Q&A LEITFADEN ZUR DSGVO

1. WANN WIRD DAS NEUE DATENSCHUTZREGIME ANWENDBAR?

Ab dem 25.5.2018 ist die Datenschutzgrundverordnung ("DSGVO") in allen Mitgliedstaaten der EU anwendbar. Untypisch für eine unmittelbar anwendbare Verordnung sieht sie etwa 70 Öffnungsklauseln vor, wo die nationalen Mitgliedssaaten abweichende Regelungen treffen können. In Österreich wurde zur Umsetzung dieser Regelungen das Datenschutzanpassungsgesetz 2018 ("DSG 2018") verabschiedet, das neben der DSGVO anwendbar sein wird.

2. WAS BRINGT DIE DSGVO MIT SICH?

Die neuen Bestimmungen führen zu einem kompletten Regimewechsel: Weg von den Vorab-Meldungen und Genehmigungen hin zu einer verstärkten Eigenverantwortung mit einer ex-post Kontrolle durch die Behörden und Androhung hoher Strafen bei Verstößen. Zukünftig ist es also nicht mehr erforderlich, alle Datenanwendungen der Behörde zu melden, sondern müssen die Unternehmen intern selbst die notwendigen Schritte setzen. Um sämtliche Pflichten der DSGVO einzuhalten sind umfangreiche Umsetzungsmaßnahmen erforderlich. Dieser Q&A Leitfaden bietet einen allgemeinen Überblick über die DSGVO mit Fokus auf die für Kommunikatoren wesentlichen Bestimmungen.

3. WEN BETRIFFT DIE DSGVO?

Die DSGVO betrifft alle Unternehmen, die in irgendeiner Art und Weise personenbezogene Daten verarbeiten. Die Unternehmensgröße oder Mitarbeiterzahl spielt dabei keine Rolle. Die neuen Pflichten gelten daher sowohl für Einzelunternehmer, Start-Ups als auch für KMUs und Vereine.

Unter Verarbeiten versteht man dabei jeden Umgang mit personenbezogenen Daten. Dazu zählt etwa das Erheben, Speichern, Verändern, Auslesen und Abfragen. Auch der Begriff der personenbezogenen Daten wird sehr weit ausgelegt und umfasst all jene Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (bspw Name, E-Mail Adresse, Geburtsdatum, Anschrift, IP Adresse, Interessen und Vorlieben, ...).

4. UNTER WELCHEN VORAUSSETZUNGEN DÜRFEN DATEN VERARBEITET WERDEN?

Jede Datenverarbeitung ist grundsätzlich nur dann zulässig, wenn sie sich auf eine der folgenden Rechtsgrundlagen (Rechtfertigungen) stützen lässt:

- **Einwilligung**: Der Betroffene hat seine Einwilligung zur Verarbeitung der ihn betreffenden Daten abgegeben. Dabei sind die strengen Voraussetzungen der DSGVO einzuhalten. Diese Rechtsgrundlage ist insbesondere bei der Verarbeitung von Daten zu Marketingzwecken (zB Newsletter) relevant.

- **Vertragserfüllung**: Die Datenverarbeitung ist zur Erfüllung des Vertrages mit dem Betroffenen erforderlich.

- **Gesetzliche Ermächtigung/Verpflichtung**: Die Datenverarbeitung ist gesetzlich vorgeschrieben.

- **Berechtigte Interessen**: Außerdem ist eine Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Datenverarbeiters erforderlich ist. Hier ist also immer eine Interessenabwägung im Einzelfall vorzunehmen. Die österreichische Datenschutzbehörde und die Rechtsprechung war bislang sehr streng und gingen insbesondere davon aus, dass rein wirtschaftliche Interessen eine Datenverarbeitung grundsätzlich nicht rechtfertigen können.

