BDIU 2019

Die Europäische Datenschutz-Grundverordnung

Best Practice Guide 2.0

Leitfaden für den Bereich Forderungsmanagement

www.inkasso.de

Die Europäische

Datenschutz-Grundverordnung

Best Practice Guide 2.0

Leitfaden für den Bereich **Forderungsmanagement**

INHALT

VORWORT

LIEBE MITGLIEDER DES BDIU,
LIEBE LESERINNEN, LIEBE LESER,

seit dem 25. Mai 2018 muss die Datenschutz-Grundverordnung (DS-GVO) nunmehr angewendet werden. Sie ist damit nicht nur in den Mitgliedstaaten, sondern in so gut wie jedem Unternehmen der Europäischen Union, und auch darüber hinaus, »gelandet« und findet dort bei den täglichen Datenverarbeitungen Berücksichtigung.

Der »Best Practice Guide – Leitfaden für den Bereich Forderungsmanagement« hat sich dabei in vielen Unternehmen als wertvoller Begleiter erwiesen. Nicht nur die Mitglieder des Bundesverbands Deutscher Inkasso-Unternehmen, sondern alle Firmen, die in irgendeiner Weise mit dem Einzug von Forderungen befasst sind, nutzen diesen Guide zur Klärung datenschutzrechtlicher Fragen.

Um es nicht schöner darzustellen, als es ist: Die Umsetzung der DS-GVO hat die Wirtschaft vor große Herausforderungen gestellt, bzw. sie stellt sie immer noch vor diese. Es war ein gewaltiges Stück Arbeit, die von der Verordnung betroffenen Prozesse zu implementieren – das hat tief in die Datenverarbeitung aller Unternehmen eingegriffen. Stets DS-GVO-konform zu agieren ist nach wie vor höchst anspruchsvoll!

Wir haben uns daher dazu entschlossen, eine Version 2.0 unseres Leitfadens herauszugeben. Inzwischen ist viel passiert. Die DS-GVO wird in den Unternehmen gelebt, viele Probleme konnten gelöst werden – auch solche, von denen man zunächst gar nicht annahm, dass sie überhaupt auftreten würden.

Das vorliegende Heft liefert Ihnen viele praxisbezogene Antworten auf Fragen, die in der täglichen Bearbeitung von datenschutzrelevanten Anfragen, Anträgen und Aufgaben entstehen. Mit dieser Zusammenstellung möchten wir den Unternehmen aus dem Bereich Forderungsmanagement erneut und aktualisiert Tipps an die Hand geben, wie sie am besten und praktischsten die DS-GVO in ihr Unternehmen bringen können.

Ihre

Kirsten Pedd
Präsidentin des BDIU

Berlin, im Oktober 2019

1. // ÜBERBLICK

Nach der Übergangsphase von zwei Jahren ist die Datenschutz-Grundverordnung (DS-GVO) nun seit dem 25. Mai 2018 unmittelbar in den europäischen Staaten geltendes Recht – darüber hinaus auch für Unternehmen mit Niederlassung außerhalb der EU, die Personen innerhalb der EU Waren oder Dienstleistungen anbieten und in diesem Kontext deren Daten erheben und weiterverarbeiten.

Die DS-GVO bringt erhöhte Anforderungen an den Datenschutz für Unternehmen mit sich – und hat damit Folgen für alle Inkassodienstleister

Zeitgleich mit dem Anwendungsbeginn der DS-GVO ist in Deutschland am 25. Mai 2018 das neue Bundesdatenschutzgesetz (BDSG) in Kraft getreten. Dieses Gesetz ergänzt an einigen Stellen die DS-GVO und setzt sie um. Das ist möglich, weil die europäische Verordnung zahlreiche Öffnungsklauseln enthält, die es den Mitgliedstaaten ermöglichen, eigene Regelungen zu treffen.

Das Datenschutzniveau wurde mit dem neuen Datenschutzrecht nicht abgesenkt, sondern an einigen Stellen sogar weiter angehoben. Insbesondere enthält die DS-GVO Transparenz- und Dokumentationsvorgaben für Verantwortliche der Datenverarbeitung und für Auftragsverarbeiter, die das bis 24. Mai 2018 geltende, alte BDSG so nicht kannte.

Inkassodienstleister sind Verantwortliche im Sinne der DS-GVO – der BDIU zeigt deswegen auf, welche Anforderungen sich daraus für die Branche ergeben und worauf die Unternehmen unbedingt zu achten haben. Dies vor allem vor dem Hintergrund, dass die Möglichkeiten für Eingriffe und Sanktionen der Datenschutzaufsichtsbehörden durch die DS-GVO wesentlich erweitert und verschärft wurden und die Behörden nunmehr verstärkt die Einhaltung insbesondere der Dokumentationsvorgaben überprüfen.

Anzumerken ist, dass der vorliegende Best Practice Guide 2.0 die DS-GVO hauptsächlich mit Blick auf die Verarbeitung personenbezogener Daten von Forderungsschuldnern beleuchtet. Doch Vorsicht: Die Grundsätze der Verarbeitung müssen auch bei anderen natürlichen Personen berücksichtigt werden, z. B. bei Mitarbeitern!

2. // FORDERUNGSMANAGEMENT DURCH INKASSODIENSTLEISTER

Die DS-GVO findet Anwendung auf Inkassodienstleister – denn ohne die Verarbeitung von personenbezogenen Daten kann professionelles Forderungsmanagement nicht betrieben werden.

Forderungsmanagement sichert die Liquidität von Unternehmen

Die Ziele des Forderungsmanagements sind allgemein:

- Forderungsausfälle so gering wie möglich zu halten,
- Unternehmen aus allen Wirtschaftsbereichen zu entlasten,
- die notwendige Liquidität der Wirtschaftsunternehmen zu erhalten und dabei
- die Kosten des erstattungspflichtigen Schuldners so gering wie möglich zu halten und zugleich die Justiz zu entlasten, da durch die außergerichtliche Forderungseinziehung eine Vielzahl gerichtlicher Mahnverfahren vermieden werden kann.

Inkassodienstleister sind Rechtsdienstleister

Der Schwerpunkt des Forderungsmanagements von Inkassounternehmen liegt in der Erbringung von Inkassodienstleistungen. § 2 Abs. 2 RDG regelt, dass dies die Einziehung fremder oder zum Zweck der Einziehung auf fremde Rechnung abgetretener Forderungen ist, wenn die Forderungseinziehung als eigenständiges Geschäft betrieben wird. Die Inkassodienstleistung ist eine Rechtsdienstleistung, die einer strengen gesetzlichen Regulierung unterliegt und nur von registrierten und besonders qualifizierten Personen bzw. Unternehmen erbracht werden darf.

Vom außergerichtlichen Inkasso bis zur Zwangsvollstreckung: nur solide Daten ermöglichen

Die Tätigkeit von Inkassodienstleistern umfasst im Kern das vorgerichtliche Inkasso, die Durchführung des gerichtlichen Mahnverfahrens, die Beantragung von Zwangsvollstreckungsmaßnahmen (in das bewegliche Vermögen des Schuldners) sowie die langfristige Verfolgung offener Forderungen, ggf. auch die Ausbringung insolvenzrechtlicher Maßnahmen.

Die Effektivität der Inkassodienstleistung hängt dabei entscheidend davon ab, dass die Dienstleister ein breites Spektrum an Services anbieten und durchführen können. Dazu gehören z. B. Adressermittlungen, Bonitätsprüfungen und Außendiensteinsätze.

