne weitere Zwischenschritte) zur Kenntnis nehmen. Neben diesem Teilaspekt sind auch unsere Server (Hauptserver, Backup-Server und Email-Server) zur Verhinderung unbefugten Zugriffs (z.B. dem „Auslesenkönnen“ derselben im Falle ihrer hypothetischen Entwendung) zu verschlüsseln.

KONKRET müssen wir zum einen unsere Server und alle Speichermedien verschlüsseln (und verschlüsselt halten), und zwar mit (jeweils) marktgängiger Verschlüsselungstechnik. Konkrete Empfehlungen hierzu von berufener Seite dazu (d.h. also welche Hersteller geeignete Technik anbieten), etwa durch die für uns zuständige IHK oder unseren Branchenverband, sind als Orientierungsgrundlage zu berücksichtigen. Zum anderen müssen wir gewährleisten, dass – so lange / soweit ein eigener Email-Server zum Einsatz kommt – eine flächendeckende Verschlüsselung des (Weges des) Email-Verkehrs in Eigenregie erfolgt. So lange / soweit wir (ggfs. zusätzlich) Gebrauch machen von einem externen Email-Provider (falls wir z.B. einmal eine Störung an unserem eigenen Email-Server haben sollten und dringend Emails verschicken müssten), ist darauf zu achten, dass ein Provider verwendet wird, der den Übermittlungsvorgang ebenfalls verschlüsselt. Notfalls wäre dies beim ins Auge gefassten Provider ad hoc in Erfahrung zu bringen und – bei längerer Nutzung – sodann zu „monitoren“, ob sich hieran etwas ändert.

Zu verschlüsseln ist daneben unsere Website. Dies ist in Kooperation mit unserem Web Hoster / Web Desginer sicherzustellen.

Außerdem mag es auch bei uns Fälle geben, in denen es aufgrund besonderer Umstände (etwa das in Frage stehende Handelsvolumen, ein besonderes Maß an geschuldeter Vertraulichkeit [z.B. aufgrund eines abgeschlossenen NDA]) im Einzelfall angemessen sein kann, bestimmte Kommunikation als solche zu verschlüsseln. Diese Entscheidung müssen wir allerdings nicht per se treffen, sondern können Sie auch – sogar vorzugsweise – unserem Kunden (etc.) überlassen, indem wir dort nachfragen, ob für einen bestimmten Vorgang (voll-)verschlüsselte Kommunikation gewünscht wird (oder eben nicht). Der entsprechende Vorgang sollte dann mit einem internen Vermerk ausgestattet, dokumentiert und archiviert werden.

(c) Datensicherung („back-ups“)

Die DSGVO verlangt, dass Daten – etwa im Falle eines Verlustes oder physischer Zerstörung von Speichermedien auf Seite des Unternehmens – rasch wiederherstellbar sind. Demnach müssen Daten bei Datenverlust nicht nur überhaupt „gerettet“ werden können, vielmehr muss auch sichergestellt sein, dass dies innerhalb eines kurzen Zeitabstandes möglich ist.

KONKRET bedeutet dies für uns, dass wir zumindest *eine* Redundanz vorhalten müssen, vorzugsweise in Form eines physischen (sog.) Backup Servers, der technisch eine (zumindest) tagesaktuelle 1:1 Spiegelung unseres Haupt-Servers (jedenfalls in Bezug auf das hiesige Datenthema) darstellt. Alternativ könnten wir (second-best) eine (ebenso aktuelle) Kopie des eigenen Datenbestandes in online-basierter Form bereithalten (Cloud-Lösungen etc.), wobei in diesem Falle physische Speicherkapazität eines Dritten in Anspruch genommen würde, was im Regelfall dazu führt, dass eine Auftragsdatenverarbeitung erfolgt (ggfs. auch in einem Drittland außerhalb der EU) und damit zusätzliche Anforderungen durch uns einzuhalten wären (siehe dazu ausführlicher unten Abschnitt VII Nr. 1).

(d) EDV- und Datenaktualität

Der Bereich der EDV, der Datentechnik im Allgemeinen sowie software- und hardwaremäßiger Entwicklungen ist ständigem Wandel unterworfen. Was heute noch „state of the art“ ist, kann morgen schon als veralteter Standard gelten. Daneben können Daten auch inhaltlich veralten, also zwischenzeitlich nicht mehr auf dem neuesten Stand verkehren, während die DSGVO grundsätzlich verlangt, dass Daten richtig und auf dem neuesten Stand sind.

KONKRET sollten wir daher ein Verfahren implementieren, mit dem in regelmäßigem Abstand überprüft und bewertet wird, ob das von uns vorgehaltene und betriebene EDV-System noch den dann jeweils aktuellen Anforderungen (die etwa gestiegen sein können, weil sich sog. Hacker neue Zugangswege für Dateneinbrüche erschlossen haben) entspricht, insbesondere weiterhin gewährleistet ist, dass eine sichere, in jeder Hinsicht den Vorgaben der DSGVO entsprechende Datenverarbeitung stattfindet. Verneinendenfalls wären entsprechende Abhilfemaßnahmen zu ergreifen, ggfs. auch in Kooperation mit dem Betroffenen (Kunde etc.). Zusätzlich sollten wir im Rahmen des mit vertretbarem technischen Aufwand Möglichen dafür sorgen, dass es bei uns eine Art Aktualisierungs- und Korrektur-Routine gibt, welche Fehler entweder direkt erkennt (bzw. eine mit „8“ beginnende PLZ in NRW) oder erhaltene (neue) Informationen direkt an die richtige Stelle weiterleitet, um so zu einer schnellstmöglichen Korrektur / Aktualisierung innerhalb des Datenbestandes zu kommen.

3. Wartung (intern / extern) und Vertraulichkeit von Daten

Wenn wir unsere Datenverarbeitungssysteme intern, d.h. durch Sie als unsere Mitarbeiter, warten lassen, brauchen wir keine weiteren Maßnahmen zur Wahrung der Datenintegrität zu ergreifen. Verhält es sich jedoch so, dass wir einen externen Wartungsvertrag geschlossen haben oder auch nur sporadisch externe Wartung zulassen, kann eine Situation entstehen (insbesondere bei umfangreichen Wartungsarbeiten, Fehlersuchen etc.), in denen ein Externer (gezielt oder ungezielt) Kenntnis nimmt von Daten, die bei uns gespeichert sind. Dies kann bereits ein datenrelevantes Handeln (durch uns, namentlich in Form der sog. Offenlegung durch Bereitstellung) darstellen, so dass wir gehalten sind, auch diesen Externen in ähnlicher Weise wie unserer Mitarbeiter auf Vertraulichkeitswahrung gegenüber den von seinem Handeln möglicherweise Betroffenen (Kunden, Lieferanten etc.) zu verpflichten.

KONKRET benötigen wir dementsprechend bei Fremdbeauftragung von Wartungsarbeiten der o.g. Art eine Vertraulichkeitserklärung jener Partei, welche die Wartungsarbeiten durchführt. Den Entwurf einer solchen Vereinbarung haben wir von unserer Anwaltskanzlei zur Verfügung gestellt bekommen.

III. Datenschutz durch Einsatz persönlicher Mittel

Neben der Schaffung der technischen Voraussetzungen für einen effektiven Datenschutz müssen auch die persönlichen Mittel unseres Betriebs so eingerichtet und organisiert werden (nebst Belehrung, Verpflichtung und Instruktion), dass der technisch leistbare Schutz auf sinnvolle Weise durch die personelle Komponente in der Datenbehandlung ergänzt und so den Anforderungen der DSGVO Genüge getan wird.

1. Organisation von Zuständigkeiten und Zugänglichkeit von Datenbeständen („need to know“)

Der Grundsatz der Datenminimierung gilt nicht nur für den Umfang der zu sammelnden Daten, sondern auch – in übertragenem Sinn, zusammen mit dem Vertraulichkeitsgrundsatz – für den Zugang zu selbigen durch Unternehmensangehörige. Auch letzterer unterliegt, vereinfacht gesagt, dem Erforderlichkeitsgrundsatz: genauso wie Daten nicht gesammelt werden dürfen, die für unsere Unternehmenszwecke keine Relevanz besitzen, dürfen Mitarbeiter keinen Zugang zu Daten erhalten, soweit diese keine Relevanz für deren jeweilige Aufgabenerfüllung im Unternehmen besitzen. Positiv gewendet: Zugang zu Daten nur bei Notwendigkeit von deren Kenntnis gerade durch den spezifischen Mitarbeiter (sog. „need to know“-Kriterium).