5. WELCHEN ANFORDERUNGEN MUSS DIE EINWILLIGUNG ENTSPRECHEN?

In der Praxis sind Einwilligungserklärungen, insbesondere bei der beabsichtigten Verwendung der Daten für Werbezwecke (zB Newsletter), unumgänglich. Eine zulässige datenschutzrechtliche Einwilligung muss nach der DSGVO folgende Kriterien erfüllen:

- **Klare und einfache Sprache**

- **Umfassende Information** des Betroffenen (also etwa des Empfängers des Newsletters) über (i) die konkret verarbeiteten Daten (zB Name, Email Adresse), (ii) den Zweck der Verarbeitung (zB detaillierte Beschreibung der zu erwartenden Werbeinhalte sowie der konkrete Art der Kontaktaufnahme – etwa per E-Mail), (iii) etwaige dritte Datenempfänger (inkl Name und Anschrift) und (iv) die jederzeitige Möglichkeit, die Einwilligung zu widerrufen.

- **Freiwilligkeit:** Insbesondere darf die Erfüllung eines Vertrages nicht von der Abgabe einer Einwilligungserklärung abhängig gemacht werden. Außerdem sind nach aktueller Auslegung Zustimmungen nur in AGB kritisch.

- **Nachweisbarkeit:** Die Einwilligungserklärung muss jederzeit nachweisbar sein.

In der Praxis sollten Einwilligungen daher am besten durch das Anklicken einer separaten Checkbox eingeholt werden.

6. MÜSSEN BESTEHENDE EINWILLIGUNGSERKLÄRUNGEN ÜBERARBEITET WERDEN?

Ja, aktuell verwendete Erklärungen müssen angepasst werden, wenn sie den strengen Voraussetzungen der DSGVO nicht entsprechen.

7. SIND BISHER ERTEILTE EINWILLIGUNGEN WEITERHIN GÜLTIG?

Diese Frage wird von der DSGVO nicht abschließend beantwortet. Nach aktueller herrschender Ansicht sind Einwilligungserklärungen aber auch nach Mai 2018 weiterhin gültig (und müssen nicht neu eingeholt werden), wenn sie schon bisher datenschutzkonform waren.

Daher müssen beispielsweise Newsletterempfänger grundsätzlich nicht noch einmal gefragt werden, ob sie weiterhin Werbung und Neuigkeiten erhalten möchten.

Wenn allerdings schon bisher gar keine Einwilligung vorliegt oder die Erklärung ganz offensichtlich nicht der aktuellen Rechtslage entspricht (zB die Datenarten nicht konkret angegeben sind oder der Zweck nicht umschrieben ist), sollen jedenfalls neue Zustimmungen eingeholt werden. Dabei ist allerdings darauf zu achten, dass etwa potentielle Newsletterempfänger nicht proaktiv angeschrieben werden dürfen, um sie nach ihrer Zustimmung zu fragen. Diese Nachfrage wäre bereits datenschutzwidrig und verstößt gegen das Spam-Verbot.

8. WIE SCHAUT ES MIT DEM ZUKAUF VON ADRESSEN FÜR POSTSENDUNGEN AUS?

Das Versenden von Marketingmaterial per Post ist datenschutzrechtlich in der Regel mit berechtigten Interessen des werbenden Unternehmens gerechtfertigt. Daher sind Postsendungen grundsätzlich datenschutzrechtlich unproblematisch und erfordern keine Einwilligung des Empfängers. Somit können auch zugekaufte Adressen (etwa von Adresshändlern) für Postwerbung verwendet werden. Es muss allerdings darauf geachtet werden, dass der Empfänger nicht in der Robinsonliste aufscheint.

Im Fall von E-Mail-Werbung ist allerdings die Einwilligung des Empfängers erforderlich. Wenn eine solche nicht vorliegt, begeht das werbende Unternehmen einen DSGVO-und TKG Verstoß (Spam-Verbot; § 107 TKG).

9. WIE IST MIT PRESSEAUSSENDUNGEN UMZUGEHEN?

Presseaussendungen an eine Vielzahl an Journalisten bewegen sich datenschutzrechtlich in einem Graubereich, hier gehen auch die Meinungen von Juristen auseinander. Da es zu diesem Zeitpunkt noch keine gesetzlich/gerichtlich bestätigte Sichtweise oder verbindliche Rechtslage gibt, erläutern wir im Folgenden mögliche Sichtweisen und Argumentationslinien im Klagsfall. Die Wahrscheinlichkeit eines Klagsfalls und die tatsächliche Höhe einer möglichen Strafzahlung sind derzeit nicht einzuschätzen, daher können wir hier keine Empfehlung für eine der beiden Sichtweisen aussprechen. Die tatsächliche Vorgehensweise wäre Managemententscheidung der jeweiligen Agentur, bestenfalls mit Unterstützung des Rechtsbeistands.