Inkassodienstleister sind »Verantwortliche« im Sinne der DS-GVO

Inkassounternehmen sind »Verantwortliche« im Sinne der DS-GVO, da sie über die Zwecke und Mittel der Verarbeitung personenbezogener Daten selbstständig entscheiden (Art. 4 Nr. 7).

Die Inkassodienstleistung stellt keine Auftragsverarbeitung dar. Eine mögliche Ausnahme: die Tätigkeit als Verwaltungshelfer für die öffentliche Hand, die in aller Regel als Auftragsverarbeitung angesehen wird.

3. // ANFORDERUNGEN AN DIE DATENVERARBEITUNG

Nach der DS-GVO ergeben sich die wesentlichen Anforderungen an die Datenverarbeitung aus den Grundsätzen (Art. 5). Insbesondere müssen eine Rechtsgrundlage vorliegen und die festgelegten Zwecke gewahrt werden (z. B. Art. 6 Abs. 1, Art. 6 Abs. 4).

3.1. // DIE GRUNDSÄTZE DER DS-GVO

Die Grundsätze lauten gemäß Art. 5 Abs. 1:

- Prinzip der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 Buchstabe a)
- Prinzip der Zweckbindung (Art. 5 Abs. 1 Buchstabe b)
- Prinzip der Datenminimierung (Art. 5 Abs. 1 Buchstabe c)
- Prinzip der Richtigkeit (Art. 5 Abs. 1 Buchstabe d)
- Prinzip der Speicherbegrenzung (Art. 5 Abs. 1 Buchstabe e)
- Prinzip der Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchstabe f)

Wie diese Grundsätze einzuhalten sind, wird in den folgenden Kapiteln beschrieben.

3.2. // RECHENSCHAFT MITTELS DOKUMENTATION

Die Rechenschaftspflicht aus Art. 5 Abs. 2 ist in dieser Art neu im Vergleich zum früheren Datenschutzrecht. Der Inkassodienstleister muss nachweisen können, dass er die gesetzlichen Vorgaben einhält. Alle Geschäftsprozesse und sogenannten technisch-organisatorischen Maßnahmen müssen daher vom Inkassodienstleister dokumentiert werden. |1|

3.3. // RECHTSGRUNDLAGEN UND ZWECKBINDUNG IM ÜBERBLICK

Die DS-GVO setzt strenge Maßstäbe an die Datenverarbeitung.

Die Datenverarbeitung muss auf einer Rechtsgrundlage erfolgen. Außerdem muss für die Datenverarbeitung ein Zweck festgelegt sein und gewahrt werden. Dies gilt auch für jede Verarbeitung personenbezogener Daten durch Inkassodienstleister.

Verbot mit Erlaubnisvorbehalt bleibt

Nach der DS-GVO gilt: Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage (auch: »Verbot mit Erlaubnisvorbehalt«).

Das heißt: Jede Verarbeitung |2| personenbezogener Daten |3| ist grundsätzlich verboten, es sei denn, die betroffene Person |4| hat eingewilligt oder (mindestens) eine Rechtsvorschrift erlaubt diese Verarbeitung.

Außerdem ist eine Datenverarbeitung nur zu vom Inkassounternehmen festgelegten Zwecken rechtmäßig, die auch für weitere Verarbeitungen derselben Daten maßgeblich sind.

4. // RECHTMÄSSIGKEIT DER DATENVERARBEITUNG

DS-GVO-Regelungen
- *Art. 4: Begriffsbestimmungen*
- *Art. 5: Grundsätze für die Verarbeitung personenbezogener Daten*
- *Art. 6: Rechtmäßigkeit der Verarbeitung*
- *Art. 7: Bedingungen für die Einwilligung*
- *Art. 9: Verarbeitung besonderer Kategorien personenbezogener Daten*
- *Art. 10: Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten*

BDSG-Regelung
- *§ 24: Verarbeitung zu anderen Zwecken durch nicht öffentliche Stellen*

4.1. // RECHTSGRUNDLAGEN FÜR DIE DATENVERARBEITUNG

4.1.1. // Gesetzliche Erlaubnisnormen zur Datenverarbeitung

Dreh- und Angelpunkt der Datenverarbeitung im Bereich des Forderungsmanagements ist Art. 6 Abs. 1 Buchstaben b, c und f – hier sind die gesetzlichen Erlaubnisse geregelt.

Dreh- und Angelpunkt: gesetzliche Erlaubnisse

- **Art. 6 Abs. 1 Buchstabe b** ist die Rechtsgrundlage für die Verarbeitungen personenbezogener Daten, die für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich sind – dazu gehören auch Datenverarbeitungen rund um die Zahlungsverpflichtung des Schuldners. Immer wenn es um das Forderungsmanagement in Bezug auf durch Vertrag entstandene Forderungen geht, kommt diese Erlaubnisnorm zur Anwendung. Diese Rechtsgrundlage gilt unter den gleichen Voraussetzungen bereits für Datenverarbeitungen des Mandanten und wird vom Inkassodienstleister quasi »übernommen«.

- **Art. 6 Abs. 1 Buchstabe c und Abs. 3** ist die Rechtsgrundlage für Verarbeitungen personenbezogener Daten, die zur Erfüllung rechtlicher Verpflichtungen erforderlich sind, z. B. zur Einhaltung nationaler gesetzlicher Aufbewahrungsfristen. Im deutschen Recht ergeben sich die Aufbewahrungspflichten aus der Abgabenordnung (AO), dem Handelsgesetzbuch (HGB) und dem Umsatzsteuergesetz (UStG).

- **Art. 6 Abs. 1 Buchstabe f** ist die Rechtsgrundlage für Verarbeitungen personenbezogener Daten, die zur Wahrung der berechtigten Interessen des Verantwortlichen (des Inkassounternehmens) oder eines Dritten (des Mandanten) erforderlich sind. Auch z. B. die Verarbeitung von Schuldnerdaten für eine optimale Schuldneransprache, die Einmeldung von forderungsbezogenen Daten bei Auskunfteien sowie für die Betrugsprävention fallen unter diese Regelung.

- **§ 24 Abs. 1 Nr. 2 BDSG** ist die Rechtsgrundlage, wenn es um Datenverarbeitungen zu einem weiteren, im Vergleich zum ursprünglichen Zweck anderen Zweck geht und dieser der Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche dient.

|1| Siehe: 8. // Umfangreiche Dokumentationspflichten, Seite 33.
|2| Siehe: 18. // Begriffe, Seite 59.
|3| Siehe: 18. // Begriffe, Seite 59.
|4| Siehe: 18. // Begriffe, Seite 59.

Die Erhebung von Daten durch einen Inkassodienstleister ist im Rahmen der Beitreibung einer offenen Forderung nach Art. 6 Abs. 1 Buchstaben b bzw. f erlaubt, da der Betroffene seinen Zahlungsverpflichtungen aus einem bestehendem Schuldverhältnis nicht nachgekommen ist.

Bei Übergabe der Forderung an ein Inkassounternehmen werden alle zur Forderungseinziehung erforderlichen Daten von Mandanten an den Rechtsdienstleister übermittelt, d. h. zum einen die Forderungsdaten wie Forderungshöhe, Nebenkosten, Zinsen, Fälligkeitsdaten, Forderungsgrund, Mahndaten, zum anderen die Informationen über den Schuldner selbst, z. B. Namensdaten, Geburtsdaten, Adress- und Kommunikationsdaten.

Diese Daten benötigt das Inkassounternehmen, um die vom Mandanten beauftragte Forderungseinziehung durchführen zu können.

