DATENSCHUTZAKTUELL
MAI 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH
Schweiz

SIND IHRE ÄLTEREN EINSCHÄTZUNGEN NOCH AKTUELL?

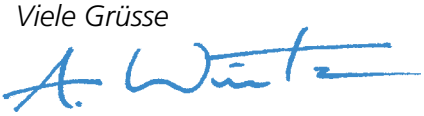
Denken Sie immer zwei Schritte weiter

Liebe Leserin, lieber Leser,

Sie kennen den Spruch „Wer A sagt, muss auch B sagen". Da ist viel Wahres dran, auch wenn Sie sich Ihre Rolle und Ihre Arbeit als Datenschutzberater vor Augen führen. Alles, was Sie beraten, bewerten oder entscheiden, hat Folgen, und zwar für Ihr Unternehmen, dessen Geschäftstätigkeit und die Beschäftigten.

Also ist es unerlässlich, dass Sie möglichst frühzeitig bedenken, welche Folgen Ihr Aktivwerden oder Ihre Entscheidungen haben können. Das bringt nicht nur allen Beteiligten etwas. Sie bewahren sich selbst davor, weniger professionell zu wirken, etwa wenn Sie Entscheidungen über denken oder revidieren zu müssen.

Viele Grüsse



Andreas Würtz,
Rechtsanwalt und Chefredaktor

Ihr Experte für Datenschutz
Andreas Würtz verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz pragmatisch umsetzen lässt.

Inhalt

Zu Ihrem Onlinebereich:
https://kurzlink.ch/privacy

Expertenhotline:
https://kurzlink.ch/kontakt-wuertz

Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Bonn

V.i.S.d.P.: Michael Jodda (Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | MØREfoto;
Seite 1: Adobe Stock | Thapana Studio

Erscheinungsweise: 17-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Nutzen Sie unsere Checkliste für Ihren Datenschutz-Check.

Gut aufgestellt im Datenschutz? Machen Sie den Check

Datenschutz ist kein Selbstzweck. Vielmehr schützt Ihr Unternehmen damit nicht nur Daten um des Schutzes willen. Es geht Ihrem Unternehmen in erster Linie darum, Gefahren und Risiken zu minimieren, um etwa Datenschutzverstösse zu vermeiden und keinen Ärger zu riskieren. Damit das so ist und bleibt, muss Ihr Unternehmen gut im Datenschutz aufgestellt sein. Machen Sie den Check!

Stellen Sie den Datenschutz auf den Prüfstand

Um zu beurteilen, wie es um die systematische Umsetzung des Datenschutzes im Unternehmen steht und inwieweit wichtige Aspekte des Bundesgesetzes über den Datenschutz (DSG) umgesetzt sind, können Sie auf folgende Checkliste setzen. Stellen Sie fest, dass etwas nicht in Ordnung ist, sollten Sie die Initiative ergreifen und mit den zuständigen Kollegen oder der Unternehmensleitung sprechen. Schliesslich besteht ernsthafter Handlungsbedarf.

CHECKLISTE: Bewertung des Datenschutzes im Unternehmen

Thema	Das ist besonders relevant	Erledigt?
Besteht eine solide Datenschutzorganisation?	› Hinterfragen Sie, wie der Datenschutz in Ihrem Unternehmen organisiert ist. Klären Sie insbesondere, inwieweit die vorhandene Organisation zu Struktur, Geschäftstätigkeit, Umfang der Bearbeitung von Personendaten sowie Zahl und Qualifikation der Beschäftigten passt. › Seien Sie auch selbstkritisch im Hinblick auf Ihre Rolle und Ausstattung als Datenschutzberater. Sind Sie eher „Feigenblatt" und können Sie Ihre Aufgaben nicht richtig wahrnehmen, ist das ein Problem, das das Unternehmen angehen muss.	○ Ja ○ Nein
Inwieweit ist ein Datenschutzmanagementsystem (DSMS) umgesetzt?	› Mit einem solchen System werden Strukturen und Prozesse etabliert, um den Datenschutzanfor derungen gerecht zu werden.Tabelle-Muster-Auflistung › Typisch sind das systematische Vorgehen und das Ziel, kontinuierlich die Datenschutzsituation zu verbessern. Dazu wird meist auf den PDCA-Kreislauf gesetzt, der für die Phasen Plan, Do, Check, Act steht, also Planen, Umsetzen, Überprüfen und Verbessern. › Im Fokus sind in erster Linie Regelungen zum Datenschutz, eine Organisation, relevante Prozesse sowie deren Umsetzung und fortlaufende Optimierung. › Ein solches Managementsystem ist an sich als „strukturiertes und systematisches Vorgehen" zu verstehen. Gerade bei grösseren Unternehmen kann der Einsatz einer entsprechenden Software zur Umsetzung des DSMS vieles erleichtern.	○ Ja ○ Nein