Die Verwendung von zulässigerweise veröffentlichten Daten (für die Zwecke für die die Daten veröffentlicht wurden) ist datenschutzrechtlich grundsätzlich zulässig. Die Aufnahme der Daten von Journalisten in eine eigene Datenbank ist daher auf Basis berechtigter Interessen zulässig. Selbiges gilt auch für postalische Zusendungen, solange der Journalist nicht widerspricht. Schlussendlich sind auch elektronische Zusendungen, die der Informations- und Medienfreiheit unterliegen jedenfalls zulässig. Eine Presseaussendung mit entsprechend relevanten Informationen an eine öffentlich kundgemachte berufliche E-Mail Adresse eines Journalisten ist daher idR unproblematisch. Dies trifft allerdings nicht auf etwaige Aussendungen zu Werbezwecken zu, die im weitesten Sinne den Waren- oder Dienstleistungsansatz eines Unternehmens fördern oder zu dessen Rufsteigerung beitragen sollen. Für diese ist eine vorherige Einwilligung gemäß § 107 TKG erforderlich.

Wenn die E-Mail Adresse selbst allerdings nicht öffentlich abrufbar ist (zB interner Bereich; Privatadresse; Intuitives Erraten der aus Vor- und Nachname des Journalisten bestehenden Adresse), liegt bereits damit ein Datenschutzverstoß vor, sofern keine vorherige

Einwilligung des Angeschriebenen eingeholt wird. Hier ist also auch die bloße Speicherung schon problematisch.

10. WIE SIEHT ES MIT INFORMATIONSPFLICHTEN AUS?

Die DSGVO sieht eine ganze Fülle an Informationspflichten vor. Die Details müssen jeder Person, deren Daten verarbeitet werden (zB Kunden oder auch Mitarbeiter), in klarer und einfacher Sprache zur Verfügung gestellt werden. Insbesondere muss jeder Betroffene über (i) den Zweck der Verarbeitung, (ii) die Rechtsgrundlage, (iii) etwaige Empfänger der Daten, (iv) die Speicherdauer und (v) Betroffenenrechte informiert werden. In der Praxis werden die Informationen üblicherweise über Datenschutzbestimmungen oder Datenschutzerklärungen (Privacy Policies) veröffentlicht.

11: WELCHE RECHTE HABEN PERSONEN, DEREN DATEN VERARBEITET WERDEN?

Betroffene haben nach der DSGVO insbesondere folgende Rechte:

- **Recht auf Auskunft:** Jeder Betroffene kann jederzeit und ohne Begründung Auskunft über (i) die verarbeiteten Datenkategorien, (ii) die Zwecke der Verarbeitung, (iii) etwaige Empfänger, (iv) die Speicherdauer sowie (v) die Herkunft der Daten verlangen.

- **Recht auf Berichtigung:** Unrichtige Daten sind auf Antrag des Betroffenen zu berichtigen; unvollständig Daten sind zu vervollständigen.

- **Recht auf Löschung ("Vergessenwerden"):** Auf Antrag des Betroffenen müssen seine Daten dauerhaft gelöscht werden. Dies gilt allerdings nur, sofern (i) die Daten nicht mehr erforderlich sind, (ii) der Betroffene seine Einwilligung widerrufen hat oder (iii) die Daten unrechtmäßig verarbeitet werden. Betroffene Personen haben daher kein unbegründetes oder grenzenloses Recht auf Löschung.

Neben diesen in der Praxis wichtigsten Betroffenenrechten sieht die DSGVO zusätzlich ein Recht auf Einschränkung der Verarbeitung sowie auf Datenübertragbarkeit und ein Widerspruchsrecht vor.

Einem Antrag zur Ausübung eines Betroffenenrechts ist innerhalb eines Monats ab Einlangen zu entsprechen. Alle Anfragen der Betroffenen müssen grundsätzlich unentgeltlich beantwortet werden. Nur bei unbegründeten oder exzessiven Anträgen kann ein angemessenes Entgelt verlangt oder die Beantwortung verweigert werden.