4.1.2. // Einwilligung

Einwilligung bleibt die Ausnahme

Die Einwilligung als Rechtsgrundlage für Datenverarbeitungen durch den Inkassodienstleister als Verantwortlichen bildet eher die Ausnahme. Selbst im Bereich des Forderungsmanagements in Bezug auf privatärztliche Forderungen ist Rechtsgrundlage regelmäßig Art. 6 Abs. 1 Buchstabe b bzw. f und ggf. Art. 9 Abs. 2 Buchstabe f (z. B. Gesundheitsdaten |5|).

Einwilligung – nur mit Hinweis auf Widerrufsrecht

Wird eine erteilte Einwilligung als Rechtsgrundlage herangezogen, muss die betroffene Person auf ein ihr diesbezüglich jederzeit zustehendes Widerrufsrecht hingewiesen werden |6|.

Wenn eine Einwilligung die Rechtsgrundlage sein soll, ergeben sich aus Art. 6 Abs. 1 Buchstabe a, Art. 7 und 4 Nr. 11 zahlreiche Voraussetzungen. Unter anderem muss dieser Widerruf genauso einfach möglich sein wie die Erteilung der Einwilligung.

4.1.3. // Erforderlichkeit (Grundsatz der Datenminimierung)

Bei allen Rechtsgrundlagen, bis auf die Einwilligung, muss die Verarbeitung der personenbezogenen Daten »erforderlich« sein. Diese zentrale Voraussetzung konkretisiert den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c). Um dem Grundsatz der Datenminimierung nachzukommen, sollte das Inkassounternehmen sich an folgende Faustformel halten: »So viel wie nötig, so wenig wie möglich«. Daten, die nicht zum Forderungsmanagement und zur Erfüllung der weiteren Zwecke erforderlich sind, dürfen nicht verarbeitet werden.

- **Umgang mit Vorgangsnotizen/Freitextfeldern**

  Ein besonderes Augenmerk ist daher auch auf Vorgangsnotizen zu legen, die von den jeweiligen Mitarbeitern angelegt werden können.

  Informationen über den Betroffenen, die in solch unstrukturierter Form verarbeitet werden, müssen bezüglich der Löschung gesondert geprüft und berücksichtigt werden. Den geringsten Aufwand dürfte es bedeuten, wenn personenbezogene Daten in den Vorgangsnotizen/Freitextfeldern nicht hinterlegt werden (z. B. Verzicht auf Verwendung von Namensdaten). Dies kann durch Arbeitsanweisungen und Schulungsmaßnahmen im Unternehmen beim Verantwortlichen umgesetzt werden, mit deren Hilfe die Mitarbeiter entsprechend sensibilisiert werden.

- **Umgang mit Bonitätsmerkmalen**

  Merkmale zum Zahlungsverhalten des Schuldners werden in der Regel im Laufe der Forderungseinziehung bei einer Auskunftei abgefragt, um prüfen zu können, welche Maßnahmen im Beitreibungsprozess sinnvoll sind. Diese Bonitätsmerkmale einer Person können ebenso wie alle übrigen Daten gespeichert werden, soweit und solange sie für den Beitreibungsprozess benötigt werden.

- **Umgang mit Daten von »Mehrfachschuldnern«**

  Die Erfahrung zeigt, dass Personen, die sich häufiger im Zahlungsverzug befinden und schon einmal von einem Inkassodienstleister angeschrieben worden sind, mehrfach als Schuldner bei diesen auftauchen. Für eine ordnungsgemäße und angemessene Vorgehensweise gegenüber solchen »Mehrfachschuldnern« ist in aller Regel die Kenntnis von Daten erforderlich, die bei anderen Vorgängen gespeichert wurden. Dies entspricht zudem dem zivilrechtlichen Grundsatz der Schadensminderungspflicht.

4.2. // GRUNDSATZ DER ZWECKBINDUNG

Zwecke der Datenverarbeitung müssen eindeutig und legitim sein

Art. 5 Abs. 1 Buchstabe b regelt den Grundsatz der Zweckbindung: Schon vor der Datenerhebung muss jeder Verantwortliche festlegen, zu welchem Zweck die jeweilige Datenverarbeitung erfolgt. Auch jeder Inkassodienstleister muss daher festlegen, welche Daten für welche Zwecke verarbeitet werden sollen.

Jeder Zweck im Sinne der DS-GVO muss eindeutig und legitim sein: Der Zweck der Verarbeitung von Daten durch den Inkassodienstleister muss dem ursprünglichen Zweck entsprechen, der mit bzw. vom Mandanten festgelegt worden ist.

Wird vom Inkassodienstleister ein anderer Zweck verfolgt als der ursprüngliche, ist die Datenverarbeitung nach § 24 Abs. 1 Nr. 2 BDSG möglich, wenn sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist und die Interessen des Schuldners nicht überwiegen. § 24 BDSG kann somit nicht nur als Rechtsgrundlage herangezogen werden, sondern auch dann, wenn es darum geht, festzustellen, ob der Zweck der Datenverarbeitung zulässig ist.

Aber: Datenverarbeitungen, die zu einem anderen Zweck als dem ursprünglichen erfolgen, aber nicht die Voraussetzungen des § 24 BDSG erfüllen, können ebenfalls zulässig sein. Insofern ist Art. 6 Abs. 4 anzuwenden. Dabei ist darauf zu achten, dass der nunmehr festgelegte, neue Zweck nicht in Widerspruch zum ursprünglichen Zweck steht und beide Zwecke miteinander vereinbar sind.

4.2.1. // Zweckfestlegung

Inkassodienstleister legen Zweck der Datenverarbeitung fest

Inkassodienstleister müssen (mindestens) einen Zweck der Datenverarbeitung festlegen, so wie jeder andere Verantwortliche auch.

Die Übergabe einer Forderung des Mandanten an den Inkassodienstleister sowie die dortigen Datenverarbeitungen können, aber müssen nicht aufgrund derselben Rechtsgrundlage erfolgen, die für die Datenverarbeitungen rund um die Forderungseinziehung bei dem Mandanten gilt. Mit dem Zweck verhält es sich vergleichbar. Der vom Mandanten für die Datenverarbeitung festgelegte Zweck der »Vertragsabwicklung« bzw. in aller Regel der »Rechtsverfolgung« wird auch bei der Übergabe an den Inkassodienstleister sowie bei den Datenverarbeitungen im Rahmen der Inkassodienstleistung weiterverfolgt.

Im Übrigen muss der Inkassodienstleister, ebenso sein Mandant, die gesetzlichen Aufbewahrungsfristen beachten, sodass die entsprechenden Datenverarbeitungen auch zum Zweck der Erfüllung der Aufbewahrungspflichten erfolgen.

4.2.2. // Forderungsmanagement als weiterer Zweck

Mit der Übergabe der Forderung und der für die Forderungseinziehung erforderlichen personenbezogenen Daten kommt aber ein weiterer Zweck beim Inkassodienstleister hinzu.

|5| Siehe: 4. // Rechtmäßigkeit der Datenverarbeitung, Seite 11, und 18. // Begriffe, Seite 59.

|6| Siehe: 7. // Informationspflichten und Betroffenenrechte, Seite 21.

Der Rechtsdienstleister legt regelmäßig für Datenverarbeitungen ab Erhebung der Daten den eigenen Zweck »Forderungsmanagement« fest. Damit ist es dem Inkassodienstleister möglich, Daten nicht nur in Bezug zu einer konkreten Forderung zu verarbeiten, sondern diese darüber hinaus bei der Einziehung weiterer Forderungen mitzuberücksichtigen. Denn nur so kann der Inkassodienstleister dazu beitragen, Forderungsausfälle so gering wie möglich zu halten, die notwendige Liquidität der Wirtschaftsunternehmen zu erhalten und dabei den erstattungspflichtigen Schuldner so wenig wie möglich mit weiteren Kosten zu belasten.