Wie werden Risiken mit Datenschutzbezug gemanagt?	› Risikomanagement ist in jedem Unternehmen eine unerlässliche Aufgabe, auch im Datenschutz. › Prüfen Sie, inwieweit Gefahren identifiziert, Risiken bewertet und passende Gegenmassnahmen festgelegt werden. Dabei sollten Risikoanalysen systematisch ablaufen und klaren Regeln folgen. › Denken Sie nicht nur an Risiken mit Bezug zum Datenschutz bei der Bearbeitung von Personendaten. Blicken Sie auch über den Tellerrand. So sind Mitarbeiter, die nicht über das nötige Know-how verfügen, genauso eine relevante Gefahr wie eine Tür zum Serverraum, die immer sperrangelweit offen steht.	○ Ja ○ Nein
Ist ein vollständiges und aktuelles Verzeichnis von Bearbeitungstätigkeiten vorhanden?	› Das betreffende Verzeichnis nach Art. 12 DSG ist nötig, um beispielsweise gegen über der Datenschutzaufsichtsbehörde auskunftsfähig zu sein. Doch es ist auch wichtig für die Arbeit des Datenschutzberaters. Es hilft dabei, den Überblick zu behalten und leichter die Bearbeitungen auszumachen, die einer besonderen Aufmerksamkeit bedürfen. › Achten Sie auf die Vollständigkeit und Aktualität der Angaben. Manchmal wird das Verzeichnis nur halbherzig geführt. Drängen Sie hier darauf, dass sich das schleunigst ändert. › Prüfen Sie auch, inwieweit Bearbeitungstätigkeiten ohne Technik (z. B. Bearbeitungen auf Messen, Listen) enthalten sind. Die werden gerne vergessen.	○ Ja ○ Nein
Sind für die Bearbeitungen von Personendaten Risikoanalysen durchgeführt, Massnahmen abgeleitet und umgesetzt?	› Grundsätzlich ist für jede Bearbeitung von Personendaten Daten eine Risikoanalyse erforderlich. Schliesslich lassen sich nur so risikoangemessene technische bzw. organisatorische Massnahmen auswählen. › Achten Sie darauf, dass Risikoanalysen nachvollziehbar und dokumentiert sind. Dann sind Sie auf der sicheren Seite. › „Einmal Durchführen und dann vergessen" ist nicht drin. Die Risiken müssen fortlaufend beobachtet und die Bewertung sowie Massnahmen müssen ggf. angepasst werden.	○ Ja ○ Nein
Ist die Einhaltung der Grundsätze der Bearbeitung von Personendaten Standard?	› Jede Bearbeitung von Personendaten muss die Grundsätze aus Art. 6 DSG einhalten. › Schauen Sie, inwieweit die Prüfung der Grundsätze bzw. der daraus abgeleiteten Anforderungen aus dem DSG in Regelungen und Prozessen verpflichtend ist.	○ Ja ○ Nein
Inwieweit wird „Data protection by design and default" umgesetzt?	› Damit Datenschutz von Anfang an mitgedacht und schon bei der Gestaltung berücksichtigt wird, müssen die Vorgaben aus Art. 7 DSG beachtet werden. › Schauen Sie sich an, inwieweit Leitfäden oder Vorgaben für Projekte und IT-Vorhaben entsprechende Vorgaben machen. › Meist ist es unerlässlich, dass Sie als Datenschutzberater schon in der Ideenphase eingebunden werden. Nur so werden Anforderungen frühzeitig bedacht.	○ Ja ○ Nein
Sind die nötigen Datenschutz-Folgenabschätzungen durchgeführt?	› Prüfen Sie, welche Regelungen es zu diesem Aspekt gibt und wie das Vorgehen aussieht. › Entscheidend ist nicht nur, dass Folgenabschätzungen durchgeführt werden. Mindestens genauso wichtig ist, dass man Sie zur Beratung hinzuzieht. Das sollte am besten als klare Anweisung geregelt sein. › Halten Sie im Verzeichnis von Bearbeitungstätigkeiten Ausschau nach relevanten Bearbeitungen und prüfen Sie, ob die Folgenabschätzungen dokumentiert und mit dem nötigen Inhalt (Art. 22 Abs. 3 DSG) durchgeführt wurden.	○ Ja ○ Nein
Sind Prozesse zur richtigen Reaktion auf Zwischen-, Not- und Katastrophenfälle eingerichtet?	› Um für den Fall der Fälle vorbereitet zu sein, braucht es entsprechende Pläne und Prozesse sowie die erforderlichen qualifizierten Mitarbeiter. › Haben Sie insbesondere ein Auge auf Regelungen und Prozesse mit Bezug zum Datenschutz, beispielsweise zum Vorgehen bei Datenpannen oder bei einem Hackerangriff.	○ Ja ○ Nein
Wie werden Betroffenenrechte gemanagt?	› Hier sind klare Vorgaben zum Vorgehen unerlässlich. So sollte es Prozesse zur Bearbeitung an sich sowie speziell z. B. zum Vorgehen bei Auskunft oder Löschung geben. › Schauen Sie, wie es um das Wissen bei besonders relevanten Stellen steht. Das sind vor allem Kollegen, bei denen Betroffenenanfragen eingehen, etwa der Kundenservice oder die Poststelle. › Auch diejenigen, die Betroffenenrechte umsetzen, müssen über alles Relevante Bescheid wissen.	○ Ja ○ Nein
Werden Beschäftigte im angemessenen Umfang geschult, qualifiziert und sensibilisiert?	› Generell gilt: Wer Bescheid weiss, macht weniger falsch und erkennt Gefahren, bevor sie zum Problem werden. Also sollte jeder Mitarbeiter über das für seine Aufgabe nötige Datenschutz-Know how verfügen. › Schauen Sie, inwieweit es ein Schulungs- und Sensibilisierungskonzept gibt. Auch hier sollte sich die Risikoorientierung widerspiegeln. Ausserdem ist das Dokumentieren wichtig. › Klären Sie, inwieweit sichergestellt ist, dass es keine „Durchrutscher" bei den zu sensibilisierenden Mitarbeitern gibt. Auch im Datenschutz gilt: Eine Kette ist nur so stark wie ihr schwächstes Glied.	○ Ja ○ Nein
Sind Dienstleister sorgfältig ausgewählt und passen die vereinbarten Schutzmassahmen?	› Meist gibt es Festlegungen zur Auswahl von Dienstleistern. Klären Sie, inwieweit hier auch der Datenschutz eine Rolle spielt. Ist das nicht der Fall, muss das Thema Datenschutz integriert oder ein spezifischer Prozess aufgesetzt werden. › Achten Sie darauf, dass etwa im Verzeichnis von Bearbeitungstätigkeiten auch die beauftragten Dienstleister aufgeführt sind. Idealerweise sind die vereinbarten spezifischen Schutzmassahmen vermerkt oder verlinkt.	○ Ja ○ Nein
Bestehen Aufbewahrungs- und Löschkonzepte?	› Kennzeichnend für den Datenschutz ist, dass Personendaten nicht für immer und ewig bearbeitet werden dürfen. › Damit der Löschpflicht aus Art. 32 Abs. 2 Buchst. c DSG nachgekommen wird, müssen Fristen festgelegt und eine Löschung auch tatsächlich umgesetzt werden.	○ Ja ○ Nein

5 Praxistipps für die Altgeräteverwertung

Früher oder später ist es in jedem Unternehmen so weit: Bisherige Arbeitsmittel wie Computer, Notebooks oder Smartphones werden ausrangiert und durch modernere Geräte ersetzt. Grund dafür können neben dem technischen Fortschritt auch steuerrechtliche Abschreibungsmöglichkeiten sein. Doch bei der Sache darf nicht gelten: aus den Augen, aus dem Sinn. Denn der Datenschutz ist hier wichtig.