12. DÜRFEN DATEN AN DRITTE ÜBERMITTELT WERDEN?

Werden Daten auch an Dritte übermittelt, ist für die Zulässigkeit zu unterscheiden, wofür er diese benutzt:

Verarbeitet der Empfänger die Daten für eigene Zwecke als Verantwortlicher (zB Werbezwecke), muss die Übermittlung ebenso wie die Verarbeitung selbst auf einer Rechtsgrundlage nach Punkt 4 basieren. In der Praxis ist die Übermittlung der Daten daher rechtmäßig, wenn sie (i) zur Vertragserfüllung erforderlich, (ii) gesetzlich verpflichtend oder (iii) von der Einwilligung des Betroffenen gedeckt ist.

Verarbeitet der Dritte als Auftragsverarbeiter die Daten bloß im Auftrag eines anderen (zB IT Provider oder Softwarehersteller) braucht es keiner besonderen Rechtfertigung oder Rechtsgrundlage. Allerdings muss eine schriftliche Vereinbarung mit bestimmten Mindestanforderungen abgeschlossen werden. In diesem Vertrag sind etwa die konkreten Datenverarbeitungen genau zu beschreiben und die wesentlichen Pflichten der Parteien festzulegen.

13. WANN IST EIN DATENVERARBEITUNGSVERZEICHNIS ZU ERSTELLEN UND WAS MUSS ES ENTHALTEN?

Grundsätzlich hat jeder, der Daten verarbeitet, auch eigenständig ein internes Verzeichnis über diese Prozesse zu führen. Die Dokumentation ist ein dynamischer Prozess und das Verzeichnis ist dabei laufend zu aktualisieren.

Jedenfalls sind darin folgende Informationen aufzunehmen:

- Name und Kontaktdaten (und des Vertreter sowie gegebenenfalls des Datenschutzbeauftragten);
- Zwecke jeder einzelnen Datenverarbeitung;
- Kategorien betroffener Personen;
- Kategorien verarbeiteter Daten;
- Empfänger oder Kategorien von Empfängern (am besten aufgeteilt in interne Zugriffsberechtigte, externe Verantwortliche und externe Auftragsverarbeiter);
- Aufbewahrungsdauer der verschiedenen Datenkategorien;
- allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen.

Auftragsverarbeiter, die nur Daten im Auftrag eines Anderen verarbeiten, müssen dafür nur folgende Angaben machen:

- Name und Kontaktdaten (und des Vertreter sowie gegebenenfalls des Datenschutzbeauftragten);
- Name und Kontaktdaten jedes einzelnen Verantwortlichen, für den Daten verarbeitet werden;
- Kategorien der für jeden Verantwortlichen durchgeführten Verarbeitungen;
- allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen.

14. WELCHE DATENSICHERHEITSMASSNAHMEN MÜSSEN GETROFFEN WERDEN?

Bei der Datenverarbeitung sind angemessene technische und organisatorische Datensicherheitsmaßnahmen zu treffen. Die DSGVO nennt hier etwa die Pseudonymisierung und Verschlüsselung oder die Fähigkeit, Daten nach einem Zwischenfall rasch wiederherzustellen. Im Detail ist auf die best practice abzustellen. Relevant sind hier insbesondere ISO Normen (vor allem die ISO 27000-Familie) sowie das österreichische Informationssicherheitshandbuch (abrufbar unter https://www.sicherheitshandbuch.gv.at/).

15. WAS IST BEI EINEM DATENSCHUTZVERSTOSS ZU TUN?

Sollte es trotz Sicherheitsmaßnahmen zu einem Datenschutzverstoß (Datenleck, einem Hackerangriff oder einem Datendiebstahl) kommen, ist rasch zu handeln: Ist damit nämlich ein Risiko für den Betroffenen verbunden, ist der Verstoß innerhalb von 72 Stunden an die Datenschutzbehörde zu melden. Daneben ist außerdem der Betroffene unverzüglich zu verständigen, wenn das Risiko voraussichtlich hoch ist, zB wenn Gesundheitsdaten oder Kreditkarteninformationen veröffentlicht werden.