Die Datenverarbeitungen zu einem weiteren, anderen Zweck müssen den Anforderungen des § 24 BDSG bzw. des Art. 6 Abs. 4 genügen.

Denn: Verarbeitet das Inkassounternehmen personenbezogene Daten im Rahmen des »Forderungsmanagements«, wird damit ein weiterer, neuer Zweck verfolgt, wobei dies den Anforderungen der erwähnten Vorschriften standhalten muss. |7|

Forderungsmanagement ist mit ursprünglichem Zweck vereinbar

Die Verfolgung dieses weiteren Zwecks ist rechtlich nicht zu beanstanden, da das professionelle Forderungsmanagement durch einen Inkassodienstleister mit dem ursprünglichen Zweck des Mandanten (dort: »Vertragsabwicklung« bzw. »Rechtsverfolgung«) zumindest vereinbar im Sinne der gesetzlichen Vorgaben ist, wenn es nicht sogar der Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche dient.

Tipp

Das Inkassounternehmen sollte als Zweck der Datenverarbeitung »Forderungsmanagement« angeben. Ist dies der Fall, muss er entsprechend bei den Informationen an die betroffene Person gemäß Art. (13 bzw.) 14 sowie im Rahmen der Auskunftserteilung gemäß Art. 15 angegeben werden.

Zweckangabe – so funktioniert es!

4.3. // SONDERFÄLLE

Bei der Verarbeitung von Gesundheitsdaten und Co. beim Forderungseinzug gelten weiterhin Besonderheiten

4.3.1. // Verarbeitung besonderer Kategorien personenbezogener Daten

Die Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. Gesundheitsdaten oder Daten zu religiöser Überzeugung) ist grundsätzlich untersagt (Art. 9 Abs. 1).

Das Verbot der Verarbeitung gilt allerdings nicht, soweit Art. 9 Abs. 2 Buchstabe f herangezogen werden kann. Hiernach ist die Verarbeitung zur »Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen«, wozu auch der Forderungseinzug gehört, erlaubt, soweit die Verarbeitung erforderlich ist.

Soweit im Bereich des Forderungsmanagements in Bezug auf privatärztliche Forderungen eine Verarbeitung von Gesundheitsdaten erforderlich sein sollte, ist diese regelmäßig ebenfalls nach Art. 9 Abs. 2 Buchstabe f erlaubt.

4.3.2. // Verarbeitung personenbezogener Daten hinsichtlich strafrechtlicher Verurteilungen und Straftaten

Geht man nur nach dem Wortlaut des Art. 10, dürfen Inkassounternehmen nicht Daten hinsichtlich einer gegen einen Schuldner geltend gemachten Forderung verarbeiten, die im Zusammenhang mit einer etwaigen strafrechtlichen Verurteilung des Schuldners stehen (z. B. wegen Betrugs).

Sinn und Zweck der Regelung ist es aber, neben dem behördlichen Strafregister (Bundeszentralregister) kein »privates« Strafregister entstehen zu lassen.

Insofern kann eine – rein erläuternde – Speicherung über die Strafverfolgung, sofern ein Schuldner im Zusammenhang mit der geltend gemachten Forderung strafrechtlich verurteilt wurde, nicht von diesem Verbot umfasst sein.

Nach Erledigung der Forderung sollten solche Daten jedenfalls schon nach den Grundsätzen der Speicherbegrenzung gelöscht werden, soweit nicht besondere Gründe die weitere Speicherung erforderlich machen.

4.3.3. // Dynamische Prozesssteuerung

Um erfolgreiche und kostengünstige Maßnahmen, insbesondere im Hinblick auf die Schadensminderungspflicht gegenüber dem Schuldner, vorzunehmen, wird eine dynamische Prozesssteuerung bei der Erfüllung von Inkassoaufträgen im Rahmen des Forderungsmanagements genutzt.

Dynamische Prozesssteuerungen können vom sehr weiten Begriff »Profiling« erfasst sein. Profiling ist in Art. 4 Nr. 4 definiert und kann auf die Rechtsgrundlage des Art. 6 Abs. 1 Buchstabe f gestützt werden.

Profiling ist nicht verboten – besondere Vorschriften sind aber zu beachten!

So werden im Rahmen der dynamischen Prozesssteuerung Daten analysiert und die entsprechenden Analyseergebnisse für die Steuerung interner Abläufe im Inkassounternehmen genutzt, die im Rahmen des Forderungsmanagements erforderlich sind.

Damit erlaubt die DS-GVO grundsätzlich Profiling und ermöglicht damit auch eine dynamische Prozesssteuerung im Rahmen des Forderungsmanagements. Bei diesen Maßnahmen handelt es sich um Maßnahmen zur internen Ablaufsteuerung mit der weiteren Konsequenz, dass der Inkassodienstleister grundsätzlich keine Entscheidungen aufgrund automatisierter Verarbeitung im engeren Sinne des Art. 22 trifft, sodass ihn auch dahingehende Informations- bzw. Auskunftspflichten nicht treffen. |8|

|7| Sollten darüber hinaus andere Zwecke verfolgt werden, müssen diese ebenfalls gemäß Art. 6 Abs. 4 vereinbar mit dem ursprünglichen Zweck sein.

|8| Whitepaper zu den Anforderungen der DS-GVO an die Tätigkeit von Inkassodienstleistern von Dr. Kai-Uwe Plath, KNPZ Rechtsanwälte, abrufbar unter: https://www.inkasso.de/files/bdiu-dsgvo-white-paperpdf.

5. // DATENÜBERTRAGUNG AN AUSSEREUROPÄISCHE EMPFÄNGER (DRITTLÄNDER)

DS-GVO-Regelungen

- *Art. 44–50: Übermittlung personenbezogener Daten an Drittländer*

In der DS-GVO werden die Anforderungen an den internationalen Datentransfer, d. h. die Übermittlung und Verarbeitung von Daten von einem Unternehmenssitz in der Europäischen Union bzw. im Europäischen Wirtschaftsraum (EWR) |9| in ein Drittland, geregelt.

Der europäische Gesetzgeber hat mit der DS-GVO das Datenschutzniveau unter den Mitgliedsländern der EU vereinheitlicht. Darüber hinaus gilt sie – indirekt – auch für die anderen Länder, die Teil des EWR sind, also Norwegen, Island und Liechtenstein. Innerhalb des gesamten EWR (einschließlich EU) können Daten unter denselben Voraussetzungen übertragen werden wie innerhalb Deutschlands.

Für bestimmte Staaten außerhalb des EWR gibt es erhebliche Erleichterungen, wenn die Europäische Kommission die Gleichwertigkeit des Datenschutzniveaus festgestellt hat. Das ist bisher der Fall für Andorra, Argentinien, Kanada, die Färöer-Inseln, Guernsey, Israel, die Isle of Man, Japan, Jersey, Neuseeland, die Schweiz, Uruguay und die Vereinigten Staaten von Amerika. Die Einzelheiten ergeben sich aus dem jeweiligen EU-Kommissionsbeschluss.

Datentransfers in Drittstaaten können im Rahmen der Kundenbeziehungen, bei Auslandsinkasso, innerhalb von Konzernen oder gegenüber Dienstleistern erfolgen. Insofern ist in diesen Bereichen ein besonderes Augenmerk auf die Einhaltung der datenschutzrechtlichen Vorgaben zu achten.