Verwertung bzw. Entsorgung darf nicht schieflaufen

Manchmal sind es eher die kleineren oder weniger präsenten Datenschutzthemen, die grosse Probleme verursachen können. So ist es, wenn Computer & Co. ausgetauscht werden. Dann liegt der Fokus auf den neuen Geräten. Um die ausrangierten Geräte macht man sich vielleicht weniger Gedanken. Das sollten Sie ändern. Beraten Sie frühzeitig, wenn ein grösserer Austausch ansteht oder auch vorbeugend. Beherzigen Sie dabei diese Tipps:

Tipp Nr. 1: Bringen Sie Licht ins Dunkel

Gerade wenn viele Geräte mit Datenspeichern ausrangiert werden sollen, mit denen auch Personendaten bearbeitet wurden, sollten Sie mit den verantwortlichen Kollegen oder mit der Unternehmensleitung klären, welche Geräte ausrangiert werden. Idealerweise gibt es hierzu Listen mit weiteren Informationen, etwa zu Gerätetyp, bisherigem Einsatzart, Art und Umfang der Daten(träger)verschlüsselung.

Hatte man bislang nicht über das Löschen nachgedacht, sollten Sie klarmachen, dass das unerlässlich ist. Auch beim Löschen handelt es sich um eine Massnahme, um die Sicherheit der Bearbeitung von Personendaten im Sinne von Art. 8 Bundesgesetz über den Datenschutz (DSG) zu gewährleisten.

Gehen Sie lieber vom Personenbezug aus

Vielleicht hören Sie, dass mit dem Gerät keine Personendaten bearbeitet wurden. Das können Sie meist in Zweifel ziehen. So gibt es bestimmt Benutzerkonten auf dem Gerät. Zudem zeigt die Erfahrung, dass Geräte meist nicht nur für den Zweck genutzt werden, für den sie gedacht sind. Auch wenn Datenträger verschlüsselt sind, entfällt nicht automatisch der Personenbezug.

Tipp Nr. 2: Sorgen Sie für Sensibilität

Unter Umständen stossen Sie nicht unbedingt auf Verständnis, dass Geräte vor der Verwertung oder vor der Entsorgung „sauber" sein müssen. Führen Sie in diesen Fällen den betreffenden Kollegen vor Augen:

- **Daten dürfen nicht in falsche Hände geraten:** Gibt es Personendaten auf Geräten, müssen diese angemessen geschützt werden, etwa vor dem Zugriff und der Kenntnisnahme Unbefugter. Die Anforderungen des Art. 8 DSG zur Sicherheit der Bearbeitung gelten über den gesamten Lebenszyklus von Daten bzw. der diese bearbeitenden Technik, eben von Anfang bis Ende.
- **Auch Geschäftsgeheimnisse sind schützenswert:** Jedes Unternehmen hat etwas zu verbergen. Und selbst anscheinend Belangloses kann für Dritte oder die Konkurrenz von grossem Wert sein. Schon allein zu wissen, wie Ihr Unternehmen arbeitet, kann für Wettbewerber von grossem Wert sein.
- **Datenpannen sorgen für grossen Ärger:** Erlangen Unbefugte Kenntnis von zu schützenden personenbezogenen Daten, liegt regelmässig eine Datenpanne vor, die oft auch der Aufsichtsbehörde zu melden ist. Zudem können Schadensersatzforderungen von Betroffenen drohen. Auch das Image des Unternehmens kann tiefe Kratzer bekommen, weil amateurhaftes Vorgehen schnell viel Vertrauen zerstört.

Tipp Nr. 3: Auf den Schutzbedarf kommt es an

Wie viel Aufwand auch in Sachen Löschen von Datenträgern getrieben werden muss, hängt vor allem davon ab, wie schutzwürdig die damit bearbeiteten Daten sind. Sind die Daten nicht besonders schutzwürdig und war der Datenträger verschlüsselt, kann es ausreichen, den Datenträger einfach nur zu löschen. Ein Überschreiben der Daten ist nicht zwingend nötig. Anders sieht die Sache bei schutzwürdigeren Daten aus. Hier kann es sinnvoll sein, selbst verschlüsselte Daten ggf. sogar mehrfach zu überschreiben. Auch was die Anforderungen an eine Software oder einen Dienstleister angeht, sollten diese mit der Schutzwürdigkeit der Daten steigen.

Tipp Nr. 4: Vorsicht bei Gerätespenden

Auch diese Idee ist weit verbreitet: Mit der ausrangierten Technik kann man noch Gutes tun. Aber: Ausrangierte Geräte sollten allenfalls blitzblank an soziale Einrichtungen, Schulen, Vereine oder Kindergärten gespendet werden. Ein vollständiges Löschen kann auch unter folgendem Aspekt wichtig sein: Lizenzen. Denn die will Ihr Unternehmen ggf. gerade nicht spenden oder die Lizenzen auf neu beschafften Geräten weiterhin nutzen.

Tipp Nr. 5: Achten Sie auf die Dokumentation

Je wichtiger es ist, dass richtig gelöscht wurde, desto wichtiger ist, dass Ihr Unternehmen die Löschung auch belegen kann. Professionelle Löschsoftware erstellt beispielsweise auch Löschprotokolle, aus denen alles Wesentliche hervorgeht. Auch beim Einsatz von Dienstleistern sollten Löschnachweise Standard sein.

Sind Ihre älteren Einschätzungen noch aktuell?

Die Zeit bleibt nicht stehen. Was vielleicht vor einigen Jahren noch „State of the Art" war, ist heute ein alter Hut. Das gilt auch für das Bearbeiten von Personendaten und die damit im Zusammenhang stehende Technik. Ist auch Ihre Bewertung einer Bearbeitung schon in die Jahre gekommen, sollten Sie diese einmal auf den Prüfstand stellen.

Reviews sind wichtig

Es leuchtet schnell ein, dass ein Review, sprich eine Nachüberprüfung oder Nachbewertung, sinnvoll ist. Das vor allem, wenn Bearbeitungen von Personendaten schon lange im Einsatz sind.