16. WAS IST EINE DATENSCHUTZ-FOLGENABSCHÄTZUNG?

Werden Datenverarbeitungen durchgeführt, die voraussichtlich besonders riskant sind, ist vorab eine Folgenabschätzung durchzuführen. Damit werden in einen ersten Schritt die potentiellen Risiken identifiziert und bewertet. Daran anschließend ist für jedes identifizierte Risiko die getroffenen Sicherheitsmaßnahmen zu beschrieben.

In der Praxis kann die Datenschutz-Folgenabschätzung auf der internen Dokumentation aufbauen und wird um die zusätzlich erforderlichen Informationen ergänzt.

17. WANN BRAUCHT EIN UNTERNEHMEN EINEN DATENSCHUTZBEAUFTRAGTEN?

Unabhängig von der Größe eines Unternehmens ist ein Datenschutzbeauftragter zu bestellen, wenn die Kerntätigkeit

- eine umfangreiche regelmäßige und systematische Überwachung der Betroffenen darstellt; oder
- in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten (sensible oder strafrechtlich relevante Daten) liegt.

Zur "*Kerntätigkeit*" gehören nach bisher herrschender Auslegung neben der Haupttätigkeit eines Unternehmens auch sämtliche Schlüsseltätigkeiten, die untrennbar mit der Erreichung des Unternehmensziels verknüpft sind. Bloße Nebentätigkeiten (wie etwa Personalverwaltung) und untergeordnete Hilfstätigkeiten zählen aber nicht dazu.

Eine umfangreiche regelmäßige und systematische Überwachung liegt insbesondere beim Einsatz von Tracking, Scoring und Profiling vor.

In der Praxis hängt es also von den konkret durchgeführten Verarbeitungstätigkeiten ab, ob ein Datenschutzbeauftragter zu bestellen ist. Sollte man zu dem Ergebnis kommen, dass kein Datenschutzbeauftragter erforderlich ist, sollten diese Überlegungen für den Anlassfall einer Prüfung durch die Datenschutzbehörde sorgfältig dokumentiert sein.

18. WELCHE AUFGABEN HAT DER DATENSCHUTZBEAUFTRAGTE UND WER KANN DAZU BESTELLT WERDEN?

Der Datenschutzbeauftragte hat eine beratende und kontrollierende Funktion. Im Einzelnen unterstützt er Unternehmen bei der Datenverarbeitung und dem Erstellen der Datenschutz-Folgenabschätzung, überwacht die Datenschutz-Compliance und ist Kontaktperson für die Zusammenarbeit mit der Datenschutzbehörde.

Die Position kann intern durch Mitarbeiter aus den eigenen Reihen oder extern besetzt werden. Vorab ist bei der Auswahl darauf zu achten, dass keine Interessenkonflikte bestehen. Aufgrund der Beratungs- und Kontrollfunktion scheiden Personen mit Entscheidungsbefugnis in Datenschutzsachen aus, da sie sich andernfalls selbst beraten und kontrollieren würden. Wenig geeignet für diese Position sind daher Geschäftsführer, da sie wesentliche Entscheidungsträger in allen Bereichen eines Unternehmens sind. Auch Leiter der IT-Abteilung oder des Personalwesens können nicht als Datenschutzbeauftragte bestellt werden.

Mitbringen sollte der Datenschutzbeauftragte juristische, technische und organisatorische Kenntnisse sowie die erforderliche soziale Kompetenz.

Besteht keine Pflicht zur Bestellung, kann es trotzdem sinnvoll sein, einen Datenschutzkoordinator als zentrale Anlaufstelle für Datenschutz einzurichten. Da dieser nicht der DSGVO unterliegt, kann er auch Entscheidungsfunktion sowie Erstellung und Betreuung des Verfahrensverzeichnisses übernehmen.

19. HAFTET DER DATENSCHUTZBEAUFTRAGTE?

Der Datenschutzbeauftragte berät das Unternehmen lediglich und ist in seiner Funktion weder entscheidungs- noch vertretungsbefugt. Nach herrschender Auffassung ist für die Einhaltung der DSGVO ist weiterhin das datenverarbeitende Unternehmen verantwortlich.