Genaue Überprüfung bei Nutzung von Cloud-Services erforderlich

Typische Beispiele für Drittlandtransfers können auch Cloud-Services sein, z. B. die folgenden:

- Microsoft Online Services
  (Office-365-Produkte, wie z. B. OneDrive, Outlook, SharePoint, Azure)
- Dropbox
- Apple iCloud
- Google Cloud und andere Google-Dienste (z. B. Google Docs, Google Übersetzer),
- Web-Messenger,
- Amazon Web Service (AWS)

Diese Liste ist nur ein kleiner Ausschnitt und jeden Tag kommen neue Cloud-Provider hinzu. Es ist unerlässlich, bei solchen Anbietern nachzufragen, wo die Daten tatsächlich verarbeitet werden (z. B. auch bei Fernzugriffen).

Es ist auch auf Leistungen zu achten, die unter den Stichworten »Software as a Service« (SaaS), »Platform as a Service« (PaaS) oder »Infrastructure as a Service« (IaaS) beworben werden. Diese Leistungen werden üblicherweise immer im Cloud-Modell angeboten. Auch hier sollte genau geprüft werden, wo Daten verarbeitet bzw. gespeichert werden und wer ggf. von wo Zugriff auf die Daten hat.

Tipp

Empfohlen wird der Abschluss von EU-Standard-Vertragsklauseln mit dem Anbieter.

Neben den EU-Standard-Vertragsklauseln gibt es noch bei der Datenübermittlung innerhalb von Konzernen die Möglichkeit »verbindlicher Datenschutzrichtlinien« (BCR) sowie der Einwilligungserklärung der betroffenen Person, die jedoch für das Forderungsmanagement nicht relevant sein dürften.

|9| Vgl.: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:22018D1022&from=DE.

6. // LÖSCHEN VON PERSONENBEZOGENEN DATEN

DS-GVO-Regelung
- *Art. 17: Recht auf Löschung (»Recht auf Vergessenwerden«)*

BDSG-Regelung
- *§ 35: Recht auf Löschung*

6.1. // GRUNDSÄTZLICHES

Die DS-GVO regelt in Art. 17 das Recht des Betroffenen, die Löschung seiner Daten beim Verantwortlichen zu verlangen, sowie die Verpflichtung des Verantwortlichen, personenbezogene Daten nach Erfüllung der Verarbeitungszwecke seinerseits zu löschen.

Dies stellt (auch) Inkassounternehmen vor Herausforderungen, da vielfach eine längerfristige Speicherung von Schuldnerdaten, insbesondere der Adresshistorie, von großer Bedeutung und im Sinne der Schadensminderungspflicht sein kann.

Die Regelungen der DS-GVO zur Löschung sind in weiten Teilen auslegungsbedürftig. Sie geben damit aber, ähnlich wie das alte Datenschutzrecht, einem Unternehmen z. B. den nötigen Spielraum für die Festlegung der Speicherdauer, die es zur Erfüllung seiner Unternehmenszwecke benötigt.

Tipp

Für die spätere Löschung macht es Sinn, gleichartige Daten zu Datenkategorien zusammenzufassen, z. B.:

- *Namensdaten (abgebildet in einer Inkassosoftware mit den Datenfeldern »Titel«, »Vorname«, »Nachname«)*
- *Geburtsdaten (z. B. »Geburtsdatum«, »Geburtsort«, »Geburtsname«)*
- *Adressdaten (»Straße«, »Hausnummer«, »Postleitzahl« und »Ort«)*
- *Kommunikationsdaten (»E-Mail«, »Mobilnummer«, »Festnetznummer«, »Fax«)*

Erstellen Sie zu jeder Datenkategorie ein eigenes Sperr- und Löschkonzept und prüfen Sie, ob dies auch für Ihr aktuelles IT-Inkassosystem anwendbar ist. Lassen Sie sich bei Fragen am besten von Ihrem Softwareanbieter/Dienstleister unterstützen.

6.2. // AB WANN ZU LÖSCHEN IST

Löschverpflichtung an Zweck gekoppelt

Personenbezogene Daten sind dann zu löschen, wenn diese nicht mehr für den Verarbeitungszweck benötigt werden. Anders gesagt: Eine Löschverpflichtung besteht nicht, solange Gründe vorliegen, bestimmte Daten einer Person vorzuhalten, die für den Forderungseinzug – damit für die Zwecke »Vertragsabwicklung« bzw. »Rechtsverfolgung« und »Forderungsmanagement« – dienlich sind oder sein können.

6.2.1. // Aufbewahrung bis zur Erledigung einer Forderung

Solange gegen den Schuldner noch eine Forderung offen ist oder der Auftrag des Mandanten zum Forderungseinzug nicht durch andere Gründe als die Forderungsbegleichung beendet ist, darf der Inkassodienstleister die »Schuldnerdaten«, d. h. alle personenbezo-

genen Daten, die zur Forderungseinziehung erforderlich sind, verarbeiten und muss diese nicht löschen. Auch wenn der Betroffene dies ausdrücklich wünscht, kann er sein Recht auf Löschung nicht durchsetzen, da Rechtsansprüche gegen den Schuldner geltend gemacht werden können (Art. 17 Abs. 3 Buchstabe e).

Insofern können auch in der Inkassosoftware, da technisch bedingt so aufbereitet, Personendaten (z. B. Kundenstammsatz, Schuldnerdaten oder Kontaktdatensatz) nur an einer Stelle gespeichert und mit Forderungsdaten verknüpft werden, z. B.: Schuldner 1 ist referenziert zu Forderung 1, Schuldner 2 ist referenziert zu Forderung 2 und Forderung 3 (»Mehrfachschuldner«) etc.

Zu beachten ist, dass personenbezogene Daten nicht nur in der Inkassosoftware verarbeitet werden, sondern oftmals auch in anderen Datensätzen enthalten sind (z. B. in Briefen an den Schuldner oder in Telefonnotizen, die separat aufbewahrt und nicht in den Datenfeldern der Inkassosoftware abgebildet werden). Letztere sind bei einer Löschung separat zu betrachten.

6.2.2. // Falsche oder unzulässige Daten

Daten, die falsch sind, müssen stets berichtigt werden, d. h., alte, falsche Daten müssen an sich gelöscht werden. Aber: Eine Löschung kommt nur dann in Betracht, wenn diese Daten nicht mehr zur Dokumentation, für eventuelle Nachweispflichten und/oder zur Abwehr von Rechtsansprüchen sowie zur Vermeidung einer erneuten Nutzung dieser falschen Daten benötigt werden.

Tipp

Regeln Sie die manuelle Löschung von Daten durch Arbeitsanweisungen. Geben Sie dort Gründe an, wann und wie Daten zu löschen sind. Definieren Sie auch die Ausnahmen und dokumentieren Sie beides, also die Löschung und deren Begründung wie auch die Ablehnung einer Löschung, in der Forderungsakte.

6.2.3. // Antrag eines Betroffenen auf Löschung

Dokumentations- und Nachweispflichten auch bei Frage nach Löschung zu beachten

Wenn ein Betroffener mündlich oder schriftlich fordert, dass bestimmte Daten, die das Inkassounternehmen von einem Dritten (z. B. dem Mandanten) oder vom Betroffenen selbst erhalten hat, zu löschen sind, muss das Inkassounternehmen prüfen, ob Gründe vorliegen, die einer Löschung entgegenstehen. Sind die jeweiligen Daten für den Beitreibungsprozess und die Aufgabenwahrnehmung des Inkassounternehmens (insbesondere zur Erreichung des Zwecks »Forderungsmanagement«) relevant oder zur Erfüllung der gesetzlichen Aufbewahrungspflicht erforderlich, besteht gemäß Art. 17 Abs. 3 Buchstaben b und e kein Löschanspruch.

