ZENTRALVERBAND DES DEUTSCHEN FRISEUR HANDWERKS

Roadmap neuer Datenschutz

Am 25.Mai 2018 tritt die neue Datenschutzgrund-Verordnung (DSGVO) in Kraft. Zuvor erfolgte eine Anpassung des Bundesdatenschutzgesetzes (BDSG 2018 neu). Über diese Entwicklung hatten wir unter verschiedenen Aspekten informiert und 2 umfangreiche Leitfäden des ZDH, speziell an die betroffenen Betriebe und an die Innungen gerichtet, weitergeleitet.

Der 25. Mai 2018 ist einerseits ein wichtiges Umsetzungsdatum – andererseits sind viele Fragen hinsichtlich Anforderungen und Umsetzung gerade in kleineren Betrieben nicht ausreichend geklärt. Dazu kommt, dass kleine Betriebe mit einem an Großbetrieben und international agierenden Handelsunternehmen orientierten Regelungsniveau schlichtweg überfordert sind. Das schafft ein hohes Maß an Verunsicherung. Was muss zuerst und was muss überhaupt angegangen werden – und wo ist Vorsicht vor allzu geschäftstüchtigen Offerten geboten?

Mit einer kleinen Roadmap wollen wir eine pragmatische Handlungsorientierung unter Abwägung der Risiken geben. Hier ein kleiner **Überblick über die Themenbereiche:**

1. Positiv ist: Friseurbetriebe müssen in der Regel **keine Datenschutzbeauftragten** (weniger als 10 Mitarbeiter, die dauerhaft mit personenbezogener Datenverarbeitung befasst sind) bestellen und auch kein aufwendiges **Verfahrensverzeichnis** (unter 250 Mitarbeiter und keine negative Folgeabschätzung) erstellen oder schwierige **Risikofolgeabschätzungen** vornehmen. Ein **Zertifizierungsverfahren** ist ebenfalls nicht erforderlich.

2. **Datenschutz ist/wird Chefsache** – auch die neue Rechtslage verlangt eine klare Verantwortung. Ggf. sollte ein Stellvertreter für längere Abwesenheiten und Urlaubszeiten auch für diesen Bereich beauftragt werden. Chefsache bedeutet, *dass der Betriebsinhaber selber erwägen muss, ob durch die Verwendung personenbezogener Daten im eigenen Betrieb die Rechte und Freiheit seiner Kunden (und auch Mitarbeiter) unzulässig eingeschränkt werden.*

3. Besonders zu beachten ist, dass Friseurbetriebe z. T. und in unterschiedlichem Umfang **gesundheitsbezogene Daten** im Sinne des Datenschutzes erheben. Dies geschieht in erster Linie in Zusammenhang mit der vertraglichen Leistungserbringung.

4. Neu ist eine **Informationspflicht**: Die Betriebe müssen ihre Kunden darüber informieren, welche Daten, warum anlassbedingt oder dauerhaft gespeichert werden und was mit diesen geschieht. Es besteht bei der zuständigen Datenschutzbehörde eine **Meldepflicht** bei Hacking und unbefugtem Datenzugriff.

5. Statt großbetrieblichem **Daten-Managementsystem** empfiehlt sich momentan die Nutzung eines ***wachsenden Ordnersystems*** mit allen in Frage kommenden Unterlagen und nützlichen „Tools" - zur Dokumentation der eigenen Maßnahmen und deren Kontrolle bzw. später erforderlichen Überarbeitung und entsprechender Änderungen einzelner Vorgänge.

6. Ob die große **Kontroll- und Bußgeldwelle** nach dem 25.Mai 2018 ausbricht, ist trotz teilweise kursierender Behauptungen und überzogener Vorstellung in der Berater- und Dienstleisterscene absolut fraglich. Es ist aber von einer zunächst hinweisorientierten und abgestuften Vorgehensweise auf der Grundlage eines zu beantwortenden Fragebogens der zuständigen Ämter für Datenschutz auszugehen. Im Vordergrund werden Hinweise und Hilfestellungen sowie die Klärung von Frage- und Problemstellungen stehen. Erst bei beharrlich unkooperativem und beratungsresistentem Handeln sowie vorsätzlicher Missachtung datenschutzrechtlicher Vorgaben kommen Bußgeldsanktionen in Relation zu den konkreten Umständen und Firmenverhältnissen in Frage.