KONKRET bedeutet dies, dass es eine weitgehende Übereinstimmung geben muss zwischen unserer internen Organisationsstruktur / Ressorts / Zuständigkeitsbereichen und unserer Datenstruktur in Bezug auf deren Zugänglichkeit. Mitarbeiterbezogen könnte man es auch umschreiben als Kongruenz zwischen Aufgaben- und Zugangsreichweite. Die Marktseite braucht andere Daten als die Marktfolgeseite, und wer mit dem Zahlungsverkehr eines Kunden nichts zu tun hat, benötigt beispielsweise keinen Zugang zu dessen Bankdaten. Unser Datenflussschema ist demzufolge daraufhin zu überprüfen, ob es dem vorgenannten Prinzip Rechnung trägt. Wo bzw. soweit dies nicht der Fall ist, sind virtuelle Barrieren einzurichten, die als Zugangssperren für nicht erforderliche Datenzugriffe wirken. Generell sind PC-Arbeitsplätze wie auch mobile Datenträger (z.B. Mobil-Telephone) mit einem individuellen Passwort-Schutz für den jeweiligen Mitarbeiter auszustatten, wobei generelle Kriterien dafür festgelegt werden sollen, wie komplex ein Passwort zu sein hat und wie häufig es zu ändern ist. Auf die Anlage „Passwortrichtlinie“ wird verwiesen. (Soll das Unternehmen selbst anfertigen)

2. Persönliche Entscheidungsfindung

Die Entscheidungsfindung in unserem Unternehmen soll stets – wenn auch in unterschiedlichem Umfang – eine menschliche Interaktion erkennen lassen. Dies bedeutet im Umkehrschluss, dass der Kunde etc. im Grundsatz (d.h. von besonderen Ausnahmefällen abgesehen) das Recht hat, nicht einer ausschließlich auf automatisierter Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, wenn diese Ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Sollten wir ausnahmsweise doch einmal mit derlei (automatisierten) Entscheidungsstrukturen arbeiten, wäre der Kunde etc. zuvor separat darüber zu informieren, und müssten wir dessen ausdrückliche (vorherige) Zustimmung hierzu einholen.

3. Mitarbeiterschulung / „Mind-Set“

Datenschutz ist eine das ganze Unternehmen erfassende Aufgabe und daher letztlich auch nur so gut wie der Einsatz und Wille der unserer Belegschaft, dazu ihren Beitrag zu liefern. Ein solches Wollen hängt dabei eng mit dem entsprechenden Können zusammen. Nur wer weiß, was er in datenschutzrechtlicher Hinsicht schuldet, kann auch entsprechend liefern. Zudem soll intern eine entsprechende „Awareness“ für die Belange des Datenschutzes geschaffen werden.

KONKRET erwarten wir von unseren Mitarbeitern die Teilnahme an von uns angebotenen Schulungen (welche etwa durch unsere Anwaltskanzlei abgehalten werden), wobei es jedem Mitarbeiter als Basisqualifikation und Mindestanforderung obliegt, sich durch Kenntnisnahme von der Datenschutzerklärung und dieser Unternehmensrichtlinie mit den Grundprinzipien der DSGVO vertraut zu machen. Wir beabsichtigen, das entsprechende Kenntnisniveau von Zeit zu Zeit zu monitoren, etwa durch kleine Tests, Wissensabfragen

u.Ä., die sich ggfs. auch einmal komplexere Fälle wie beispielhafte Datenzyklen mit den spezifischen Anforderungen der jeweiligen Phase (von der Erhebung bis zur Löschung) erstrecken könnten.

4. Ergänzung zum Arbeitsvertrag / Vertraulichkeitsverpflichtung gegenüber Dritten

Konkreter Datenschutz kann selbst unter Berücksichtigung der Möglichkeiten, welche die Technik für dessen Zwecke zur Verfügung stellt, in letzter Instanz immer nur von Menschen, also unseren Mitarbeitern, geleistet werden. Dazu gehört, dass unsere Mitarbeiter nicht nur Kenntnis von Existenz und Inhalt der DSGVO haben, sondern sich auch rechtsverbindlich zu deren Zielsetzungen bekennen. Durch ein solches Vertraulichkeits-Commitment innerhalb unseres Unternehmens kommt mittelbar auch ein entsprechender Wille zur Vertraulichkeit gegenüber Kunden, Lieferanten etc. zum Ausdruck.

KONKRET werden wir eine Anlage zum Arbeitsvertrag zu verwenden, mittels welcher jeder Mitarbeiter sich zu den Zielen und Anforderungen der DSGVO bekennt und uns deren Wahrung als eigenständige Verpflichtung aus dem Arbeitsverhältnis verspricht. Der entsprechende Entwurf stammt von der uns beratenden Anwaltskanzlei.

5. Datenschutzbeauftragter

Ist ein Unternehmen nach der DSGVO (in Verbindung mit dem BDSG) verpflichtet, einen Datenschutzbeauftragten zu bestellen, wird dieser eine erhebliche Rolle im Unternehmen spielen. Er ist, innerhalb wie außerhalb des betreffenden Unternehmens, der zentrale Ansprechpartner für alle Aspekte rundum das Thema Datenschutz. Seine Aufgabe nimmt er fachlich weisungsunabhängig wahr, zugleich muss er die entsprechende Kompetenz besitzen, um seiner Verantwortung tatsächlich nachkommen zu können.

(a) Unternehmensgröße

Die „kritische“ Unternehmensgröße liegt – vereinfacht gesagt – bei 10 Beschäftigten mit einem PC-Arbeitsplatz.

KONKRET wird diese Größe wird durch unser Unternehmen nicht erreicht. Diese Aufgabe wird bei uns durch Herrn Heinz Schmidt erfüllt.

(b) Arten von Daten (Sensibilitätsgrade) und Art der Datenverarbeitung

Die DSGVO differenziert in Bezug auf das Thema Datenschutzbeauftragter weiter danach, ob bestimmte Arten von Daten oder diese in bestimmter Weise oder mit bestimmter kommerzieller Zweckrichtung verarbeitet werden, und legt dann ggfs. auch Unternehmen mit einer geringeren Beschäftigtenzahl die Verpflichtung zu Benennung eines Datenschutzbeauftragten auf.

KONKRET ändert sich für uns hierdurch nichts, weil wir bereits aus „formellen“ Gründen – Mitarbeiterzahl < 9 – nicht benennungspflichtig sind.

IV. Datenschutz durch Einsatz informativer Mittel / Dokumentation Richtung Kunde

Eine zentrale Rolle im Konzept der DSGVO zur Gewährleistung eines wirksamen Datenschutzes spielt die umfassende Aufklärung des Betroffenen (Kunden etc.) über dasjenige, was er an Daten preisgibt, was damit geschieht und – vereinfacht formuliert – welche Mitbestimmungsrechte ihm insoweit zustehen.

1. Die Datenschutzerklärung; Einwilligung in die Datenverarbeitung

Durch unsere Anwaltskanzlei ist uns eine umfangreiche Datenschutzerklärung zur Verfügung gestellt worden. Inhaltlich müssen wir uns mit dieser nicht weiter auseinandersetzen, entscheidend ist, dass diese in sachgerechter Weise verwendet wird. Namentlich ist dieses Dokument – neben der konkreten Einwilligungserklärung – das zentrale Aufklärungsinstrument in Richtung des Betroffenen unserer Datenverarbeitungsmaßnahmen.

KONKRET sorgen wir dafür, dass jede Person, in Bezug auf welche wir Daten (erstmals) verarbeiten oder beabsichtigen zu verarbeiten, zum frühestmöglichen Zeitpunkt (wenn irgend möglich schon vor der Verarbeitung):

(1) unsere Datenschutzerklärung erhält, und

(2) uns deren Erhalt bestätigt, und zwar

(3) in einer Weise, die für uns archivierbar / reproduzierbar ist.

In einer rein mündlichen Situation, die datenschutzrelevant ist oder werden kann (z.B. eine Abfrage bestimmter Daten im Rahmen der Anbahnung eines Rechtsgeschäfts), soll der Betroffene wählen können, auf welche Weise er belehrt zu werden wünscht, wobei hier ggfs. auch mit Bandansagen und daraufhin erfolgender Interaktion des (z.B.) Anrufers gearbeitet werden kann. Diese Interaktion, welche eventuell auch nur in einem Drücken von Tasten bestehen kann, sollte – nach Aufzeichnungshinweis und entsprechender Einwilligung (welche u.U. auch konkludent in der anruferseitigen Nichtbeendigung des Gesprächs trotz Aufzeichnungshinweises liegen kann) – für Nachweiszwecke aufgezeichnet werden. Die genaue Gestaltung solcher Verfahren bedarf noch weiterer Detaillierung. Möglicherweise könnten wir hier auch mit „Verzichtslösungen" arbeiten, etwa indem der Anrufer, der keine Lust hat, sich eine überlange Bandansage anzuhören, zusätzlich die Gelegenheit erhält, kurz (z.B. durch Tastatureingabe) zu bestätigen, dass er von unserer Datenschutzerklärung im Internet Kenntnis genommen hat und eine weitere „Belehrung am Telefon" nicht benötigt.