20. WELCHE SANKTIONEN UND RISIKEN DROHEN?

Die DSGVO sieht sehr hohe **Geldbußen** für Datenschutzverstöße von bis zu EUR 20 Mio oder 4 % des weltweiten Konzernumsatzes abhängig vom Grad der Verletzung vor (je nachdem welcher Betrag höher ist). Es haftet primär die Gesellschaft selbst. Daneben kann die Behörde die Geldbußen auch gegen natürliche Personen (in der Praxis Geschäftsführung, Vorstand oder ein bestellter verwaltungsstrafrechtlicher Vertreter; nicht der Datenschutzbeauftragte) aussprechen.

21. WAS IST ZU TUN?

Für die Praxis lassen sich als wesentliche To Do's folgende Umsetzungsmaßnahmen zusammenfassen:

- Rechtzeitig alle **Datenverarbeitungen** zusammentragen, um zu prüfen, ob diese zum eigenen Zweck oder im Auftrag eines Dritten durchgeführt werden und ob sie datenschutzrechtlich zulässig sind (siehe Punkt 4).

- **Verarbeitungsverzeichnis** mit den unter Punkt 0 genannten Informationen erstellen.

- Bestehende **Einwilligungen** überprüfen und aktualisieren (siehe Punkt 5).

- **Datenschutzbestimmungen** mit allen nach der DSGVO erforderlichen Informationen überarbeiten bzw erstellen (siehe Punkt 10).

- **Schriftliche Vereinbarungen** mit externen Dritten nach den Vorgaben der DSGVO abschließen (siehe Punkt 12).

- Prüfung, ob ein **Datenschutzbeauftragter** zu bestellen ist und Dokumentation der Entscheidungsfindung (siehe Punkt 0).

- Überprüfen, ob für bestimmte Verarbeitungen eine **Datenschutz-Folgenabschätzung** durchzuführen ist (siehe Punkt 0).

- Implementierung eines Standardprozess, wie **Betroffenenrechte** (fristgerecht) gewahrt werden können und Vorbereitung entsprechender Vorlagen für die Erledigung (siehe Punkt 11).

- Überprüfen, ob und welche **Datensicherheitsmaßnahmen** bereits implementiert wurden und gegebenenfalls nachjustieren (siehe Punkt 14).

Q&A FÜR PR-AGENTUREN/PR-BERATER

Was muss eine **Datenschutzerklärung für die Website** konkret beinhalten?

Die Datenschutzerklärung oder Privacy Policy muss nach Art 13 DSGVO insbesondere folgende Inhalte abdecken:

(i) Name und Kontaktdaten des verantwortlichen Websitebetreibers (z.B. aus dem Impressum),
(ii) Kontaktdaten des Datenschutzbeauftragten (sofern einer bestellt wurde),
(iii) Zweck und Rechtsgrundlage der Verarbeitung (warum werden welche Daten verarbeitet),
(iv) Empfänger von Daten (wer erhält zu welchem Zweck personenbezogene Daten),
(v) Informationen zu internationalen Datentransfers (an Empfänger außerhalb des EWR),
(vi) Speicherdauer bzw. Löschfristen,
(vii) Aufklärung über die Betroffenenrechte (z.B. Auskunft, Berichtigung, Löschung, Widerrufsrecht etc.),
(viii) Aufklärung über das Beschwerderecht bei der Datenschutzbehörde,
(ix) Aufklärung, ob die Datenbereitstellung verpflichtend ist und
(x) Informationen zu etwaigen automatisierten Einzelentscheidungen und Profiling.

Für die konkrete Ausgestaltung einer richtigen Datenschutzerklärung, insbesondere wenn diese zusätzlich mit einer Einwilligungserklärung verknüpft werden soll, kommt es daher auf die konkreten Websiteinhalte an (z.B. Kontakformular, Newsletteranmeldung, Cookies, Tracking, Webshop etc.). In Anbetracht des Umfangs der Informationspflichten ist eine individuelle Rechtsberatung daher sinnvoll.

Wenn kein Datenschutzbeauftragter bestellt wird, wie soll die geforderte **Erklärung** gestaltet sein?