6.2.4. // Aufbewahrungspflichten nach Erledigung einer Forderung

Sobald eine Forderung, z. B. nach Zahlung, erledigt ist, ist zu prüfen, welche Daten weiterhin in der Inkassosoftware aufbewahrt werden können.

Alle Dokumente, die vom Inkassounternehmen an die Beteiligten innerhalb eines Beitreibungsprozesses versendet wurden, sind als Geschäftsbriefe zu behandeln und unterliegen einer gesetzlichen Aufbewahrungsfrist von sechs Jahren (§ 257 HGB). Darüber hinaus können anderweitige gesetzliche Aufbewahrungspflichten dazu führen, dass diese Daten noch länger aufzubewahren sind, z. B. buchhalterisch relevante Informationen aus der Forderungsakte für zehn Jahre (§ 147 AO). Daten der Kategorien »Ausgangspost« und »Buchungsvorgänge« unterliegen dieser Aufbewahrungsfrist.

Auch Daten aus Datenfeldern der Inkassosoftware, die zur Erstellung dieser Daten geführt haben, sind aufzubewahren. Sie sollen als Nachweis zur ordnungsgemäßen Erstellung der Geschäftsbriefe und der Buchungen dienen.

6.3. // WIE ZU LÖSCHEN IST

Eine DS-GVO-konforme Inkassosoftware stellt Löschfunktionen zur Verfügung. Die Konfiguration ist aber technisch anspruchsvoll.

Softwarehersteller helfen weiter! Verantwortlich bleibt das Inkassounternehmen

Tipp

Kontaktieren Sie Ihren Softwarehersteller und lassen Sie sich zur Löschfunktion bzw. dem Löschen von personenbezogenen Daten informieren. Meist bieten die Softwarehersteller hier datenschutzadäquate Lösungen, die jedoch noch an das individuelle Unternehmen angepasst werden müssen.

6.4. // LÖSUNGSANSÄTZE FÜR EIN LÖSCH- UND SPERRKONZEPT

Ein solches Konzept legt fest, welche Daten nach der Erledigung einer Forderung noch für den Zweck des Forderungsmanagements bzw. zur Wahrung von Aufbewahrungsfristen benötigt werden und welche Rechtsgrundlage dafür jeweils besteht. Weiterhin ist festzulegen, wann Daten archiviert werden können. Archivierungsfunktionen können so aussehen, dass die Daten nur bei Vorliegen bestimmter Voraussetzungen (z. B. wenn ein Schuldner erneut zum Schuldner wird oder für eine Steuerprüfung) reaktiviert werden können, wie ein internes Verweisungssystem aussieht und welcher Personenkreis nach der Archivierung noch Zugriff hat.

7. // INFORMATIONSPFLICHTEN UND BETROFFENENRECHTE

Nach der DS-GVO darf die Verarbeitung personenbezogener Daten nicht »hinter dem Rücken« des Betroffenen stattfinden. Eine faire und transparente Verarbeitung setzt voraus, dass der Betroffene über die Existenz eines Verarbeitungsvorgangs und dessen Zweck unterrichtet wird.

Informationen nach Art. 13 und 14 dienen der Transparenz

Inkassodienstleister müssen daher als Verantwortliche im Sinne der DS-GVO umfassend informieren, wenn sie Daten verarbeiten. Dabei steht der Schutz der Betroffenen im Mittelpunkt.

Art. 5 Abs. 1 Buchstabe a enthält den Grundsatz der Transparenz. Er muss auch die Belange und Interessen der betroffenen Person berücksichtigen. In Bezug auf die Informationspflichten und Betroffenenrechte muss die betroffene Person jederzeit klar erkennen können, welche ihrer personenbezogenen Daten von wem für welche Zwecke verarbeitet werden.

Betroffene Personen sind grundsätzlich über die Datenerhebung nach (Art. 13 bzw.) Art. 14 Abs. 1 und Abs. 2 zu informieren. Inkassodienstleister müssen aber auch zu einem späteren Zeitpunkt informieren, wenn der Betroffene es entsprechend seinen Rechten aus Art. 15 bis 21 erst später verlangt. Darüber hinaus bestehen ggf. noch Benachrichtigungspflichten nach Art. 33, 34 bei einer »Datenpanne« |10|.

Art. 13–14 DS-GVO

- *Informationen bei Erhebung beim Betroffenen*
- *Benachrichtigung bei Dritterhebung*

Art. 15 DS-GVO

- *Auskunftsrecht (Selbstauskunft)*

Art. 16–22 DS-GVO, v. a.

- *Berichtigung*
- *Löschung*
- *Einschränkung (»Sperrung«)*
- *Datenübertragbarkeit*
- *Widerspruch*

Art. 12 DS-GVO

Modalitäten für die transparente Information, Kommunikation und Ausübung der Rechte der Betroffenen

7.1. // INFORMATIONSPFLICHTEN

DS-GVO-Regelungen

- *Art. 13: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person*
- *Art. 14: Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Dritterhebung)*

BDSG-Regelungen

- *§ 32: Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person*
- *§ 33: Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Dritterhebung)*

|10| Siehe: 9. // Verletzungen des Schutzes personenbezogener Daten, Seite 37.

Die DS-GVO unterscheidet zwischen der Erhebung der Daten bei der betroffenen Person (Art. 13) und der Erhebung von jemand anderem (Art. 14).

Da sich die Zwecke der Datenspeicherung je nach betroffener Personengruppe unterscheiden, erscheint es sinnvoll, die zu erteilenden Informationen personengruppenspezifisch zu gestalten. Für folgende Personengruppen können mit Blick auf die Forderungseinziehung beim Schuldner spezifische Informationen bereitgestellt werden:

- Schuldner
- Dritte/Beteiligte in Forderungsangelegenheiten

Daneben können spezielle Informationen z. B. für Bewerber, Beschäftigte und Mandanten vorgehalten werden, die aber hier nicht weiter behandelt werden.

Bei der Information der betroffenen Person sind Fristen und Formvorschriften zu beachten. Die detaillierten Informationen sind der betroffenen Person, egal ob die betroffene Person ein Interesse an diesen Informationen bekundet hat oder nicht, zur Verfügung zu stellen.

7.1.1. // Informationspflichten gegenüber Schuldnern

Alle Informationen, die dem Schuldner gegeben werden müssen, wenn das Inkassounternehmen direkt von ihm Daten erhält, sind in Art. 13 zu finden. Erhält das Inkassounternehmen die Daten vom Auftraggeber, muss der Schuldner nach Art. 14 informiert werden.

Grundsätzlich erhalten die Inkassodienstleister zu Beginn der Bearbeitung die Informationen über den Schuldner vom Mandanten oder vom Verkäufer der Forderung. Das Inkassounternehmen muss dann als Verantwortlicher seiner Informationspflicht nach (Art. 13 bzw.) Art. 14 nachkommen, und zwar unter Berücksichtigung der spezifischen Umstände der Verarbeitung der Daten innerhalb einer angemessenen Frist nach Erlangung der Daten, längstens jedoch nach Art. 14 Abs. 3 Buchstabe a innerhalb eines Monats. Werden die Daten zur Kommunikation mit der betroffenen Person verwendet, entsteht die Informationspflicht spätestens zum Zeitpunkt der ersten Mitteilung nach Art. 14 Abs. 3 Buchstabe b. Der Zeitpunkt der ersten Mitteilung kann das erste Aufforderungsschreiben sein, aber auch ein Telefonat mit dem Schuldner.