(a) Allgemeines / „Wer schreibt, der bleibt"

Einige Vorgaben, welche die DSGVO enthält und im Verhältnis Unternehmen – Kunde etc. zu erfüllen sind, sind nicht an eine bestimmte Form gebunden. So findet sich dort neben ausdrücklichen Schriftformerfordernissen beispielsweise auch die Formulierung, dass eine bestimmte Pflicht „schriftlich oder in anderer Form" erfüllt werden kann. Beispielsweise ist auch die Mitteilung des Datenschutzbeauftragten an die Behörde an keine besondere Form gebunden. Andererseits trifft uns nach der DSGVO eine umfassende Rechenschaftspflicht, und im Zweifel müssen wir die Einhaltung von Vorschriften, das Nachkommen von Pflichten etc. nachweisen. Offensichtlich kann dies nur gelingen, wenn datenschutzrelevante Vorgänge in weitestgehendem Umfang dokumentiert werden, wobei dies in geeigneten Fällen natürlich auch elektronisch erfolgen kann. Geeignet sind insbesondere solche Fälle, bei denen der elektronische Nachweis gegenüber einem schriftlichen Nachweis (als unmittelbar lesbare Aufzeichnung o.ä.) keine nennenswerten Nachteile in Sachen Aussagewert und Reproduzierbarkeit aufweist.

KONKRET bedeutet das für uns, das wir uns als Unternehmen und konkret Sie als Mitarbeiter nachweispflichtige Vorgänge so gut wie eben möglich in reproduzierbarer Form dokumentieren müssen, wobei der angeführte Grundsatz („Wer schreibt, der bleibt.") nicht wörtlich zu verstehen ist, sondern je nach Fallgestaltung auch textliche, elektronische, magnetische etc. Dokumentation ausreichen kann. Was ggfs. nachgewiesen werden muss, ist in der DSGVO nicht abschließend aufgezählt und hängt praktisch gesehen wesentlich davon ab, mit welchen Anträgen man von Seiten Betroffener (Kunden etc.) oder der Behörde (Audits etc.) konfrontiert wird. Wesentliche Mitwirkungshandlungen des Betroffenen (z.B. Einwilligung), Verhalten gegenüber der Behörde (z.B. Benennung Datenschutzbeauftragter), erhebliche Änderungen der EDV-Umgebung (z.B. neue Verschlüsselungsart) und Wahrnehmung prinzipienrelevanter Pflichten der DSGVO (z.B. Prüfung der weiteren Aufbewahrung von Daten nach Zeitraum X) müssen stets dokumentiert werden, es gilt der Grundsatz: lieber zu viel als zu wenig Dokumentation, weil ersteres „nachweisfreundlicher" ist.

(b) Graphische Gestaltung, Verweise via Link-Funktion

Transparenz, Verständlichkeit und Einfachheit sind Pfeiler der DSGVO, an welchen sich auch die Gestaltung unserer Datenschutzerklärung zu orientieren hat. Die Erklärung als solche wurde uns durch unsere Anwaltskanzlei zur Verfügung gestellt.

KONKRET müssen wir insbesondere in graphischer Hinsicht dafür sorgen, dass die Erklärung gut lesbar ist, was z.B. eine entsprechende Schriftgröße voraussetzt. Dies sollte – gleich in welchem Anwendungszusammenhang – die Größe 10 nicht unterschreiten. Größere Schriften sind vorzugswürdig. Außerdem ist dem Leser die Kenntnisnahme von der Datenschutzerklärung dadurch zu erleichtern, dass die dort enthaltenen Verweise (auf vor- oder nachstehende Hinweise) mittels Hyperlinks direkt auffindbar sind, ohne dass noch weiter in der Erklärung selbst nach dem richtigen Abschnitt, auf den verwiesen wird, gesucht werden muss.

2. Übersichtlichkeit unserer Website in datenschutzrechtlicher Hinsicht, auch zum Thema „one click" und datenschutzfreundlichen Voreinstellungen

Das Transparenzgebot gilt nicht nur den für Inhalt der Datenschutzerklärung selbst, sondern auch für deren Auffindbarkeit, namentlich im Bereich unserer Website. Der Grundsatz der Datenminimierung verlangt darüber hinaus datenschutzfreundliche Voreinstellungen.

KONKRET sollte unsere Datenschutzerklärung daher in einer Weise auf unserer Website platziert werden (und verfügbar) sein, dass sie bereits mit einem einzigen „click" erreichbar ist, was im einen entsprechenden „button" (mit entsprechender Benennung) auf der „home" / Start-Seite unserer Website verlangt. Die Datenschutzerklärung ist dort einmal als direkt lesbarer Text zu veröffentlichen, zum anderen als downloadbare Variante in einem gängigen Format (vorzugsweise .pdf) vorzuhalten. Bei konkreter Interaktion zwischen Betroffenem und uns (z.B. ein potentieller Kunde meldet sich über das Kontaktformular) ist die Datenschutzerklärung – Link-unterlegt – ebenfalls (noch einmal) zum Lesen und zum Download anzubieten. Auf der Website wie auch sonst vorgehaltene Formulare sind datenschutzfreundlich auszugestalten. Das bedeutet insbesondere, dass Zusatzverwendungen von Daten des Betroffenen (etwa dessen Email-Adresse für den Versand eines Newsletters) nicht einwilligungsfingierend voreingestellt sein dürfen (also etwa das entsprechende Kreuzchen bereits für den Betroffenen gesetzt wurde, er dieses also erst aktiv löschen musste, um eine Datenverwendung insoweit zu vermeiden), stattdessen jeweils bestätigende Einzel"clicks" zu setzen sind.

3. Einwilligung im Allgemeinen; Einwilligungserklärung oder berechtigtes Interesse? Zugleich zum besonderen Schutz von Minderjährigen

Die DSGVO benennt mehrere Rechtsgründe / Rechtfertigungen für die Verarbeitung von Daten, so etwa die Gewährleistung der Erfüllung eines Vertragsverhältnisses oder die Erfüllung (sonstiger, z.B. öffentlich-rechtlicher) Pflichten. In der Praxis jedoch wird als Rechtfertigung der Datenverarbeitung die Einwilligung des davon Betroffenen eine zentrale Rolle spielen, nicht zuletzt deshalb, weil deren Vorliegen im Zweifel leichter nachzuweisen sein wird als ein berechtigtes Interesse (an der Datenverarbeitung), weil letzterenfalls stets eine Abwägung mit (eventuell) gegenläufigen Interessen des Betroffenen stattzufinden hat.

KONKRET müssen wir darum stets bestrebt sein, Einwilligungserklärungen von unseren Kunden etc. zu erhalten und diese sodann jederzeit abruffähig vorzuhalten, sollte sich unsere entsprechende Nachweispflicht einmal aktualisieren (z.B. aufgrund behördlicher Anforderung oder kundenseitigen Bestreitens). Als Einwilligungserklärung verwenden wir das uns von unserer Anwaltskanzlei zur Verfügung gestellt Formular. Auch hier gilt, dass jede Person, in Bezug auf welche wir Daten (erstmals) verarbeiten oder beabsichtigen zu verarbeiten, zum frühestmöglichen Zeitpunkt (wenn irgend möglich schon vor der Verarbeitung):

(1) unsere Einwilligungserklärung erhält, und

(2) darin seine Einwilligung erklärt, und zwar

(3) in einer Weise, die für uns archivierbar / reproduzierbar ist.

Das hierfür anzuwendende Verfahren ist oben unter II. 1. (b) näher beschrieben. Die Einwilligungserklärung darf keine sachwidrige Kopplung enthalten, also etwa einen

Geschäftsabschluss von der Offenlegung von Daten abhängig machen, deren Verarbeitung für diesen Geschäftsabschluss und dessen Abwicklung nicht erforderlich ist (sachwidrig wäre es z.B., eine Ware nur dann bestellen zu können, wenn gleichzeitig in den Empfang eines Newsletters eingewilligt würde). Durch geeignete Maßnahmen, u.a. den Text der Einwilligungserklärung, ist im Rahmen des Möglichen sicherzustellen, dass eine Datenverarbeitung in Bezug auf Minderjährige unter 16 Jahren nicht stattfindet.