Dazu ein Beispiel: Sie haben vor Jahren eine Videoüberwachung datenschutzrechtlich unter die Lupe genommen und eventuell sogar eine Datenschutz-Folgenabschätzung nach Art. 22 Bundesgesetz über den Datenschutz (DSG) beratend begleitet.

Bei genauerem Hinsehen merken Sie schnell: die Zeit ist nicht stehen geblieben. Eventuell hat sich die Bearbeitung an sich verändert, weil Bereiche hinzugekommen oder weggefallen sind bzw. weil die Videoüberwachung technisch verändert wurde. Unter Umständen haben sich auch Gefahren und Risiken verändert, sodass Ihre Einschätzung anders ausfallen könnte. Dass das auch passieren kann, weil sich juristische Sichtweisen oder einschlägige Rechtsprechung ändern, liegt auf der Hand. Natürlich ist es auch Teil Ihrer Aufgaben, dass Sie (veränderte) Risiken erkennen und entsprechend darauf hinweisen bzw. beraten.

Oftmals ändert sich mehr, als man denkt

Auf den ersten Blick wirken Bearbeitungen von Personendaten relativ statisch, sprich sie ändern sich kaum. Doch wenn Sie genauer hinschauen, können Sie gerade bei schon länger aktiven Bearbeitungen erhebliche Veränderungen erkennen. So z. B. im Zusammenhang mit Folgendem:

- **Zeitlicher Aspekt**
  Eine Bewertung haben Sie zu einem bestimmten Zeitpunkt vorgenommen. Inzwischen kann sich vieles verändert haben. Unter Umständen haben Sie manche durchgeführte Änderung überhaupt nicht mitbekommen. Die wurde einfach umgesetzt. Ihre Expertise als Datenschutzberater wurde nicht eingeholt.
- **Änderungen beim Sachverhalt**
  Nicht selten sehen Bearbeitungen mit der Zeit ganz anders aus. So können Anpassungen bei Betroffenengruppen oder bearbeiteten Daten vorgenommen werden. Auch interne Regelungen, Prozesse oder Verantwortlichkeiten können sich wesentlich ändern. Denken Sie vor diesem Hintergrund auch an Kollektivvereinbarungen, die eventuell spezielle Vorgaben machen, die auch auf den Datenschutz Auswirkungen haben können.
- **Veränderte rechtliche Rahmenbedingungen**
  Auch beim Recht bleibt die Zeit nicht stehen. Da wären nicht nur neue oder veränderte gesetzliche Rahmenbedingungen. Gerade Gerichte, die das Gesetz mit Leben füllen, können dafür sorgen, dass manches heute anders zu sehen ist als zum Zeitpunkt Ihrer Bewertung.
- **Technischer Fortschritt**
  Denken Sie nur daran, dass heutzutage auch Software fast immer irgendetwas mit künstlicher Intelligenz zu tun hat. Zudem können neue Funktionalitäten auch neue Bearbeitungsmöglichkeiten eröffnen Das kann eine alte Bearbeitung erheblich verändern. Doch auch die Schutzmassnahmen müssen mit der Zeit gehen.

Gehen Sie pragmatisch an die Sache ran

Eines ist klar: Sie können nicht alles auf den Prüfstand stellen. Dazu fehlen Ihnen die (zeitlichen) Kapazitäten. Also ist Risikoorientierung gefragt. Dazu können Sie sich an folgender Faustformel orientieren: Je kritischer eine Bearbeitung ist und je länger Ihre Bewertung zurückliegt, desto eher sollten Sie die Bearbeitung und Ihre Bewertung unter die Lupe nehmen. Für eine Prüfung können Sie auf folgende Checkliste setzen.

Prüfen Sie generell in 5 Schritten

Damit Ihre Prüfung Hand und Fuss hat, konzentrieren Sie sich auf die folgenden Punkte:

- **Wählen Sie die richtigen Bearbeitungen aus**
  Hier können Sie auch stichprobenhaft bzw. nach dem Zufallsprinzip vorgehen. Besser ist jedoch meist: die ältesten und kritischsten Bearbeitungen zuerst zu prüfen.
- **Beschaffen Sie sich Informationen**
  Sowohl Informationen als Basis Ihrer ursprünglichen Bewertung als auch aktuelle Informationen sind unerlässlich. Denn nur so können Sie beurteilen, ob eine veränderte Situation vorliegt.
- **Machen Sie Ihren Check**
  Prüfen Sie umfassend, ob bezüglich Ihrer Bewertung der betreffenden Bearbeitung Anpassungsbedarf besteht, etwa weil sich Rahmenbedingungen verändert haben.
- **Dokumentieren Sie Ihre Prüfung**
  Halten Sie fest, was Sie geprüft und was Sie festgestellt haben. Dokumentieren Sie Ihren Review auch bei der betreffenden Bearbeitung, etwa im Verzeichnis von Bearbeitungstätigkeiten.
- **Bewerten Sie die Dinge neu**
  Gibt es erhebliche Abweichungen zur damaligen Situation, sollten Sie die Dinge neu bewerten. Muss dann etwas an der Bearbeitung geändert werden, adressieren Sie das bei den verantwortlichen Kollegen.