Die Informationspflichten gelten für Inkassofälle, die vom verantwortlichen Inkassodienstleister ab dem 25. Mai 2018 in die Bearbeitung genommen worden sind – unabhängig davon, ob Forderungen vom Inkassodienstleister gekauft oder im Rahmen der Inkassodienstleistung nach § 2 Abs. 2 RDG für einen Mandanten geltend gemacht werden. Sie gilt dagegen nicht für Inkassoaufträge, die vor dem 25. Mai 2018 in die Bearbeitung genommen worden sind.

Bei Übernahme eines neuen Inkassoauftrags werden personenbezogene Daten nicht direkt bei der betroffenen Person erhoben. In diesem Fall muss der Verantwortliche (Inkassounternehmen) nach Art. 14 Abs. 1 und Abs. 2 die weiter unten stehenden Informationen mitteilen. Es bietet sich an, die Informationen zusammen mit dem ersten Aufforderungsschreiben (Hello Letter) zu erteilen.

Art und Umfang der Informationen

Die Informationen, die im Folgenden blau markiert sind, müssen der betroffenen Person unmittelbar zur Verfügung gestellt werden, die anderen genannten Informationen können auch über einen Link zugänglich gemacht werden (»Medienwechsel«) |11|. Die kompletten Informationen können dann etwa über einen Link oder einen QR-Code zu einer Internetseite oder aber durch die Möglichkeit zum Faxabruf oder die Anforderung der Information per Brief zur Verfügung gestellt werden.

- **Name und Kontaktdaten des Verantwortlichen:** Der Verantwortliche, d. h. der Inkassodienstleister, muss seinen Namen und seine Kontaktdaten angeben.
- **Gegebenenfalls Name und Kontaktdaten des Vertreters in der EU:** Gilt ggf. für Namen und Kontaktdaten des Vertreters des Verantwortlichen nach Art. 27, wenn der Verantwortliche selbst nicht in der EU niedergelassen ist.

- **Kontaktdaten des Datenschutzbeauftragten, sofern er bestellt sein muss:** Der Name des Datenschutzbeauftragten sollte nicht mitgeteilt werden. Es reicht eine postalische Angabe oder eine E-Mail-Adresse.

- **Verarbeitungszwecke:** Der Verantwortliche muss über alle Zwecke der Datenverarbeitungen informieren.

- **Rechtsgrundlagen:** Der Verantwortliche muss auch über die Rechtsgrundlagen informieren. Er muss dem Betroffenen damit die konkreten einschlägigen Erlaubnistatbestände aus der DS-GVO und ggf. dem BDSG mitteilen, auf die er seine Datenverarbeitung stützt.

Informationen müssen zum (Groß-)Teil direkt erfolgen. »Medienwechsel« ist aber erlaubt

- **Kategorien personenbezogener Daten:** Der betroffenen Person sind die Datenkategorien mitzuteilen, die zuvor vom Inkassodienstleister für die einzelnen Gruppen der Datenverarbeitungen festzulegen sind (z. B. Stammdaten, Forderungsdaten).

- **Empfänger oder Kategorien von Empfängern:** Betroffene Personen sind grundsätzlich in allen Fällen, in denen personenbezogene Daten übermittelt werden sollen, über die Identität der Empfänger zu informieren. Es genügt zur Information aber bereits die Angabe über Kategorien von Empfängern.

- **Absicht, personenbezogene Daten in ein Drittland zu übermitteln:** Beabsichtigt der Verantwortliche eine Übermittlung personenbezogener Daten in Drittländer (Achtung z. B. bei Serverstandorten in den USA und vielen Cloud-Lösungen), vor allem auch bei einer Abgabe von Forderungen an ausländische Unternehmen in Drittländern, muss er darüber informieren. Der Inkassodienstleister muss dann zusätzlich mitteilen, auf welcher besonderen Bedingung nach Art. 44 ff. die Übermittlung beruht und welche Maßnahmen ergriffen werden, um beim Empfänger ein angemessenes Datenschutzniveau herzustellen. Im Fall der Übermittlung an Drittländer empfiehlt sich aber in jedem Fall eine gesonderte rechtliche Beratung! |12|

Nach Art. 14 Abs. 2 muss der Verantwortliche dem Betroffenen außerdem weitere Informationen mitteilen, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten. Das sind im Detail:

- **Dauer der Speicherung:** Inkassodienstleister müssen möglichst konkret angeben, wie lange personenbezogene Daten gespeichert werden. Wenn das nicht möglich ist, reichen Kriterien für die Festlegung der endgültigen Dauer der Speicherung aus. Auch wenn die Speicherung grundsätzlich an den Zweck gebunden ist, muss der Verantwortliche Fristen vorsehen, innerhalb derer er die Löschung der Daten vornimmt bzw. zumindest die Notwendigkeit der Speicherung überprüft.

- **Berechtigtes Interesse:** Sollte die Verarbeitung personenbezogener Daten zur Wahrung berechtigter Interessen des Verantwortlichen nach Art. 6 Abs. 1 Buchstabe f erforderlich sein, muss das Inkassounternehmen seine konkreten Interessen bzw. die des Mandanten (als »Dritten«) mitteilen.

- **Rechte der betroffenen Person:** Betroffene sind über ihre Rechte gemäß Art. 15 bis 22 zu informieren, vor allem über: Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und die Möglichkeit des Widerspruchs gegen die Verarbeitung.

|11| Einen noch weiterreichenden möglichen Medienwechsel sieht der GDD e.V.: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_7.pdf.

|12| Siehe: 5. // Datenübermittlung an außereuropäische Empfänger, Seite 16.

Achtung

Zur Erfüllung der Informationspflichten muss die betroffene Person (auch) über ihr Widerspruchsrecht informiert werden. Hier ist darauf zu achten, dass dies »getrennt« von den anderen Informationen über die anderen in Art. 14 Abs. 2 Buchstaben c bis e (bzw. Art. 13 Abs. 2 Buchstaben b bis d) aufgeführten Rechte erfolgt, d. h. beispielsweise in einem separaten Absatz.

- **Widerrufbarkeit von Einwilligungen** (hier nur zur Vollständigkeit – für Inkassodienstleister meistens nicht relevant): Basiert eine Verarbeitung auf der Einwilligung der betroffenen Person, ist auf deren Widerrufbarkeit gesondert hinzuweisen. Die entsprechende Informationspflicht ist nur erfüllt, wenn darüber aufgeklärt wird, dass die Einwilligung jederzeit widerrufen werden kann und die Datenverarbeitung bis zum Zeitpunkt des Widerrufs rechtmäßig bleibt.

- **Beschwerderecht bei einer Aufsichtsbehörde:** Die betroffene Person ist darüber aufzuklären, dass sie sich bei einer Aufsichtsbehörde beschweren kann, sofern sie der Ansicht ist, dass die Verarbeitung ihrer personenbezogenen Daten rechtswidrig erfolgt. Angegeben werden sollte auch die regionale bzw. für die Hauptniederlassung des Verantwortlichen zuständige Aufsichtsbehörde.

- **Quelle der personenbezogenen Daten:** Der Verantwortliche muss die betroffene Person über die Quelle informieren, aus der die personenbezogenen Daten stammen, d. h. über die Herkunft der Daten informieren, und ggf. ob sie aus öffentlich zugänglichen Quellen stammen. Inkassodienstleister werden also (hauptsächlich) den Mandanten als Quelle angeben müssen.