4. Ausdrückliche Einwilligungserklärung in Sonderfällen

Bei besonders sensiblen Daten – welche in unserem Unternehmen im Regelfall nicht verarbeitet werden – wäre im Zusammenhang mit deren Verarbeitung grundsätzlich eine ausdrückliche Einwilligung einzuholen.

KONKRET: sollte es ausnahmsweise einmal zu einem solchen Fall kommen (beispielsweise Daten in Bezug auf ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, oder von biometrischer Qualität in Rede stehen), ist der Vorgang zur weiteren Veranlassung und Entscheidung der Geschäftsleitung und dem Datenschutzbeauftragten vorzulegen.

5. Zweckänderung zwischen erstmaliger Erhebung und späterer Nutzung

Es kann vorkommen, dass der Zweck, zu dem in der Vergangenheit gespeicherte Daten heute verwendet werden sollen, ein anderer ist als jener, zu welchem damals die Speicherung erfolgte. Dies kann verschiedene Gründe haben, etwa eine Unternehmenszweckänderung: ein Bioladen wird zu einem Burger-Restaurant. Dürfen die Kunden des Bioladens jetzt auch als Kunden des Burger-Restaurants betrachtet werden, so dass Ihre Daten weiterhin verarbeitet werden dürfen? Die DSGVO bejaht dies, falls der aktuelle Zwecke noch mit dem ursprünglichen Zweck vereinbar ist, wobei eine umfassende Interessenabwägung anzustellen ist, die u.a. folgendes berücksichtigt: den Kontext der damaligen Erhebung, das Maß an Zusammenhang zwischen damaligen Erhebungs- und aktuellen Verarbeitungszwecken, die Art (Sensibilität) der Daten und die Folgen der Weiterverarbeitung für den Betroffenen ebenso wie das Vorhandensein verarbeitungsbegleitender Garantien (z.B. Verschlüsselung).

KONKRET müssen wir – da eine solche Abwägung mitunter schwer zu treffen, nicht verallgemeinerungsfähig und stets mit Unsicherheiten belastet ist – danach streben, in Situationen erkennbarer Zweckänderung (nicht ganz untergeordneter Art) Kontakt mit dem / den Betroffenen aufzunehmen und eine erneute Einwilligung (jetzt für den geänderten Zweck) einzuholen.

V. Datenschutz durch Einsatz informativer Mittel / Dokumentation Richtung Behörde

Die sich aus der DSGVO ergebende Rechenschaftspflicht entfaltet Wirkung nicht nur gegenüber dem Betroffenen von Datenschutzmaßnahmen, sondern auch gegenüber den Behörden, namentlich der Aufsichtsbehörde.

1. Nachweispflichten im Allgemeinen

Die Nachweispflichten der DSGVO sind dort nicht abschließend geregelt, teilweise auch nur prinzipienorientiert gefasst. So bezieht sich die Nachweispflicht jedenfalls auf all das, was in der DSGVO an Grundsätzen zulässiger Datenverarbeitung festgehalten ist: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. Daran wird deutlich, dass jeweils noch eine „Übersetzungsleistung“ erforderlich ist, um ermitteln zu können, welche konkreten Handlungen mit Datenschutzrelevanz im Zweifel (namentlich auf konkrete Aufforderung hin) nachweispflichtig sind. Ein besonders wichtiger Bezugspunkt von Nachweispflichten ist – auch gegenüber der Behörde – die Einwilligung(serklärung) des von Datenverarbeitung Betroffenen.

KONKRET gilt auch hier, dass unternehmensinterne Handlungen mit datenschutzrechtlicher Relevanz so nachweisfähig wie möglich ausgeführt werden sollen, und entsprechend zu dokumentieren sind. Sollen Daten z.B. einmal länger aufbewahrt werden als gemäß der regulären Aufbewahrungsfrist – was z.B. aufgrund eines berechtigten (unternehmensseitigen) Interesses möglich sein kann –, dann sollte im relevanten Kontext jedenfalls ein kurzer Vermerk erstellt werden, in dem unserer berechtigten Interessen immerhin skizziert und die Gründe, warum diese jene des Betroffenen überwiegen, umrissen werden. Das oben unter IV. 1. (a) Gesagte gilt hier entsprechend.

2. Das sog. Datenverarbeitungsverzeichnis

Unternehmen ab einer Größenordnung von 250 Mitarbeitern haben ein Verzeichnis von deren Verarbeitungstätigkeiten zu erstellen, in welchem – abstrahierend vom Einzelfall – durch den Datenverantwortlichen u.a. niederzulegen ist, welche Verarbeitungszwecke verfolgt werden, welche Kategorien von Empfängern existieren, denen gegenüber Daten ggfs. offengelegt werden, ob es bei Datenübermittlungen zu Drittlandinvolvierungen kommt, welche Maßnahmen des technischen Datenschutzes getroffen worden sind etc. Ist das Unternehmen mit weniger Personal ausgestattet als vorstehend genannte Mitarbeiterzahl, besteht ausnahmsweise gleichwohl eine entspreche Verzeichnispflicht.

KONKRET benötigen wir ein solches Verzeichnis nicht. Zum einen unterschreiten wir die o.g. Mitarbeiterzahl deutlich, zum anderen treffen auch die Ausnahmetatbestände (jedenfalls gegenwärtig) auf uns nicht zu. Diese sind nur gegeben, wenn es um Datenverarbeitung in einem Risikokontext für die Rechte und Freiheiten betroffenen Personen geht, Datenverarbeitung den eigentlichen Geschäftszweck des Unternehmens darstellt oder Daten besonderer Kategorien (mit hervorgehobener Sensibilität, wie beispielsweise Gesundheitsdaten) verarbeitet werden – allesamt Voraussetzungen, die wir mit unserem Unternehmen nicht erfüllen.

3. Was tun bei einem sog. Daten-Leck oder sonstigem Datenverlust?

Ein Daten-Leck ist eine ernste Angelegenheit. Üblicherweise versteht man darunter einen Vorgang, bei welchem Unbefugte Zugriff auf Datenbestände erhalten, wobei es jedenfalls für die DSGVO keinen Unterschied macht, ob es sich um eine gezielte Aktion (Dritter, z.B. einen sog. Hackerangriff) handelt oder Daten versehentlich (z.B. durch Unachtsamkeit eines Mitarbeiters, der einen „falschen Knopf“ gedrückt oder ein physisches Speichermedium im öffentlichen Raum verloren hat) verloren gegangen bzw. in die Öffentlichkeit „entlassen“ worden sind. Hier kann eine – ggfs. unverzüglich zu erfüllende – Hinweispflicht sowohl gegenüber der (Aufsichts-)Behörde als auch gegenüber den direkt Betroffenen entstehen.

KONKRET müssen wir bei einem Daten-Leck / Datenverlust o.ä. eine entsprechende Meldung an die Aufsichtsbehörde absetzen, die zumindest den folgenden (Mindest-)Inhalt haben muss: Art der Verletzung, (falls möglich) Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze (Quantitativschätzung), Kontaktdaten unseres Datenschutzbeauftragten, Folgenbeschreibung des Verletzungsereignisses (was droht wahrscheinlich), ergriffene / vorgeschlagene Maßnahmen zur Behebung der Verletzung und ggfs. zur Reduzierung von deren Auswirkungen. Die Meldung ist unverzüglich zu erstatten und soll jedenfalls auch – schon für eigene Dokumentationszwecke – schriftlich erfolgen. Nur ausnahmsweise gestattet dieses Unverzüglichkeitsgebot einen längeren (und dann begründungspflichtigen) Zeitraum als 72 Stunden, von unserer Kenntniserlangung vorgenannter Umstände an gerechnet. Von dieser grundsätzlichen Meldepflicht sind wir nur dann enthoben, wenn es trotz des Daten-Lecks o.ä. nicht wahrscheinlich ist, dass es zu Verletzung der Rechte und Freiheiten Betroffener (etwa einer Diskriminierung, Identitätsdiebstahl oder -betrug, finanziellen Verluste, unbefugter Aufhebung von Pseudonymisierung(en), Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person) kommt. Dies ist stets eine Einzelfallbewertung, die in Abstimmung mit dem Datenschutzbeauftragten zu treffen ist. Dabei kann es durchaus Situationen geben, in denen trotz unbefugter *Erlangung* von Daten diesen bzw. den davon Betroffenen (nach menschlichem Ermessen) keine Gefahr droht,

weil die Daten derart sicher verschlüsselt sind, dass jedenfalls mit unbefugter *Kenntnisnahme* nicht zu rechnen ist. Bleiben danach Zweifel, ob die Meldung nötig ist oder nicht, so ist sie abzusetzen. In gleicher Weise ist der Betroffene zu unterrichten (ohne die o.g. Quantitativschätzung), falls das Risiko der Verletzung seiner Rechte und Freiheiten ein hohes ist und weder Verschlüsselung noch nachträgliche Eindämmungsmaßnahmen zu einer deutlichen Risikoreduzierung führen und die Meldung auch nicht mit unverhältnismäßigen Aufwand verbunden ist. Ist (nur) letzteres der Fall, so ist eine alternative Offenlegung des Problems zu bewirken, beispielsweise mittels öffentlicher Bekanntmachung. Auch hier ist der Datenschutzbeauftragte unverzüglich zu involvieren und hat eine führende Rolle inne.