Für den Fall einer Prüfung durch die Aufsichtsbehörde ist es sinnvoll, intern zu dokumentieren, auf Basis welcher Argumentation kein Datenschutzbeauftragter bestellt wurde. Da es dafür keine konkrete, gesetzliche Verpflichtung gibt genügt grundsätzlich ein kurzer Text, der darlegt, wie die Entscheidung zustande kam.

Wie soll die **Datenschutzfolgeabschätzung** aussehen?

Für die Form der Datenschutzfolgeabschätzung gibt es keinerlei gesetzliche Vorgaben oder behördliche Muster. In der Praxis ist eine Orientierung an ISO/IEC 29134:2017 sinnvoll (https://www.iso.org/standard/62289.html). Da die Datenschutzfolgeabschätzung gewissermaßen den Kern der Datenschutzgrundverordnung bildet und neben einer

rechtlichen Beurteilung auch technische und organisatorische Maßnahmen sowie eine konkrete Risikoanalyse erforderlich sind, ist die Hinzuziehung externer Experten zu empfehlen.

Wie geht man damit um, wenn man als Agentur für Kunden zum Beispiel E-Mail Newsletter an Adressen verschickt, die der Kunde bereitstellt?

Hier ist es besonders wichtig, dass die Agentur sich als datenschutzrechtlicher Auftragsverarbeiter deklariert. Das bedeutet, dass

(i) der Kunde für die Einholung einer gültigen Zustimmung verantwortlich bleibt und

(ii) die Agentur die Aussendung auch nur im Namen des Kunden und für dessen Zwecke vornehmen darf.

Zusätzlich ist eine "Auftragsverarbeitervereinbarung" mit dem Kunden abzuschließen.

Dürfen bestehende "alte" Datensätze, die seit Jahren laufend mit Presseinfos oder Newslettern beschickt werden, ohne dass je eine Einwilligung eingeholt wurde, weiterverarbeitet werden?

Nein. Die Zusendung jeglicher Art von Direktwerbung – dies schließt auch Presseaussendungen mit ein – über E-Mail, SMS oder andere elektronische Medien sowie per Telefon erfordert (seit 2007) eine vorherige, freiwillige Einwilligung. Ab dem 25.5.2018 wird zusätzlich der Strafrahmen für etwaige Verstöße drastisch erhöht.

Dürfen Agenturen **Verteiler an Kunden oder Partner weitergeben oder verkaufen**?

Nein, da die Agentur als Auftragsverarbeiter die erhaltenen Daten in den meisten Fällen nur für den jeweiligen Kunden nutzen darf. Nur dann, wenn die Agentur über eine Gewerbeberechtigung für Adressvermittlung gemäß § 151 GewO verfügt.

Darf man veröffentlichte E-Mail- und Postadressen (nicht nur Journalisten, sondern auch Blogger, Influencer, Personen der Öffentlichkeit wie Bürgermeister), per E-Mail oder Post beschicken/kontaktieren, ohne eine Einwilligung einzuholen?

Per Post ja, sofern der Empfänger nicht in der Robinsonliste der WKO eingetragen ist. Die Kontaktaufnahme per E-Mail oder Telefon erfordert jedenfalls vorab eine Einwilligung.

Wie soll die **Zustimmung/Einwilligung** eingeholt werden?

Sofern bisher keine Einwilligung vorliegt, ist lediglich eine Kontaktaufnahme per Post möglich. Daneben besteht freilich die Möglichkeit, auf der eigenen Homepage Newsletter-Anmeldungen und ähnliche Opt-in Masken zu implementieren, bei denen sich Interessenten aktiv zu bestimmten Datenverarbeitungen anmelden können.

Darf man bei Kommunikation zwischen PR-Agenturen und Journalisten von **„anzunehmenden beruflichen/geschäftlichen Interessen"** ausgehen?

Nein. Es gibt bereits Fälle in Deutschland und auch in Österreich, bei denen Journalisten trotz veröffentlichten Kontaktdaten gegen Zusendungen aufgrund der Spam-Bestimmungen mit Erfolg vorgegangen sind.

Muss eine **Datenweitergabe an Nicht-EU-Kunden** extra genehmigt/geregelt werden?

Ja, dafür ist der Abschluss von EU Standardvertragsklauseln erforderlich (http://archiv.dsb.gv.at/site/6208/default.aspx)