7. Wir werden im Rahmen der weiteren Entwicklung und sich klärender Einzelfragen ein **Beantwortungskonzept** für diese sehr umfangreichen Fragebögen entwickeln, das deren Erledigung erheblich vereinfachen und restliche Risiken oder weitere Kontrollmaßnahmen weitgehend verhindern soll. Trotzdem müssen aber die erforderlichen Maßnahmen aktiv umgesetzt und im Betriebsalltag auch konsequent realisiert werden.

8. Insbesondere ist die konkrete Handhabung von **Kundenbeschwerden** oder darauf beruhende Änderungsverlangen als Chefsache unmittelbar umzusetzen. Hier droht andernfalls das Risiko, dass betroffene Kunden eine Beschwerde bei der zuständigen „Datenschutzbehörde" einreichen, womit man in den Fokus des dortigen Interesses gerückt würde. Solche Konstellationen gilt es möglichst zu vermeiden.

Roadmap

Webpräsenz

1. **Internetauftritt** – alleine schon durch das Betreiben einer Website entstehen Datenkontakte und werden personenbezogene Daten gespeichert. Je nach weiterer Ausgestaltung mit interaktiven Elementen, Bestellfunktionen und/oder Newsletter-Funktionen werden in umfassender Weise Daten verarbeitet und gespeichert. Das erfordert die Berücksichtigung verschiedener datenschutzrechtlicher Anforderungen bei Errichtung der Website. So muss z. B. auch den neuen datenschutzrechtlichen Anforderungen (z. B. in Form einer aktualisierten Datenschutzerklärung nach neuer DSGVO) einschließlich der speziell erforderlichen Einwilligungserklärungen genüge getan werden. Generell muss auch das **Impressum** entsprechend der Vorgaben des Telemediengesetzes gestaltet werden. In der Regel sollte dies Teil eines Auftragsverhältnisses mit einem professionellen Dienstleister bzw. Webdesigner sein.
   Aufgrund der besonderen Anforderungen und der jederzeitigen Überprüfung der Internetpräsenz durch Dritte, einschließlich des dadurch bedingten wettbewerbsrechtlichen Abmahnrisikos, sind in diesem Bereich Gefälligkeitsverhältnisse oder Do-it-Yourself nicht empfehlenswert. Deshalb sollte auch der Dienstleister oder ein entsprechend qualifizierter Berater mit der Überprüfung und der Umstellung bzw. Ergänzung des Internetauftritts beauftragt werden. Einige Stichworte zu den einzelnen Themenbereichen:

   a. **Datenschutzerklärung**

      Wozu dient eine Datenschutzerklärung? Gemäß **Telemediengesetz** (TMG) hat jeder Websitebetreiber den Websitebesucher „zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten […] in allgemein verständlicher Form zu unterrichten“ (§ 13 Abs. 1 S. 1 TMG). Auch nach der neuen DSGVO müssen Websitebetreiber mit einer **Datenschutzerklärung** umfassend über die Datenerhebung und -verarbeitung auf ihrer Website informieren.

      Dabei gilt es, nicht nur über eigene Verarbeitungen (etwa mittels Kontaktformular) aufzuklären, sondern auch über die Erhebung und Verarbeitung von in die Website eingebundenen Diensten wie z. B. Social-Sharing, Social-Sign-In, Website-Nutzungsanalysen oder Retargeting. Details zur Verarbeitung in datenschutz-kritischen Staaten (z. B. den USA) dürfen dabei ebenso wenig fehlen wie das Angebot einer rechtskonformen Widerspruchsmöglichkeit.

      Die Datenschutzhinweise müssen jederzeit von jeder einzelnen Website des Webauftritts erreichbar sein. Hierzu sollten die Hinweise mit einem Link „Datenschutzhinweise“ oder „Datenschutzerklärung“ verknüpft werden. Fehlerhafte oder gar fehlende Hinweise können von Mitbewerbern und Verbraucherverbänden abgemahnt werden. Die Datenschutzaufsichtsbehörden haben in der Vergangenheit bereits hohe Bußgelder für unzureichende Datenschutzerklärungen verhängt.