VI. Erleichterungen in Sachen Nachweispflichten durch Zertifizierung und Verbandsarbeit

Die nach der DSGVO bestehenden umfangreichen Nachweispflichten schaffen für die Praxis ein unabweisbares Interesse an einer Vereinheitlichung routinemäßiger Abläufe und wiederkehrender Fragestellungen. Außerdem kann die Bewertung bestimmter Abläufe innerhalb unseres Betriebs durch externe Dritte wenigstens subjektiv ein gewisses Plus an Rechtssicherheit schaffen, wenn von dort die DSGVO-Konformität bestimmter Verfahrensschritte bestätigt wurde.

1. Zertifizierer

Die Möglichkeit für eine Art außerbehördliches Audit ohne Sanktionsrisiko besteht darin, gewisse Unternehmensabläufe durch einen Zertifizierer unter die Lupe nehmen zu lassen und daraufhin zu untersuchen, ob sie sich in Übereinstimmung mit den Anforderungen der DSGVO befinden. Ggfs. könnte dies (auch) unter Marketinggesichtspunkten interessant für uns sein / werden, je nachdem, wie schwer dieses Thema künftig in der Bevölkerung / jedenfalls unserem Kundenkreis etc. gewichtet werden wird. Gegenwärtig ist davon auszugehen, dass aufgrund der Neuheit der DSGVO das Zertifizierungsthema noch in den Kinderschuhen steckt und zunächst eine Orientierungsphase stattfindet, in der wir den Markt sondieren werden, um sodann zu entscheiden, ob sich die Kooperation mit einem Zertifizierer lohnt. Auch muss noch abgewartet werden, welche Preise hierfür aufgerufen werden, wobei bereits jetzt klar ist, dass Zertifikate nach 3 Jahren erneuert werden müssen und sodann also mit neuerlichem Kostenanfall zu rechnen ist. Zu beachten wäre in jedem Fall, dass ein positives Testat eines Zertifizierers keineswegs einen „Freifahrtschein“ (im Sinne von: „alles richtig gemacht“) darstellt, die Einhaltung der DSGVO (bzw. der geprüften Teile derselben) vielmehr nur indizieren kann. Eine gegenteilige Beurteilung durch die Behörde bleibt weiterhin möglich.

KONKRET soll die Sondierung dieser Thematik durch unseren Datenschutzbeauftragten erfolgen.

2. Aufsichtsbehördlich genehmigte Verbandsregularien

Eine gewisse Vereinheitlichung von Datenschutzstandards – jedenfalls per Branche – kann sich mit der Zeit auch dadurch ergeben, dass Verbände und andere Vereinigungen, die Kategorien von Unternehmen / bestimmte Branchen vertreten, Verhaltensregeln ausarbeiten, mittels welcher die DSGVO in der ein oder anderen Hinsicht präzisiert bzw. für die Praxis besser anwendbar / handhabbar macht. Dies kann sich etwa beziehen auf die Formulierung berechtigter Interessen, die Entwicklung von Standards, bei deren Einhaltung von einer technisch sicheren EDV-Anlage ausgegangen werden kann, Pseudonymisierung von Daten, die Ausübung von Rechten der Datenbetroffenen usw. Derartige Verhaltensregeln können der Aufsichtsbehörde zur Genehmigung vorgelegt werden, dort genehmigt, in ein Verzeichnis aufgenommen und veröffentlicht werden. Bei grenzüberschreitender Datenverarbeitung können solche Verhaltensregeln nach einem Abstimmungsverfahren zwischen lokaler und europäischer Aufsichtsbehörde sogar im Nachgang durch die EU-Kommission für allgemeinverbindlich erklärt werden. Derartige Verfahren würden in jedem Fall einen Gewinn an Rechtssicherheit mit sich bringen.

KONKRET gilt auch hier die Feststellung, dass sich das vorgeschriebene Thema – Verbände stellen Verhaltensregeln auf, Behörden genehmigen sie, hieraus entsteht eine Art offizielle Auslegung der DSGVO – bestenfalls in einem Anfangsstadium befindet, ja nur befinden kann. Auch hier gilt, dass die weitere Entwicklung durch unseren Datenschutzbeauftragten im Auge behalten werden soll.

VII. Zusammenarbeit mit Dritten

Die DSGVO regelt eine Vielzahl von Fällen, in denen es in Bezug auf Datenverarbeitungsvorgänge zur Beteiligung Dritter kommt. Dort können z.B. Daten gewonnen werden, oder man lässt sie dort verarbeiten. Auch konzernangehörige Unternehmen sind für die DSGVO zunächst einmal „Dritte“. Besondere Anforderungen entstehen, wenn involvierte Dritte sich im Ausland befinden.

1. Kooperation mit sog. Auftragsverarbeitern

Unter einem Auftragsverarbeiter versteht man eine Partei, die im Auftrag einer anderen Partei für diese Daten verarbeitet. Da der Begriff der Datenverarbeitung nach der DSGVO sehr weit ist und z.B. auch reines Speichern, Offenlegen und Löschen umfasst, gelangt jede größere Organisation, die nicht alles selber macht, schnell in den Anwendungsbereich der Zusammenarbeit mit einem Datenverarbeiter. Wir nehmen die Dienste der folgenden Datenverarbeiter in Anspruch:

Steuerberatung und Wirtschaftsprüfung

Rechtsanwälte Maas & Kollegen, Düsseldorf

KONKRET bedeutet dies für uns, dass wir in Bezug auf vorgenannte Parteien (und alle weiteren, die anderen Stelle treten oder diese ergänzen) die folgenden Vorgaben zu beachten bzw. unsere Rechte wie folgt auszuüben haben:

- es muss ein schriftlicher (hilfsweise elektronischer) Vertrag mit dem jeweiligen Auftragsverarbeiter abgeschlossen werden, in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und (auch) die Pflichten und Rechte unseres Unternehmens geregelt sind;

- der Auftragsverarbeiter muss uns gegenüber die Einhaltung der Anforderungen der DSGVO garantieren;

- eine allgemeine Zustimmung zum Einsatz von Subunternehmen an den Auftragsverarbeiter wird diesseits nicht erteilt, allenfalls kann diese im Einzelfall gewährt werden;

- verarbeitet werden darf nur auf unsere zu dokumentierende Weisung;

- der Auftragsverarbeiter muss nachgewiesen haben, dass dessen Mitarbeiter einer vertraglichen oder gesetzlichen Vertraulichkeitsverpflichtung unterliegen;

- der Auftragsverarbeiter gewährleistet eine technisch sichere Datenverarbeitung;

- es ist vertraglich abzusichern, dass der Auftragsverarbeiter uns unterstützt bei der Abhandlung geltend gemachter Betroffenenrechte, der Zusammenarbeit mit Behörden insbesondere im Fall von Datenpannen, und die gesetzlichen Voraussetzungen einhält, falls er selbst mit einem Datenverarbeiter in Erfüllung der Pflichten uns gegenüber zusammenarbeitet;

- es ist ebenfalls vertraglich abzusichern, dass nach Beendigung des Vertragsbeziehung mit dem Datenverarbeiter dieser in Ermangelung einer gesetzlichen Aufbewahrungspflicht die durch ihn verarbeiteten Daten nach unserem Wunsche entweder löscht oder retourniert und er alle erforderlichen Informationen zum Nachweis der Einhaltung seiner vertraglichen

und gesetzlichen Pflichtendarüber anliefert und eine durch uns ggfs. angesetzte Prüfung ermöglicht und unterstützt.

Außerdem ist durch unseren Datenschutzbeauftragten zu monitoren, ob die Aufsichtsbehörde und / oder die EU-Kommission von ihren Möglichkeiten Gebrauch machen, für Verträge mit Auftragsverarbeitern Standard-Klauseln zu entwickeln und ob es, sobald diese vorliegen, sinnvoll ist, selbige einzusetzen.