Checkliste: Review früherer Bewertungen des Datenschutzberaters

Aspekt	Hintergrund	Geprüft und in Ordnung?
Sind die Einträge im Verzeichnis von Bearbeitungstätigkeiten vorhanden, vollständig und offensichtlich aktuell?	› Werfen Sie einen Blick ins Verzeichnis und prüfen Sie, ob die Angaben nach Art. 12 Abs. 2 DSG zu den Bearbeitungstätigkeiten stimmig sind. › Finden Sie Lücken vor oder erkennen Sie, dass etwas veraltet ist, sollten Sie die Verantwortlichen bitten, für ein entsprechendes Update zu sorgen.	○ Ja ○ Nein
Von wem und von wann stammt die Bewertung?	› Eventuell stammt die Bewertung von Ihnen. Unter Umständen haben Sie jedoch auf der Vorarbeit einer anderen Person oder Ihres Vorgängers aufgebaut. › Haben Sie sich auf die Einschätzung anderer verlassen, etwa weil Sie noch nicht genügend Know-how hatten, sollten Sie die übernommene Einschätzung kritisch hinterfragen. Ggf. sehen Sie die Dinge mit dem heutigen Know-how anders.	○ Ja ○ Nein
Auf welchen Unterlagen und Informationen basiert die Einschätzung?	› Prüfen Sie, inwieweit die damaligen Bewertungsgrundlagen noch vorhanden sind. Fehlen Informationen oder Unterlagen, sollte Sie das vorsichtig werden lassen. › Schauen Sie, inwieweit Sie eine vollständige Dokumentation Ihrer Entscheidungsfindung haben. Diese kann nötig sein, um die damaligen Erwägungen heute noch nachvollziehen zu können.	○ Ja ○ Nein
Welche beurteilungsrelevanten Rahmenbedingungen galten damals?	› Führen Sie sich die Rahmenbedingungen vor Augen. Gerade bei älteren Bearbeitungen können noch andere Massstäbe angelegt worden sein. › Haben Sie nicht nur ein Auge auf rechtliche Rahmenbedingungen. Auch betriebliche Regeln oder Organisatorisches können in Ihre Einschätzung eingeflossen sein. Eventuell sieht die Welt heute anders aus.	○ Ja ○ Nein
Gibt es Veränderungen beim der Bewertung zugrunde liegenden Sachverhalt?	› Verschaffen Sie sich Klarheit darüber, inwieweit der damalige Sachverhalt auch heute unverändert zutrifft. › Prüfen Sie insbesondere, inwieweit Zielgruppen, Bearbeitungsmodalitäten und Bearbeitungsumfang noch passen. Ist hier manches anders, kann das auch eine Neubewertung der Sache erforderlich machen.	○ Ja ○ Nein
Passen die rechtlichen Rahmenbedingungen noch?	› Im Datenschutz tut sich immer viel. Schauen Sie, inwieweit Sie Ihre Bewertung auf die aktuell gültigen gesetzlichen Regelungen gestützt haben. › Bedenken Sie auch interne Regelungen, etwa betriebliche Reglements. Im Gegensatz zur Sichtweise früher müssen diese zwingend den Mindeststandard des DSG einhalten.	○ Ja ○ Nein
Gibt es Änderungen bei der technischen Umsetzung der Bearbeitung?	› Gerade bei schon lange aktiven Bearbeitungen kann es zwischenzeitlich zu erheblichen Anpassungen gekommen sein. › Sprechen Sie im Zweifel mit den Betreibern bzw. mit der IT-Abteilung und lassen Sie sich die Veränderungen und deren mögliche Auswirkungen auf die Bearbeitung erklären.	○ Ja ○ Nein
Inwieweit gibt es Veränderungen bei den an der Bearbeitung Beteiligten?	› Hier geht es nicht nur um die intern Beteiligten. Denken Sie auch an Dienstleister und Kooperationspartner, die bei der Bearbeitung unterstützen. Eventuell wurden auch Softwareanbieter ausgetauscht oder Bearbeitungen in die Cloud verlagert. Das kann eine Neueinordnung im Datenschutz nötig machen. › Gerade in Unternehmensgruppen und Konzernen gibt es oft Änderungen und Verlagerungen von Zuständigkeiten bzw. Aufgaben. Auch hier muss z. B. in Sachen Auftragsbearbeitung alles passen.	○ Ja ○ Nein
Hat sich die Gefahren- und Risikosituation verändert?	› Über die Zeit können sich Gefahren und die sich daraus ergebenden Risiken erheblich verändern. › Fordern Sie ggf. ein Update der entsprechenden Einschätzungen ein, damit Sie darauf Ihre Bewertung stützen können.	○ Ja ○ Nein
Liegen Veränderungen bei den technischen und organisatorischen Schutzmassnahmen vor?	› Gerade wenn Gefahren und Risiken sich verändern, kann das zu nicht mehr angemessenen Massnahmen führen. Hier kann eine Anpassung unerlässlich sein. › Haben Sie vor allem ein Auge auf den Aspekt „Stand der Technik". Der war vor längerer Zeit meist ein ganz anderer. Auch das kann Grund für eine neue Bewertung und für Nachbesserungen sein.	○ Ja ○ Nein
Sind die Grundsätze der Bearbeitung weiterhin gewahrt?	› Machen Sie auch hier den Check. Die Grundsätze gelten für alle Bearbeitungen von Personendaten. Prüfen Sie, inwieweit gerade Rechtmässgkeit, Zweckbindung und Verhältnismässigkeit eingehalten sind. › Haben Sie auch ein Auge auf die Rechenschaftspflicht. Die Einhaltung der Grundsätze muss Ihr Unternehmen auch belegen und nachweisen können.	○ Ja ○ Nein
Sind Anpassungen bei den Rechtsgrundlagen nötig?	› Schauen Sie, ob Rechtsgrundlagen noch passen. Hier kann es zwischenzeitlich erhebliche Veränderungen gegeben haben, etwa durch eine veränderte Rechtslage oder Rechtsprechung. › Gerade bei Einwilligungen sollten Sie genauer hinschauen. Gab es generelle Veränderungen bei der Bearbeitung oder zum Umfang der Bearbeitung, kann Anpassungsbedarf bestehen.	○ Ja ○ Nein
Ist die Umsetzung der Betroffenenrechte weiterhin gewährleistet?	› Machen Sie den Check zunächst hinsichtlich des Rechts auf Transparenz. Verändern sich Bearbeitungen, müssen ggf. auch die Transparenzinformationen, etwa nach Art. 19 DSG, angepasst werden. › Schauen Sie sich auch interne Regelungen, Zuständigkeiten oder Prozesse an. Eventuell passt hier manches nicht mehr. Den nötigen Veränderungs- und Anpassungsbedarf sollten Sie bei Ihrer Bewertung berücksichtigen.	○ Ja ○ Nein

Geben Sie der internen Kommunikation einen Überblick

Gerade in grösseren Unternehmen gibt es ganze Abteilungen, die sich um die interne Unternehmenskommunikation kümmern. Doch offen und transparent kommunizieren zu wollen bedeutet nicht, dass einfach alles erlaubt ist. Auch bei Mitarbeiterzeitung, Newsletter oder Intranet muss unter Datenschutzaspekten so manches bedacht werden.