Es gibt in diesem Zusammenhang eine Reihe von angebotenen Musterformulierungen die als Formulierungshilfe genutzt werden können und gesonderter anwaltlicher Überprüfung bedürfen. (Z. B.: https://www.datenschutz.org/datenschutzerklaerung-muster.pdf). Ebenso gibt es Dienstleistungsanbieter für kostenlose oder kostenpflichtige Datenschutzerklärungsgeneratoren, die teilweise auch rechtliche Garantien abgeben.

b. Newsletter – erfordert einen **„**Einwilligungsbutton“ und Abbestellhinweis mit den erforderlichen Verfahrens- und Adresshinweisen.

Weitere Hinweise enthält unser anliegendes Arbeitspapier „Handlungsaspekte bzgl. der eigenen Webseite“ sowie das Entwurfspapier „Erklärung zu Datenschutz“. Diese Unterlagen sollen die Orientierung und eine professionelle Betreuung erleichtern, können diese in der Regel aber nicht ersetzen. Die Musterdatenschutzerklärung der Firma datenschutz.org. ist ein Beispiel für eine allerdings kostenpflichtig im Internet zu generierende Datenschutzerklärung.

2. **Datensicherheit –** die Datensicherheit einer EDV-Anlage ist ebenfalls durch professionellen Support sicherzustellen und dauerhaft zu gewährleisten. Zu diesem Themenbereich stellen wir ein weiteres Arbeitspapier mit Stichworten möglicher Themen bzw. Prüfungsschritte anliegend zur Verfügung.

3. Im Falle eines **Datencrashs** oder **Hackings** können ggf. besondere Informations- oder auch Meldepflichten gegenüber dem zuständigen Landesamt für Datensicherheit entstehen. (Z. B. www.datenschutz-berlin/meldung-datenleck.html)

4. **Verschwiegenheitsanweisung** gegenüber Mitarbeitern im Umgang mit Daten

   In kleineren Betrieben wird es keines speziellen Vertraulichkeitsmanagements bedürfen. Es bedarf aber einer grundsätzlichen Anweisung, wie Mitarbeiter mit personenbezogenen Daten im Salon umzugehen haben und wie ggf. Daten in der Kundendatei, im Kassensystem oder im PC zu erfassen sind. Weiterhin sollte eine auch diesen Bereich regelnde arbeitsrechtliche Verschwiegenheitserklärung - ggf. aktualisiert oder grundsätzlich neu – zu der Personalakte genommen werden. (Vgl. auch den ebenfalls anliegenden Entwurf einer *Verpflichtungserklärung zur Einhaltung der datenschutzrechtlichen Anforderungen* nach der Datenschutz-Grundverordnung (DSGVO))

Besonderer Umgang mit Kundendaten

1. Umgang mit Kundendaten und Einwilligung

Persönliche Daten dürfen nur verarbeitet oder genutzt werden, wenn eine gesetzliche Erlaubnis besteht oder der Kunde zuvor einwilligt. Im Friseurhandwerk stehen eine Reihe von Kundendaten in einem engen Zusammenhang mit der Abwicklung des vertraglichen Verhältnisses. So ist z. B. für die Terminvergabe und das Reservierungsmanagement mindestens zur Identifizierung des Kunden die Bekanntgabe und Erfassung des Kundennamens nebst einer Telefonnummer und ggf. anderer Kommunikationsdaten (z. B. eine E-Mail-Adresse) erforderlich. In solchen Fällen jedes Mal eine umfangreiche schriftliche Einwilligungserklärung mit Widerrufsbelehrung einzufordern, erscheint unverhältnismäßig und überzogen.