2. Datengewinnung bei Dritten und Informationsrechte des Betroffenen

Zuweilen ist es notwendig, Daten bei Dritten zu erheben, wobei dies grundsätzlich „2. Wahl“ bleiben und die Erhebung beim Betroffenen den Regelfall darstellen sollte. Da das Vorliegen eines berechtigten Interesses in Bezug auf die Dritterhebung zwar durchaus vorliegen kann, aber jeweils nachgewiesen werden muss – einschließlich des Überwiegens gegenüber den Interessen des Betroffenen – stellt es für gewöhnlich den einfacheren Weg dar, vom Betroffenen hierzu eine Einwilligung einzuholen.

KONKRET bedeutet dies für uns den Vorrang der Einholung einer Einwilligung des Betroffenen zur Erlangung der Drittinformation. Sollte eine solche Einwilligung nicht zu erlangen, die Erhebung der Daten für legitime Zwecke indes notwendig, sollte das hieraus resultierende berechtigte Interesse, auch in Abwägung mit jenem des Betroffenen, kurz in Vermerkform zum betreffenden Datenbestand dokumentiert werden. Ist das Überwiegen unseres Interesses gegenüber jenem des Betroffenen zweifelhaft, ist der Rat des Datenschutzbeauftragten einzuholen. Ferner haben wir den Betroffenen im Nachgang zur auf diese Weise (d.h. zustimmungslos) erfolgten Datenerhebung nach Art und Umfang spätestens innerhalb eines Monats nach Erlangung der so erhobenen Daten zu unterrichten. Dies unterbleibt nur dann, wenn uns die Erfüllung dieser Pflicht unmöglich ist oder mit unverhältnismäßigem Aufwand verbunden wäre; ist letzteres zweifelhaft, soll wiederum der Rat des Datenschutzbeauftragten eingeholt und seine Empfehlung bei der zu treffenden Entscheidung maßgeblich berücksichtigt werden.

3. Weiterleitung an Dritte

Die Weiterleitung von Daten an Dritte ist (abgesehen vom Sonderfall der Weiterleitung in ein Land außerhalb der EU, in welchem die DSGVO nicht gilt, siehe dazu folgenden Unterabschnitt 5.) von der DSGVO nicht eigens erfasst, vielmehr stellt dies einen „normalen“ Datenverarbeitungsvorgang in Form der Offenlegung durch Übermittlung dar, und zwar auch dann, wenn dies innerhalb von Konzerngesellschaften geschieht. Es gibt insoweit also keine „Privilegierung im Konzern“, sondern jedes einzelne Unternehmen innerhalb einer solchen Gruppe ist selbst Datenverantwortlicher, wenn es Daten übermittelt oder empfängt.

KONKRET muss daher auch insoweit mit Einwilligungslösungen gearbeitet werden, oder aber es muss ein berechtigtes Interesse für die Übermittlung nachgewiesen werden können, was umso eher gelingen wird, je enger die vertragliche oder gesellschaftsrechtliche Verbindung mit dem Dritten beschaffen und je stärker dessen (legitime) Einbindung in die Erfüllung vertraglicher oder gesetzlicher Pflichten gegenüber dem Betroffenen ist. Auch hier sollte wieder eine Dokumentation der Beschaffenheit solchen Interesses erfolgen.

4. „Korrektur-Wasserfall“ Richtung Dritter

Eine Besonderheit bei der Einschaltung Dritter besteht darin, dass eine unternehmerische Verpflichtung besteht, im Rahmen des Möglichen dafür zu sorgen, dass gewissermaßen in die Kette exportierte Fehler mit Datenbezug (Beispiel: wir haben über X eine falsche Information gespeichert und diese sodann an Y und Z weitergeleitet, Z seinerseits noch an A und B) berichtigt werden, sobald die Fehlerhaftigkeit der Daten erkannt wird.

KONKRET bedeutet dies für uns, dass wir bei Fehlererkennung in Bezug auf falsche Daten (auch unvollständige Daten können falsch sein, wenn gerade die Unvollständigkeit ein falsches Bild zeichnet), hinsichtlich derer wir Dritte involviert haben (z.B. durch Weiterreich solcher Daten an diese), eine sich in die Weg der Weiterleitung hinein

erstreckende Korrekturverpflichtung haben. Wir müssen die Sache also nicht nur in unserer eigenen Administration „geraderücken“, sondern auch dafür sorgen, dass die Korrekturbotschaft bei unseren unmittelbar oder mittelbaren (sofern bekannt) Empfängern ankommt. Dies gilt nicht nur für falsche Informationen, sondern auch dann, wenn Betroffene uns gegenüber berechtigte Anträge auf Einschränkung oder Löschung ihrer Daten geltend gemacht haben. Von der Durchsetzung all solcher Rechte in der Kette (gleich ob Korrektur, Einschränkung oder Löschung) sind wir nur dann befreit, falls dies unmöglich oder mit unverhältnismäßigem Aufwand verbunden wäre. Steht eine solche Konstellation in Rede, soll unser Datenschutzbeauftragter hierzu eine Stellungnahme abgeben und diese bei der zu treffenden Entscheidung maßgeblich berücksichtigt werden. Sollte der Betroffene es verlangen, müssten so oder so die (uns bekannten) Dritten ihm gegenüber noch benannt werden.

5. Dritte im Ausland

Eine Übermittlung von Daten an Dritte im Ausland ist, wenn dieses Ausland weder innerhalb der Grenzen der EU liegt noch es um einen die drei EWR-Staaten Liechtenstein, Island oder Norwegen geht (die Schweiz zählt zwar auch zum EWR, hat die DSGVO jedoch nicht ratifiziert), nur unter sehr eingeschränkten Voraussetzungen möglich, namentlich wenn (vereinfacht):

- es einen sog. Angemessenheitsbeschluss der EU-Kommission gibt, aus welchem sich ergibt, dass das betreffende Drittland ein Datenschutzniveau gewährleistet, welches in etwas vergleichbar ist mit der DSGVO; oder

- es öffentlich-rechtliche Garantien für die Einhaltung der Prinzipien der DSGVO gibt oder dies auf vertraglicher Grundlage, welche zugleich behördliche Genehmigung erfahren hat, garantiert worden ist; oder

- es einen Konzernverband gibt, der sich in ein Drittland erstreckt, und die Übermittlung nur innerhalb dieser Gruppe erfolgt, wenn es für diese Gruppe zugleich rechtlich bindende Datenschutzvorschriften gibt, die behördlicherseits genehmigt worden sind; oder

- eine ausdrückliche Einwilligung vorliegt oder erforderlich ist für die Erfüllung eines Vertrages oder die Durchführung vorvertraglicher Maßnahme oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder ein sonstiger, in der DSGVO in diesem Zusammenhang abschließend aufgezählter besonderer Recht(fertigung)sgrund vorliegt.

KONKRET hat dies für uns zur Folge, dass wir Daten an Dritte, die sich sowohl außerhalb der EU als auch außerhalb der Länder Liechtenstein, Island oder Norwegen befinden, nur dann übermitteln dürfen, wenn – neben den allgemeinen Voraussetzungen für die Rechtmäßigkeit der Datenverarbeitung unter Einbeziehung Dritter – wenigstens eine der vorgenannten Voraussetzungen erfüllt ist.

VIII. Zum Umgang mit spezifischen Kundenrechten („Rechte-Katalog“) in Sachen Datenschutz

Eine wesentliche, durch die DSGVO eingeführte Neuerung im Datenschutzrecht besteht darin, dass der Betroffene (Kunde etc.) gegenüber dem datenverantwortlichen Unternehmen mit einem umfangreichen Rechtekatalog ausgestattet worden ist, wobei diese Rechte teilweise auch nebeneinander und wiederholt geltend gemacht werden. Beim grundsätzlich reaktionspflichtigen Unternehmen kann dies zu einem nicht unerheblichen Verwaltungsaufwand führen.

1. Rechte im Einzelnen

Die Rechte, welche der Datenbetroffene hat, sind im Einzelnen in der uns von unseren Anwälten zur Verfügung gestellten Datenschutzerklärung (dortiger Abschnitt H.) erläutert worden. Der Datenbetroffene ist daher zwingend über seine Rechte so zu informieren, dass

er im Zeitpunkt unserer ersten Datenverarbeitung informiert und wirksam seine Einwilligung erklären konnte. Es handelt sich dabei um die folgenden Behelfe:

Auskunftsrecht, Widerrufsrecht, Berichtigungsrecht, Löschungsrecht, Einschränkungsrecht, Datenübertragungsrecht, Benachrichtigungsrecht, Beschwerderecht, Widerspruchsrecht sowie das Recht, nicht einer lediglich im automatisierten Verfahren getroffenen Entscheidung unterworfen zu werden, sofern diese gewisse Folgen für den Betroffenen hat.