Vermitteln Sie einige wichtige Punkte

Für die Kollegen in der internen Kommunikation steht vor allem im Vordergrund, gute und lesenswerte Artikel, Berichte oder Informationen bereitzustellen.

Dass es auch in Sachen Datenschutz und Persönlichkeitsrecht so einiges zu beachten gilt, hat man vielleicht nicht so wirklich auf dem Radar.

Daher ist wichtig: Vermitteln Sie bei Gelegenheit einige wichtige Aspekte. Auch wenn der eine oder andere Aspekt bereits bekannt sein sollte, schadet ein Austausch nie. Denn man lernt sich kennen und kommt über den Datenschutz ins Gespräch.

Machen Sie es sich einfach

Für ein Gespräch mit den Kollegen können Sie für sich die folgende Checkliste einsetzen. So stellen Sie sicher, dass Sie die wichtigsten Aspekte ansprechen und nichts Wichtiges vergessen. Alternative Idee: Sie können die Checkliste auch leicht anpassen und als Merkblatt bzw. als Selbstcheck an die Kollegen geben. Auch damit fördern Sie die Sensibilität, sprich Awareness.

Checkliste: Datenschutzthemen bei der internen Unternehmenskommunikation

Aspekt	Das können Sie erläutern	Besprochen
Veröffentlichungen sind meist auch ein Datenschutzthema.	› Die Arbeit der internen Kommunikation geht meist mit einer Bearbeitung von Personendaten einher. Insofern sind in der Regel die Anforderungen des Bundesgesetzes über den Datenschutz (DSG) und der entsprechenden Verordnung (DSV) anwendbar. So z. B., wenn Personendaten zumindest teilweise elektronisch bearbeitet werden. › Hinzu kommen können auch andere Vorschriften, etwa im Zusammenhang mit Fotos und Videos das Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (URG).	○ Ja ○ Nein
Anonymität hat Vorrang.	› Um Problemen mit dem Datenschutz oder im Zusammenhang mit dem Persönlichkeitsrecht aus dem Weg zu gehen, sollten Sie nach Möglichkeit auf Personenbezug verzichten. › Auch wenn keine Namen oder Bilder verwendet werden, kann man unter Umständen auf eine bestimmte Person schliessen. Das kann zum Problem werden. Prüfen Sie immer, inwieweit auch ohne konkrete Informationen Rückschlüsse möglich sind.	○ Ja ○ Nein
Vorsicht bei privaten Informationen in Texten	› Haben Informationen keinen direkten geschäftlichen Bezug oder sind sie eher privater Natur, ist Vorsicht geboten. Meist gibt es für eine diesbezügliche Veröffentlichung nur eine Rechtsgrundlage: die Einwilligung der betreffenden Person. Gerade bei Beschäftigten heisst es hier jedoch Augen auf: Für Einwilligungen im Beschäftigungsverhältnis gelten besondere Anforderungen(Art. 328b des Obligationenrechs). › Prüfen Sie kritisch, inwieweit private Informationen für die Aussage überhaupt von Relevanz sind. Steht das Private im Mittelpunkt, ist regelmässig das Okay der betreffenden Person erforderlich.	○ Ja ○ Nein
Fotos können problematisch sein.	› Sollen Fotos veröffentlicht werden, auf denen Personen abgebildet sind, kann das unter Umständen auf ein überwiegendes berechtigtes Interesse gestützt werden. Hier heisst es jedoch, genau prüfen. In der Interessenabwägung müssen die Vorgaben des Persönlichkeitsrechts berücksichtigt werden. › Greifen keine Ausnahmen, ist die Einwilligung des Abgebildeten erforderlich. Das recht am eigenen Bild leitet sich aus Das Recht am eigenen Bild leitet sich aus dem Persönlichkeitsschutz gemäss Art. 28 Zivilgesetzbuch ab. Daher: Klären Sie unbedingt vor einer Veröffentlichung von Fotos oder Videos, inwieweit das zulässig ist.	○ Ja ○ Nein
Verhältnismässigkeit ist wichtig.	› Dabei handelt es sich um einen wichtigen Grundsatz des DSG. Bearbeiten Sie nur so viele persönliche Informationen wie nötig. Verzichten Sie auf nicht erforderliche bzw. überflüssige Informationen in Veröffentlichungen.	○ Ja ○ Nein
Löschen Sie Veraltetes.	› Wenn es um personenbezogene Informationen geht, müssen diese irgendwann gelöscht werden. Meist ist dieser Zeitpunkt gekommen, wenn der Zweck der Bearbeitung erreicht ist. › Gerade im Zusammenhang mit veröffentlichten Bildern oder privaten Informationen kann der Zweck bei Ende des Beschäftigungsverhältnisses wegfallen, sodass Sie Entsprechendes löschen sollten, auch wenn es eine Einwilligung gibt.	○ Ja ○ Nein
Binden Sie den Datenschutzberater früh ein.	› Haben Sie im Zusammenhang mit Personendaten etwas vor oder gibt es Unklarheiten: nicht lange warten! Den Datenschutzberater einbinden.	○ Ja ○ Nein

Wie kann ich mit „Drückebergern" bei Führungskräften umgehen?

FRAGE: Ich biete für Führungskräfte Schulungen zum Datenschutz an. Nachdem ich nun viele Führungskräfte geschult habe, fällt mir auf, dass es einige „Drückeberger" gibt. Die sagen kurzfristig ihre Teilnahme wieder ab oder erscheinen einfach nicht. Da es hier auch einige Mitglieder der Geschäftsleitung gibt, denen es immer wieder nicht möglich ist, teilzunehmen, frage ich mich: Wie soll ich mit solchen „Drückebergern" umgehen?