Die Erfassung wiederum der Wohnsitzanschrift macht zu diesem Zweck wenig Sinn. Dient das aber zur werblichen Kontaktaufnahme, bedarf es der ausdrücklichen Einwilligung. Ob eine solche in Schriftform zu erfolgen hat oder zumindest mündlich erklärt werden kann, ist eine Frage der Abwägung. Wer z. B. auf die Frage, „dürfen wir Ihnen zum Geburtstag gratulieren", sein Geburtsdatum nennt, willigt zumindest ein, dass man dieses Datum auch festhält. Für systematische Geburtstags- und Werbemails wird dies überwiegend anders gesehen; zur Dokumentation und aus Beweisgründen wird vielfach Schriftform empfohlen. Ein einfaches und vor allem in allen Salonsituationen praktikables Schema scheint es nicht zu geben. Vielmehr zeichnet sich ab, dass unterschiedliche Maßnahmen bei Verwendung unterschiedlicher personenbezogener Daten naheliegen oder sogar erforderlich sind:

2. **Differenzierung bei Kundendaten erforderlich** – unterschiedliche Handlungsanforderungen mit zum Teil ungeklärten Fragen bei Kollision von Rechtspflichten des Betriebes mit dem Persönlichkeits- bzw. Datenschutz von Kunden.

1. Datenverarbeitung zur **Termin- und Reservierungs-Koordination**
    a. dient der vertraglichen Abwicklung

2. Datenverarbeitung und -nutzung für **werbliche Zwecke**
    a. steht in der Regel unter Einwilligungsvorbehalt

3. Datenverarbeitung zur Erfüllung **steuerlicher Zwecke**

    a. dient dem steuer- und abgabenrechtlichen Einzelnachweis aufgrund §§ 146 a, b AO in Verbindung mit den GoBD-Grundsätzen in Konkretisierung des BMF-Schreibens vom 7. Dezember 2017 (Einzelaufzeichnungspflicht bei bekannten Kunden zumutbar).

    b. Aufbewahrung von Terminbüchern und Kundendateien sind bei steuerlichen Prüfungen und Verprobungen erforderlich.

4. Verarbeitung **gesundheitsbezogener Daten** (Vgl. w.u.).

5. Empfehlung: Keine Datenerhebung zur Erstellung von **Kundenprofilen** und Marktforschung.

Besondere Aspekte gesundheitsbezogener Daten

Gesundheitsbezogene Daten gelten datenschutzrechtlich genauso wie z. B. ethnische, religiöse und geschlechts- sowie sexualitätsbezogene Informationen und Daten als besonders schutzwürdig. Daraus ergeben sich in Bezug auf das Friseurhandwerk besondere Problemstellungen in Zusammenhang mit der **Anwendung haarkosmetischer Produkte** im Bereich der **Farb- und Strukturveränderung**, die gesundheitsrelevant angewendet werden müssen. Die übliche Praxis, die Produktanwendung (Produkt, Menge, Abmischung, Behandlungsverlauf, Nachbehandlung, Wärmezufuhr u. dergl.) in der Kundenkartei kundenbezogen zu dokumentieren, gehört zu der vertraglichen Abwicklung und den vertraglichen Nebenpflichten. In diesem Zusammenhang sind auch die kosmetikrechtlichen Allergiehinweise und Garantenpflichten der Friseure als Anwender zu sehen. Dies zu dokumentieren, steht im Interesse des Betriebes, aber auch des Kunden, wenn nachträglich

Probleme auftreten und eine spätere produktbezogene Abklärung erforderlich wird. Dies von einer besonderen Einwilligung des Kunden abhängig zu machen, dürfte wenig praktikabel sein, da sehr umfangreiche und ggf. detaillierte Anwendungen erforderlich sind. Damit wird auch die Frage einer schriftlichen Risikoaufklärung und -bewertung aufgeworfen.

Kunden- und praxisgerechter dürfte es sein, vor einer solchen haarkosmetischen Behandlung, die auf der Umverpackung oder dem Beipackzettel enthaltenen Hinweise in Bezug auf allergische Risiken und evtl. besondere Risikodispositionen zu geben und mögliche Kontraindikationen abzuklären. Ggf. ist dem Kunden eine fachärztliche Abklärung anzuraten. Danach könnte mit dem Kunden mündlich vereinbart werden, dass das verwendete Produkt und die Abmischungsverhältnisse – nicht zuletzt auch im Eigeninteresse des Kunden für evtl. Nachfragen oder spätere Abklärung möglicher Ursachen – festgehalten wird. Zusätzlich empfiehlt sich der Vermerk, dass ein der Produktkennzeichnung entsprechender Risikohinweis ergangen ist.