Zur Vermeidung von Wiederholungen wird an dieser Stelle für (weitere) Einzelheiten zu diesen Rechten auf die entsprechenden Ausführungen in der Datenschutzerklärung verwiesen.

2. Reaktionsfristen und Dokumentation

KONKRET müssen wir berücksichtigen, dass der Betroffene einen grundsätzlichen Anspruch darauf hat, dass wir uns mit seinen Anträgen zur Ausübung der vorgenannten Rechte gewissenhaft und zeitnah auseinandersetzen und selbigen nur dann nicht stattzugeben brauchen, wenn der geltend gemachte Anspruch tatsächlich nicht besteht. Dies kann etwa der Fall sein, wenn es schon an einer Tatbestandsvoraussetzung für den in Rede stehenden Anspruch fehlt: wer die Berichtigung seiner Daten erreichen will, obwohl diese sachlich korrekt sind, kommt damit letztlich nicht zum Zuge. Wer seine Daten gelöscht sehen will, kann dies ebenfalls nicht durchsetzen, wenn selbst die insoweit kürzest denkbare gesetzliche Frist, welche das Unternehmen / uns zur (vorläufig weiteren) Aufbewahrung verpflichtet, noch nicht abgelaufen ist. In vielen Fällen hingegen wird die Entscheidung nicht so einfach zu treffen sein, vielmehr prinzipiell berechtigte Interessen von Betroffenem (Kunden etc.) und uns in Frontstellung zueinander geraten. Die Entscheidung pro oder contra geltend gemachtes Recht kann dann nur anhand einer umfassenden Interessenabwägung getroffen werden, an deren Ende ermittelt sein muss, welches Interesse im konkreten Fall höher zu bewerten ist. Nur selten wird demgegenüber ein Recht daran scheitern, dass es einen unverhältnismäßigen Aufwand bedeutete, ihm nachzukommen, oder es in rechtsmissbräuchlicher Weise geltend gemacht wurde. Auch insoweit soll für die näheren Einzelheiten auf Abschnitt H. der Datenschutzerklärung verwiesen werden. Eine Aufgabe für unseren Datenschutzbeauftragten liegt hier jedenfalls darin, unsere zeitgerechte Reaktion auf durch Betroffene geltend gemacht Rechte zu überwachen (namentlich den 1-3 Monatszeitraum) und sich zumindest in Fällen schwieriger Entscheidungsfindung mit einzuschalten, namentlich dann, wenn es um Interessenabwägungen geht. Zusätzlich hat er dafür zu sorgen, dass dann, wenn das seitens des Betroffenen geltend gemachte Recht durch uns zurückgewiesen wird, eine Dokumentation der Gründe für solche Ablehnung erfolgt.

3. Aufbewahrungsfristen

Es ist davon auszugehen, dass sich in der Praxis der Geltendmachung von Betroffenenrechten aus der DSGVO häufig ein (eventuell schon entstandenes) Recht auf Löschung von Daten und eine (eventuell noch bestehende) Pflicht zur Aufbewahrung derselben gegenüberstehen werden. Da die DSGVO selbst keine Aussagen dazu trifft, wie lange Daten aufbewahrt werden dürfen, wird die hier zu treffende Entscheidung letztlich in die Sphäre des nationalen Rechts zurückverlagert (da dies für jeden EU-Mitgliedstaat gilt, wird man in Europa mit unterschiedlichen Löschungsfristen zu tun bekommen). Für die Praxis besteht jenseits zwingender gesetzlicher Aufbewahrungsfristen ein gewisser Handlungsspielraum.

KONKRET wollen wir von diesem nach folgender Maßgabe mit den dort bestimmten Aufbewahrungsfristen Gebrauch machen:

(1) zu einem Vertragsverhältnis zwischen Kunde etc. und uns ist es nicht gekommen und selbiges ist auch nicht mehr zu erwarten, ebenfalls ist keine Situation entstanden, aus der sich eine Haftung (und sei es auch nur vorvertraglicher Art) ergeben könnte, Geschäftsbriefe o.ä. sind nicht ausgetauscht worden: 2 Jahre seit Letztkontakt, Fristbeginn mit Ablauf des Jahres des Letztkontakts (vgl. zu der Definition dieses Ereignisses unsere Datenschutzerklärung);

(2) zu einem Vertragsverhältnis zwischen Kunde etc. und uns ist es nicht gekommen und selbiges ist auch nicht mehr zu erwarten, Geschäftsbriefe o.ä. sind nicht ausgetauscht worden, eine Situation, aus der heraus eine Haftung (und sei es auch nur vorvertraglicher Art) gegen uns geltend gemacht werden könnte, ist nicht gänzlich auszuschließen: 3 Jahre seit Letztkontakt, Fristbeginn mit Ablauf des Jahres des Letztkontakts (vgl. zu der Definition dieses Ereignisses unsere Datenschutzerklärung);

(3) zu einem Vertragsverhältnis zwischen Kunde etc. und uns ist es gekommen oder aber nicht gekommen, es wurden Geschäftsbriefe o.ä. mit dem Betroffenen ausgetauscht: 6 Jahre seit Empfang oder Versendung des Geschäftsbriefs o.ä. Liegt der Letztkontakt innerhalb der 6-Jahresfrist und würde, ab diesem Ereignis gerechnet, die Frist von (1) oder (2) später enden als jene der 6 Jahre, so ist für das Fristende der spätere Zeitpunkt maßgeblich. Andere Daten als jene des Geschäftsbriefs sind, falls sie mit diesem nicht zusammenhängen, ab dem Datum des Letztkontakts nur während der Frist von (1) oder (2) aufzubewahren;

(4) zu einem Vertragsverhältnis zwischen Kunde etc. und uns ist es gekommen oder aber nicht gekommen, es existieren Buchungsbelege des Betroffenen oder dessen Daten machen Teil einer zusammenfassenden geschäftlichen Dokumentation (z.B. eines Lageberichts) aus oder sind enthalten in Zollunterlagen gem. Art. 15 I und / oder Art. 163 des Zollkodex der EU: 10 Jahre seit dem Buchungsdatum, dem Datum der vorgenannten Dokumentation bzw. jenem der Übermittlung an die Zollbehörden. Liegt der Letztkontakt innerhalb der 10-Jahresfrist und würde, ab diesem Ereignis gerechnet, die Frist von (1) oder (2) später enden als jene der 10 Jahre, so ist für das Fristende der spätere Zeitpunkt maßgeblich. Andere Daten als jene des Buchungsbelegs / Lageberichts etc. bzw. der Zollunterlagen sind, falls sie mit diesem nicht zusammenhängen, ab dem Datum des Letztkontakts nur während der Frist von (1) oder (2) aufzubewahren.

In Zweifelsfragen zu diesen Aufbewahrungsregelungen, namentlich welche ggfs. in einem konkreten Fall die richtige ist, ist der Datenschutzbeauftragte beizuziehen. Nach Ablauf der relevanten Aufbewahrungsfrist werden die Daten gelöscht (es sei denn, vom Betroffenen wurde zuvor ausdrücklich die Einschränkung statt der Löschung gefordert), es sei denn, dass diese (auch dann noch) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden.

4. Im Zweifel: Prüfung durch Rechtsanwalt

Die Ausübung der vielfältigen Rechte von Seiten Betroffener und der richtige Umgang mit selbigen kann recht komplex sein und hohe rechtliche Anforderungen stellen. Auch an dieser Stelle müssen wir daher besondere Gewissenhaftigkeit an den Tag legen.

KONKRET: so lange die Sachlage nicht ganz klar ist und nur (eher) untergeordnete Rechte geltend gemacht werden (Auskunft, Berichtigung, Übertragung), ist die Abhandlung von seitens Betroffener im Einzelfall geltend gemachten Rechten aus der DSGVO eine Aufgabe für unseren Datenschutzbeauftragten. Erforderlichenfalls, insbesondere bei schwierigen Rechtsfragen, die sich in diesem Zusammenhang stellen, hat er einen Rechtsanwalt beizuziehen.

IX. Zum Umgang mit nicht automatisierter Datenverarbeitung, Vermeidung von „Parallel-Administrationen“

Die DSGVO gilt sowohl für die automatisierte wie die nicht-automatisierte (i.e. manuelle) Verarbeitung von Daten. Offensichtlich können dadurch nicht wünschenswerte Paralleladministrationen entstehen, für welche schon aus faktischen Gründen keine einheitlichen Vorgaben einer datenschutzkonformen Behandlung erstellt werden können. Beispielsweise können manuell „gespeicherte“ (d.h. ohne technische Umwandlung

aufbewahrte) Daten weder verschlüsselt noch zentral zugänglich oder unzugänglich gemacht und dem Betroffenen auch nicht auszugsweise erteilt werden.