ANTWORT: Jedermann leuchtet ein: Wer mit Personendaten zu tun hat, der muss zumindest über grundlegendes Know-how verfügen. Um auch wenig verfügbare Beschäftigte in Ihrem Unternehmen mit dem nötigen Wissen zu versorgen, können Sie Folgendes machen:

- **Verdeutlichen Sie den Betreffenden die Erforderlichkeit**
  Gerade Führungskräfte und Unternehmenslenker tragen grosse Verantwortung im Datenschutz. So verantworten sie intern oft nicht nur die Verfahren, Technik oder Prozesse, mit denen Personendaten bearbeitet werden. Sie sind auch dafür verantwortlich, dass die ihnen disziplinarisch zugeordneten Beschäftigten regelkonform und sorgsam mit Personendaten umgehen. Kommt es hier zu Fehlverhalten, kann das auch für die betreffende Führungskraft ernste Konsequenzen haben.
- **Zeigen Sie auf, wer über die Teilnahme entschieden hat**
  Hat die Unternehmensleitung entschieden, dass die Führungskräfte an einer von Ihnen angebotenen Schulung teilnehmen müssen, ist das nicht unbedingt überall angekommen. Machen Sie klar, dass ganz oben die entsprechende Entscheidung gefallen ist. Die Teilnahme ist auch unter Risikoaspekten geboten. Schliesslich muss die Unternehmensleitung dafür Sorge tragen, dass Risiken für das Unternehmen angemessen begegnet wird. Und ein Risiko ist auch, dass Führungskräfte und Beschäftigte gegen den Datenschutz verstossen.
- **Klären Sie darüber auf, welche Folgen ein Fernbleiben haben kann**
  Hier müssen Sie niemandem mit Bussgeldern & Co. drohen. Machen Sie aber deutlich, dass Sie irgendwann der Unternehmensleitung Bericht erstatten müssen, inwieweit alle Führungskräfte an Ihren Schulungen teilgenommen haben. Dann müssen Sie Ross und Reiter benennen. Sie müssen offenlegen, wer es terminlich nie geschafft hat. Und das kann unschöne Konsequenzen für diejenigen haben, die eine Teilnahme bislang umgangen haben. Zumindest ein ernstes Gespräch mit dem Chef dürfte drin sein. Und hier kann man im Ergebnis eigentlich nur schlecht aussehen.
- **Terminfindungsprobleme: Drehen Sie den Spiess um**
  Sie können nach Rücksprache mit der Unternehmensleitung über deren Assistenz einen Termin mit den „Härtefällen" koordinieren lassen. Unter Umständen wird man hier einen Termin eher möglich machen, weil das Vorzimmer des Chefs doch meist grossen Eindruck hinterlässt. Alternativ können Sie die betreffenden Führungskräfte bitten, sich untereinander abzustimmen und Ihnen einen Termin vorzuschlagen.

Wie gehen wir mit Betroffenenanfragen per Telefon um?

FRAGE: Bei uns gab es kürzlich einen Fall, dass jemand sein Recht auf Auskunft am Telefon geltend machen wollte. Unsere Mitarbeiterin bat um Zusendung einer E-Mail, was die Betroffene dann auch gemacht hat. Da hatten wir Glück, denn eine solche Anfrage in Textform ist immer verbindlicher und wir können noch mal genau nachlesen, worum es dem Betroffenen eigentlich genau geht. Wie verhält es sich aber generell mit entsprechenden Anfragen per Telefon?

ANTWORT: Auch solche Anfragen sollten Sie mit der gleichen Sorgfalt bearbeiten wie jede andere Betroffenenanfrage auch. Lässt sich beispielsweise eine Auskunft auch telefonisch erteilen, kann dies prinzipiell auch telefonisch erfolgen.

Beispielsweise, wenn ein Betroffener wissen will, wann er in den Erhalt eines Newsletters eingewilligt haben soll. Ist sichergestellt, dass der Anfragende auch tatsächlich der Betroffene ist, kann die Auskunft auch telefonisch erteilt werden. Problematisch kann es jedoch sein, wenn Sie die Erfüllung des betreffenden Betroffenenrechts dokumentieren wollen. Hier kann es dann doch vorteilhafter und damit auch besser sein, wenn etwa das Auskunftsrecht schriftlich erfüllt wird, etwa per E-Mail an den Betroffenen. Ansonsten sollten Sie zumindest eine Telefonnotiz mit Datum, Uhrzeit und dem Vermerk des Mitarbeiters anlegen, der die Anfrage beantwortet hat.

VG Berlin: keine gemeinsame Verantwortung bei Lettershop

In Sachen Briefwerbung setzen Unternehmen oft auf das Lettershop-Verfahren. Dabei wird etwa eine Agentur beauftragt, die vom Auftraggeber vorbereitete Werbung an die nur der Agentur bekannten Adressen der Zielgruppe zu schicken. Was datenschutzrechtlich „sauber" klingt, kann dennoch zu Ärger führen, wie ein Urteil des Verwaltungsgerichts (VG) Berlin vom 14.10.2025 (Az. 1 K 74/24) zeigt.

Das führte zum Rechtsstreit

Ein Berliner Theater wollte vor Weihnachten 2021 Werbung für sein Angebot machen. Die Werbung sollte per Post erfolgen und sich an eine zahlungskräftigere Zielgruppe richten. Hierzu beauftragte das Theater einen Adresshändler. Dieser sollte das Versenden von vorbereiteter Werbung im Lettershop-Verfahren übernehmen. Das Theater stellte das Werbeschreiben bereit und wählte die Zielgruppenmerkmale. Der Adresshändler selektierte entsprechend den Wünschen des Theaters die Empfängeradressen in seinem Bestand. Im Dezember wurde die Werbung per Post verschickt.

Diese erhielt auch eine Frau in Berlin, die bislang keinerlei Bezug zum Theater hatte. Der Vater der Frau, ihr Betreuer, beschwerte sich im Januar 2022 bei der Datenschutzaufsichtsbehörde. Nachdem die Behörde das Theater mehrfach anhörte, erging am 19.1.2024 ein Bescheid gegenüber dem Theater. Darin verwarnte die Behörde das Theater wegen verschiedener Verstösse gegen die Datenschutz-Grundverordnung (DSGVO). So läge keine Rechtsgrundlage für die Verarbeitung der Adressdaten vor. Ausserdem wäre gegen die Informationspflicht nach Art. 14 DSGVO sowie gegen die Vorgaben zur gemeinsamen Verantwortung nach Art. 26 Abs. 1 und Abs 2 Satz 2 DSGVO verstossen worden. Denn nach Ansicht der Behörde läge eine gemeinsame Verantwortung zwischen Theater und Adresshändler vor.