Weitere Gesundheits- und/oder Krankendaten sollten nach unserer Einschätzung in diesem intimen und höchstsensiblen Bereich grundsätzlich nicht erfasst oder dokumentiert werden. Andererseits macht es bei diesem pragmatisch auf das notwendigste reduzierten Handling im Bereich von Farb- und Strukturbehandlungen Sinn, aufgrund einer mündlichen Zustimmung so zu verfahren. Vielleicht hat das im Endeffekt weniger Beweiswert als ein schriftlich archiviertes Dokument. Als übliche Verfahrensweise in diesem Bereich und regelmäßiges Element in der Kundenkommunikation wird das aber zum akzeptierten Standard. Dazu kommt noch, dass der Kunde möglichweise unter Umständen sogar einen Auskunftserteilungsanspruch in Bezug auf die Behandlungsdaten haben könnte. Art. 20 DSGVO enthält einen Daten-Rückübertragungsanspruch, der durchaus in diesem Sinne verstanden werden kann.

Dem entsprechende und eindeutige **Mitarbeiteranweisungen** sind unbedingt zu erteilen; ebenso bedarf es einer Verschwiegenheitsvereinbarung mit den Mitarbeitern, die insbesondere diesen sensiblen Bereich einbezieht. (Vgl. auch den anliegenden Entwurf einer Verschwiegenheitsverpflichtung)

Soweit in der Salonpraxis in der Kundenkommunikation gesundheitsbezogene Informationen offenbart werden, gilt auch unter dem Gesichtspunkt des **allgemeinen Persönlichkeitsschutzes** besondere Verschwiegenheit und Nicht-Erfassung dieser Informationen. Sollten sich bei der Behandlung Krankheitsbilder oder **besondere Gesundheitsgefahren** offenbaren (z. B. Kopfhautprobleme, Haut- und Infektionskrankheiten, Läusebefall) sind ggf. entsprechende Hinweise an den Kunden zu geben und erforderliche Maßnahmen zu treffen. Von einer Dokumentation bzw. Datenspeicherung sollte, außer im Falle gesetzlicher Meldepflichten) abgesehen werden.

In Zusammenhang mit der Erbringung und Abrechnung **medizinischen Haarersatzes** dürfen nur Daten zu diesem Zweck erhoben, genutzt und gespeichert werden; auch nur so lange, wie es zur Erfüllung vertraglicher Zwecke und zur Gewährleistung erforderlich ist. Andere als vertragliche und abwicklungstechnische Zwecke dürfen nicht verfolgt werden.

Unklar ist momentan, ob und welche Vorgaben dazu momentan seitens der Leistungsträger und des GKV-Spitzenverbandes gemacht werden. Im Rahmen des Auftragsverhältnisses und der vertraglichen Abwicklung ist ein grundlegendes Einverständnis mit der Datenverwendung zu diesem Zweck zu unterstellen. Ein Einwilligungsvorbehalt des Leistungsempfängers bzw. Kunden würde keinen Sinn machen, da damit die Auftragsrealisierung gehindert würde. Medizinische Daten, Diagnosen und gesundheitsbezogene Sekundär-informationen, die für

die Abwicklung oder konkrete Gestaltung des Haarersatzes nicht relevant sind, sollten auf keinen Fall gespeichert werden. Im Übrigen ist in diesem höchst persönlichen und intimen Bereich in ganz besonderer Weise Diskretion und Schutz der Kunden geboten.

Im Präqualifizierungsverfahren als Voraussetzung für die erleichterte Abrechnung von Haarersatz mit den Versicherern wird dieser Situation hinsichtlich der Anforderungen ebenso Rechnung getragen.

In diesem Kontext stellt sich auch die Frage, ob es einen Rechtsanspruch eines Leistungsempfängers gibt, das bereits erhobene **Daten** (z. B. Vermessungsergebnisse, Planung einer Perücke, technische Daten, Anpassungsverlauf etc.) bei Wechsel zu einem anderen Leistungserbringer oder später **übertragen werden müssen**. Dies wird man unter Berücksichtigung der neuen DSGVO bejahen müssen.