KONKRET soll ein Nebeneinander von automatisierter und nicht-automatisierter Verarbeitung von Daten vermieden werden. Erzeugnisse manueller Datenverarbeitung sind innerhalb einer Woche seit ihrer Erstellung in ein Format zu überführen, welches sich für eine automatisierte Verarbeitung eignet, und danach zu vernichten, es sei denn, dass gerade dem Original des Erzeugnisses ein besonderer Wert zukommt, was beispielsweise dann der Fall ist, wenn es im Rahmen eines Rechtsstreits vorzulegen ist, ihm eine Titelfunktion zukommt oder seine Wiederbeschaffung mit erheblichem Aufwand / Kosten verbunden wäre (z.B. notarielle Urkunden). Es kann jedoch auch Bereiche geben, die zwingend noch eine analoge Speicherung von Daten erfordert, weil sich diese Praxis über Jahre hinweg bewährt hat. Typischerweise ist hier die Human-Research Abteilung zu nennen. Sollten gewichtige Gründe dafür sprechen, diese Abteilung von der Digitalisierung auszunehmen, so kann die Speicherung auch weiter analog erfolgen. Es ist darauf zu achten, dass auch dies Art der Speicherung den Richtlinien zum Umgang mit Daten im Unternehmen entsprechen.

X. Zum Umgang mit juristischen Personen

Gem. den Buchstaben der DSGVO findet diese nur Anwendung auf Daten natürlicher Personen. Damit ist das letzte Wort jedoch noch nicht gesprochen. Zwar besteht Einigkeit, dass die Verordnung nicht gilt für die Verarbeitung personenbezogener Daten juristischer Personen (insbesondere Unternehmen), wenn es sich dabei um deren Basisdaten wie Name, Rechtsform oder Kontaktdaten der juristischen Person handelt. Andererseits hat die Rechtsprechung jedenfalls nach altem Recht (bzw. auf Basis der ohnehin stets aktuellen Grundrechte) entschieden, dass auch eine juristische Person (etwa eine GmbH) in einen personenbezogenen Kontext eingebettet sein kann, etwa wenn zwischen ihr und den „hinter“ ihr stehenden Personen eine enge wirtschaftliche Bindung bestehen, was sich auch durch eine finanzielle oder personelle Verflechtung äußern kann. Auch sonst sind Fälle denkbar, in denen hinter der juristischen Person stehende natürlichen Personen auch bei unternehmensbezogenem Handeln in erkennbarer Weise als solche hervortreten und damit eine ähnliche datenschutzrechtliche Betroffenheit erfahren wie sonstige natürliche Personen.

KONKRET wollen wir daher jedenfalls dann, wenn sich eine juristische Person in ähnlicher Lage befindet wie eine natürliche Person, also eine tatsächliche Betroffenheit in personenbezogenen Daten feststellbar ist, dieser denselben Schutz in datenrechtlichen Hinsicht zukommen lassen, als handelte es sich dabei um eine natürliche Person. Ist zweifelhaft, ob eine juristische Person ein solches personales Gepräge hat oder jedenfalls die hinter ihr stehenden Personen wie natürliche Personen vor dem rechtlichen Unternehmensmantel in Erscheinung treten, soll der Datenschutzbeauftragte über die Einordnung in die Kategorie „natürliche Person“ oder „juristische Person“ entscheiden und danach der entsprechende Datenschutzumfang eingerichtet werden.

XI. Sonderthema Mitarbeiter – Datenschutz, IT-Nutzung für private Zwecke

Die DSGVO enthält selbst keine besonderen Bestimmungen zum Thema (Sonder-)Schutz personaler Daten von Mitarbeitern des datenverarbeitenden Unternehmens. Im Gesetz ist lediglich eine Öffnungsklausel enthalten, welche es dem nationalen Gesetzgeber gestattet, für diesen speziellen Bereich eigene („spezifische“) Regelungen zu erlassen. Deutschland hat von dieser Möglichkeit im BDSG Gebrauch gemacht und dort bestimmte Sonderzwecke als zulässige Grundlagen für die Datenverarbeitung im Verhältnis Unternehmen – Arbeitnehmer benannt. So dürfen etwa personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über dessen Begründung oder nach dessen Begründung für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung)

ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Selbst besonders sensible Daten (Daten besonderer Kategorien) dürfen hier verarbeitet werden, wenn dies zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Auch entsprechende Einwilligungen sind möglich.

Die Nutzung der EDV / IT unseres Unternehmens für private Zwecke (der Mitarbeiter) birgt diverse Risiken. So kann es ohne weiteres zu einer Vermischung von Kundendaten mit Mitarbeiterdaten kommen, und unfreiwillig könnten auch unsere eigenen Verpflichtungen aus der DSGVO gegenüber unseren Mitarbeitern, quasi mitwachsend mit dem Umfang von deren Nutzung unternehmenseigener Infrastruktur für private Zwecke, erheblich ansteigen.

KONKRET bedeutet das für uns, dass wir auch an dieser Stelle grundsätzlich mit Einwilligungslösungen arbeiten werden, wobei hier – d.h. im Arbeitsverhältnis (oder dessen Anbahnungssituation) – in besonderer Weise darauf zu achten ist, dass die Einwilligung freiwillig erklärt wird, wobei die im Beschäftigungsverhältnis bestehende Abhängigkeit zwischen Arbeitgeber und (künftigem) Arbeitnehmer ebenso zu berücksichtigen ist wie die Umstände der Erteilung. Als Indikation für Freiwilligkeit kann gelten, wenn für den (anzustellenden) Arbeitnehmer ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder er und der Arbeitgeber gleichgelagerte Interessen verfolgen. Die Einwilligung soll zudem stets schriftlich erklärt werden.

Unsere technische Infrastruktur (EDV / IT, gleich ob Büro- oder Handgeräte) darf durch unsere Mitarbeiter nicht (mehr) für private Zwecke verwendet werden.

XII. Sonderthema Datenschutz-Folgenabschätzung

Bestimmte Betriebe sind verpflichtet, eine sog. Datenschutz-Folgenabschätzung durchzuführen. Darunter versteht man eine umfangreiche Risikoanalyse in Bezug auf die verarbeiteten Daten, Erwägungen zur Verhältnismäßigkeit von deren Speicherung, Sicherheitsvorkehrungen, Abhilfemaßnahmen etc. Diese Verpflichtung besteht jedoch nur, wenn unter Datenschutzgesichtspunkten besonders risikogeneigte Verarbeitung stattfindet, etwa systematische Bewertung persönlicher Aspekte natürlicher Personen / Profiling oder umfangreicher Umgang mit besonders sensiblen Daten. Dies findet bei uns nicht statt.

KONKRET müssen wir hier nichts weiter veranlassen.

XIII. Ungeklärte Probleme

Es gibt bislang noch eine Vielzahl ungeklärter Probleme im Zusammenhang mit der DSGVO, nicht zuletzt zu Fragen des Löschens. Insbesondere relevant ist hierbei die Frage, ob für das geforderte Löschen ein computermäßiges Löschen ausreicht und ein definitives Löschen (einhergehend mit der technischen Unmöglichkeit der Wiederherstellung) erforderlich ist. Bis zur Klärung dieser Frage wäre die letztere Variante als sicherer im Hinblick auf Konformität mit der DSGVO anzusehen.

KONKRET werden wir erforderliche Löschungsvorgänge als endgültige (d.h. nicht wiederherstellbare) Löschung gestalten und zugleich dafür Sorge tragen, dass flächendeckend gelöscht wird, also Backup-Systeme etc. miterfasst werden.

XIV. Aufsichtsbehörde, Monitoring Rechtsentwicklung, Sonstiges

Die für uns zuständige Aufsichtsbehörde ist:

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Kavalleriestr. 2-4, 40213 Düsseldorf, Telefon: 0211/38424-0, Fax: 0211/38424-10, E-Mail: poststelle@ldi.nrw.de

Die weitere Rechtsentwicklung in Bezug auf das Thema DSGVO, soweit für uns relevant, soll durch unseren Datenschutzbeauftragten im Auge behalten und Anpassungsbedarf hinsichtlich unserer Datenschutzerklärung, Einwilligungserklärungen, internen Unternehmensorganisation etc. unverzüglich signalisiert werden.

Für eventuelle technische Fortentwicklungen in Bezug auf das Thema Datensicherheit und den dabei zu beachtenden, guten Standard, können weitere Erkenntnisse durch gelegentliche Besuche der folgenden Website gewonnen werden:

https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html;jsessionid=B236788418B2A295D3B20C7DB300D377.1_cid351