Theater wehrt sich

Diese behördliche Verwarnung wollte das Theater nicht akzeptieren. Am 23.2.2024 klagte es vor dem VG Berlin. Aus seiner Sicht war ihm nichts vorzuwerfen. Insbesondere wäre es nicht für die Verarbeitung verantwortlich. Man habe nur Zielgruppenvorgaben gemacht. Auf die Verarbeitung der personenbezogenen Daten hätte man keinen Einfluss gehabt. Eine Rechtsgrundlage für die Werbung läge vor, nämlich Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO. Das Gericht urteilte, und zwar zugunsten des Theaters. Die Verwarnung der Datenschutzaufsichtsbehörde wurde aufgehoben.

So begründete das VG sein Urteil

Die Verwarnung der Datenschutzaufsicht ist rechtswidrig und verletzt das Theater in seinen Rechten. Auf das Vorliegen einer Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten kommt es vorliegend nicht an. Das Theater wäre der falsche Adressat der Verwarnung. Es war nämlich mit dem Adresshändler nicht gemeinsam Verantwortlicher im Sinne von Art. 4 Nr. 7, Art. 26 Abs. 1 Satz 1 DSGVO.

Das Verwenden der Adressdaten für das Werbeschreiben ist eine Verarbeitung, die der DSGVO unterliegt. Allerdings lag keine gemeinsame Verantwortung vor.

Hierzu wäre es erforderlich, dass zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel der Verarbeitung festlegen. Zwar können die Beteiligten in verschiedenen Phasen und in unterschiedlichem Ausmass eingebunden sein. Auch muss nicht jeder der Beteiligten Zugang zu den betreffenden personenbezogenen Daten haben. Allerdings ist vor allem die jüngere Rechtsprechung des Europäischen Gerichtshofs (EuGH) so zu deuten: Für die Annahme einer gemeinsamen Verantwortung kommt es auf die tatsächlich im Eigeninteresse erfolgende Einflussnahme auf die Entscheidung über die Zwecke und Mittel der Verarbeitung an.

Voraussetzungen nicht erfüllt

Das Theater hatte zwar im Eigeninteresse Einfluss auf die Zwecke der Verarbeitung durch den Adresshändler genommen, etwa weil es mit der Werbung wirtschaftliche Interessen verfolgte. Allerdings hatte das Theater keinen Einfluss auf die Mittel der Verarbeitung. Es gab für es keine Möglichkeit, auf die Ausgestaltung der Prozesse beim Adresshändler Einfluss zu nehmen. Das Festlegen einer Zielgruppe reicht insofern nicht aus. Es hätte eine über die Erteilung des Auftrags hinausgehende organisatorisch konzeptionelle Mitwirkung an der Datenverarbeitung geben müssen.

§

Diese Schlüsse können Sie aus dem Urteil ziehen

Datenschutzaufsichtsbehörden, also auch der EDÖB, müssen mit ihrer Sicht der Dinge nicht immer richtigliegen. Das gilt gerade, wenn es um schwierig zu fassende Aspekte des Datenschutzrechts geht, wie vorliegend die Voraussetzungen im Sinne von Art. 26 DSGVO. Zudem wird deutlich: Auch wenn es eigentlich nur um eine Verwarnung der Aufsichtsbehörde ging, kann es nötig sein, sich dagegen zu wehren. Das ist z. B. der Fall, wenn damit das wirtschaftliche Handeln Ihres Unternehmens beeinträchtigt wird. Übrigens: An die Entscheidung sollten Sie sich erinnern, wenn „gemeinsame Verantwortung" einmal Thema bei Ihrem Unternehmen ist. Zwar begründet das Gericht seine Entscheidung mit der Rechtsprechung des EuGH. Doch auch aus der EuGH-Rechtsprechung können Sie Argumente für sich ziehen und sich einen Überblick verschaffen.

Datenschutz aktuell Live Talk: Gratis-Webinar

Moderator & Fachexperte
Andreas Würtz

Austausch, Aktualität, fachliche Tiefe für alle mit Aufgaben im Datenschutz

am letzten Freitag jeden Monats

um 16:30 Uhr 60 Minuten

Warum am Live Talk teilnehmen?

Neue Leitlinien, geplante Gesetzesänderungen, behördliche Anforderungen und praxisnahe Umsetzungsfragen stellen Datenschutzverantwortliche regelmäßig vor neue Herausforderungen. Oft bleiben dabei konkrete Fragen offen – oder es fehlt die Gelegenheit, Themen direkt mit einem Experten zu besprechen.

Der **Datenschutz aktuell Live Talk** ist aufgrund seines digitalen Formats bequem von überall erreichbar. Im Mittelpunkt steht ein **vertraulicher, fachlicher Austausch** zu aktuellen Schwerpunktthemen aus Datenschutzrecht und Datenschutzpraxis.

Die Veranstaltung wird **nicht aufgezeichnet.** So entsteht ein geschützter Rahmen, in dem auch sensible Fragestellungen offen angesprochen werden können. Sie entscheiden selbst, wie aktiv Sie teilnehmen möchten: **Bringen Sie Ihre Fragen ein oder hören Sie einfach zu** – ganz nach Ihrem Bedarf und ganz wie Sie mögen.

Der Live Talk ist bewusst kein klassisches Webinar mit Frontalvortrag, sondern ein dialogorientiertes Format, das auf Austausch, Aktualität und fachliche Tiefe setzt.

Ich freue mich auf Ihre Teilnahme!

Ihr Moderator & Fachexperte Andreas Würtz
Rechtsanwalt | Datenschutzexperte
Chefredakteur des Fachratgebers „Datenschutz aktuell“

Jetzt zum nächsten Live-Talk anmelden:

t1p.de/live-talk

PRIVACYXPERTS

Telefon: +49 2 28 95 50 150
Fax: +49 2 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: kurzlink.ch/privacy

Ein Unternehmensbereich des VNR Verlags
für die Deutsche Wirtschaft AG
Theodor-Heuss-Strasse 2–4
53177 Bonn, Deutschland

Vorschau:

Beschwerden managen:
Nutzen Sie diesen Erfassungsbogen

Anweisungen prüfen: Das sind Ihre Checkpunkte