Besonderer Umgang mit Mitarbeiterdaten

1. **Personaldaten** von Mitarbeitern sind Verschlusssache und sind vor dem Zugriff Dritter und Unbefugter zu schützen (abschließbarer Schrank). Für eine EDV-Anlage sind mindestens ein effizienter Password-Schutz und eine funktionierende Firewall erforderlich (Hinsichtlich der Hard- und Software-Voraussetzungen vgl. auch das Papier zur technischen und organisatorischen Umsetzung)

2. Vertragliche Regelungen der **„Auftragsdatenverarbeitung“**, z. B. in Bezug auf das Steuerbüro oder Dienstleister, die Personaldaten (gilt auch für Kundendaten) verarbeiten, sind in allen Fällen zu treffen. Wir gehen davon aus, dass die Steuerberater und Buchhaltungsdienstleister, aber auch professionelle Dienstleister im EDV- und Web-Design-Bereich mit Vertragsmuster auf ihre Kunden zukommen.
   (Vgl. auch Textbeispiel aus dem EDV-Bereich).

3. Einwilligung der Mitarbeiter bei **Nutzung von Fotos bzw. Teamfotos** und Veröffentlichung anderer persönlicher Daten auf der Website des Salons erforderlich
   a. Bilder von Mitarbeitern stehen aufgrund des Rechtes am eigenen Bild immer unter Zustimmungsvorbehalt des abgebildeten Mitarbeiters
   b. hinsichtlich der Berufsqualifikation ist eine Veröffentlichung vertretbar, soweit sie in Zusammenhang mit der Ausübung der Tätigkeit steht

4. Die **saloninterne Veröffentlichung** von einkommens- oder leistungslohnrelevanten individuellen Umsatzzahlen bzw. die Veröffentlichung solcher Daten bedarf ebenfalls einer individuellen Vereinbarung.

5. Die Veröffentlichung von **Fotos von Kunden** sind aufgrund des Rechtes am eigenen Bild und nach überwiegender Auffassung als personenbezogener Datensatz immer erlaubnispflichtig.

Bußgeldrisiken und Beantwortungskonzept für Fragebögen der Landesdatenschutzämter

Entgegen vielfacher Beschwörungen aus der Datenschutzberaterszene ist mit einer grassierenden **Bußgeldwelle** mit exorbitant hohen Bußgeldern nicht zu rechnen. Es wird vielmehr eine Hinweis- und Beratungstätigkeit Vorrang haben. Erst bei erkennbar unkooperativem Verhalten und vorsätzlichen Verstößen oder der Verweigerung von berechtigten Abänderungsverlangen ist mit verhältnismäßigen Bußgeldern zu rechnen. Gleichwohl sind die wichtigen dargestellten Punkte anzugehen.

Die **Landesdatenschutzämter** werden mit relativ detaillierten und komplizierten **Fragebögen** auf die Betriebe zukommen. Wir arbeiten an einem vereinfachten **Beantwortungskonzept**; zur Erleichterung des Aufwandes und zum Nachweis eines angemessenen Umgangs in dem Betrieb.

Das setzt natürlich voraus, dass die wichtigen Punkte in Angriff genommen wurden oder werden. Der Umfang kann teilweise gesteuert werden, andere Aspekte werden geklärt

werden müssen. Ein einfaches Schema, dass auf alle Varianten und betriebliche Situationen passt, wird es auch für kleinere Betriebe nicht geben.

Wir empfehlen, unter Nutzung dieser Roadmap anzufangen und die Big Points pragmatisch und doch konsequent anzugehen. Sinnvoll ist es bestimmt auch, in einem offenen Ordnersystem die einzelnen Maßnahmen zu dokumentieren - und falls es erforderlich wird, entsprechen zu ändern.

Ggf. ist es auch im Interesse der Mitgliedsbetriebe notwendig, überzogene Anforderungen oder Auslegungen des Datenschutzes zurückzuweisen. Dies setzt im Übrigen einen intensiven Dialog und Weiterverfolgung der Entwicklung in unser aller Interesse voraus.