- **Automatisierte Entscheidungsfindung** (nur zur Vollständigkeit – für Inkassodienstleister in aller Regel nicht relevant)

Sollte ein erster Kontakt mit dem Schuldner z. B. telefonisch erfolgen und die Informationspflichten noch nicht erfüllt worden sein, wird empfohlen, den Schuldner im Telefonat darüber zu informieren, dass ihm unverzüglich nach dem Telefonat die Informationen nach Art. 14 zugesendet werden oder er diese auf einer Internetseite abrufen kann.

Beispiel: Informationen zur Datenverarbeitung mit der ersten Mitteilung an den Schuldner nach Art. 14

Wie Inkassounternehmen Schuldner DS-GVO-konform informieren können, zeigt folgendes Beispiel. Hierbei handelt es sich um eine Information gemäß Art. 14 Abs. 1 und Abs. 2 an einen Schuldner einer vertraglich entstandenen Forderung. Gegebenenfalls bietet es sich auch an, die Informationen nach Art. 13 und 14 miteinander zu verbinden.

Beispiel: Informationen zur Datenverarbeitung mit der ersten Mitteilung an den Schuldner

Informationen gemäß Art. 14 Datenschutz-Grundverordnung (DS-GVO)

Sehr geehrte Frau Muster,

wir informieren Sie nachstehend gemäß Art. 14 DS-GVO über die Verarbeitung Ihrer Daten.

Name und Kontaktdaten des Verantwortlichen:
Muster Inkasso GmbH, Musterstr. 1, 11111 Musterhausen

Kontaktdaten des Datenschutzbeauftragten:
Sie erreichen den zuständigen Datenschutzbeauftragten unter: Datenschutzbeauftragter der Muster Inkasso GmbH, Musterstr. 1, 11111 Musterhausen, oder unter datenschutz@muster.de

Verarbeitungszwecke:
Die Datenverarbeitung erfolgt zum Zweck der Vertragsabwicklung bzw. Rechtsverfolgung. Weitere von uns verfolgte Zwecke der Datenverarbeitung sind das Forderungsmanagement sowie die Erfüllung von gesetzlichen Aufbewahrungspflichten.

Rechtsgrundlagen:
Die Verarbeitung Ihrer Daten ist nach Art. 6 Abs. 1 Buchstabe b DS-GVO für die Erfüllung eines Vertrags mit dem Gläubiger, somit auch der daraus resultierenden Zahlungsverpflichtung, erforderlich. Darüber hinaus ist die Datenverarbeitung nach Art. 6 Abs. 1 Buchstabe f DS-GVO zur Wahrung unserer berechtigten Interessen bzw. des Gläubigers als Dritten erforderlich. Die berechtigten Interessen bestehen in Zusammenhang mit der Forderung gegen Sie.

Soweit die Verarbeitung zur Erfüllung gesetzlicher (Aufbewahrungs-)Pflichten erfolgt, ist Rechtsgrundlage auch Art. 6 Abs. 1 Buchstabe c DS-GVO.

Datenkategorien und Datenherkunft:
Wir verarbeiten nachfolgende Kategorien von Daten: Stammdaten, Kommunikationsdaten, Vertragsdaten, Forderungsdaten, ggf. Zahlungsinformationen. Die Daten aus den genannten Datenkategorien wurden uns von unserem Auftraggeber, d. h. dem Gläubiger der Forderung, übermittelt.

Empfänger:
Im Rahmen des Inkassoverfahrens werden wir Ihre Daten an unseren Auftraggeber und ggf. an Empfänger folgender Kategorien übermitteln, sofern dies zum Einzug der Forderung erforderlich ist: Abtretungsempfänger, Auskunfteien, Dienstleister, Drittschuldner, Einwohnermeldeämter, Gerichte, Gerichtsvollzieher, Rechtsanwälte.

Dauer der Speicherung:
Personenbezogene Daten werden bis zur vollständigen Erreichung der oben genannten Zwecke verarbeitet. Hierzu gehören auch die gesetzlichen Aufbewahrungspflichten gemäß der Abgabenordnung (AO), des Handelsgesetzbuchs (HGB) und des Umsatzsteuergesetzes (UStG). Bei vollständiger Zweckerreichung werden die Daten gelöscht.

Rechte der betroffenen Person:
Ihnen stehen bei Vorliegen der gesetzlichen Voraussetzungen folgende Rechte nach Art. 15 bis 22 DS-GVO zu: Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung sowie auf Datenübertragbarkeit.

Außerdem steht Ihnen bei Vorliegen der gesetzlichen Voraussetzungen nach Art. 21 DS-GVO ein Widerspruchsrecht gegen die Verarbeitung zu, das auf Art. 6 Abs. 1 Buchstabe f DS-GVO beruht.

Beschwerderecht bei einer Aufsichtsbehörde
Sie haben gemäß Art. 77 DS-GVO das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt. Die für unser Unternehmen zuständige Aufsichtsbehörde ist die … (Die für das Inkassounternehmen regional zuständige Datenschutzaufsichtsbehörde sollte hier genannt werden).

7.1.2. // Informationspflichten gegenüber Dritten

Auch für sonstige am Inkassoverfahren beteiligte Dritte, die eine natürliche Person sind, gelten die Informationspflichten der Art. 13 und 14. Hierzu dürften insbesondere Betreuer und Bevollmächtigte der Schuldner zählen. Zur Vereinfachung der Fragestellung, ob die Informationspflicht im jeweiligen Fall auf Art. 13 oder 14 beruht, bietet es sich an, für diese Dritten eine Datenschutzinformation bereitzustellen, die eine Kombination beider Normen beinhaltet.

Wenn Dritte zu informieren sind, muss dies nur einmal erfolgen. Das heißt, wenn der Dritte in einer anderen Sache schon einmal informiert wurde, muss der Dritte bei Zuordnung zu einem weiteren Vorgang/Schuldner nicht erneut informiert werden.

Die Informationspflicht gegenüber den Dritten kann ggf. mit dem Verweis auf einen Internetlink, unter dem die Information online abrufbar ist, erfüllt werden.

Ausnahmen von der Informationspflicht gegenüber Dritten

In bestimmten Fallkonstellationen kann die Offenlegung der Erhebung personenbezogener Daten nachteilige Folgen (ggf. auch für den Betroffenen) für die Durchsetzung der Forderung haben. Dies gilt z. B. bei Entnahme der Daten des Dritten aus einer Vermögensauskunft oder aus einem Gerichtsvollzieherprotokoll oder aus einer Drittauskunft.

Der Gesetzgeber hat deshalb Ausnahmetatbestände (u. a. § 32 Abs. 1 Ziffer 4 und § 33 Abs. 1 Ziffer 2 a BDSG) normiert, nach denen die Informationen nach Art. 13 und 14 unterbleiben können, wenn durch ihre Erteilung der Erfolg der Forderungseinziehung gefährdet oder gar vereitelt würde. Die Entscheidung der Nichtinformation ist aber im Einzelfall zu dokumentieren.

Gegenüber öffentlichen Stellen – wie beispielsweise Gerichten und Gerichtsvollziehern – dürfte grundsätzlich keine Informationspflicht bestehen.

7.2. // BETROFFENENRECHTE UND WEITERE MITTEILUNGSPFLICHTEN DER VERANTWORTLICHEN

DS-GVO-Regelungen

- *Art. 15: Auskunftsrecht der betroffenen Person*
- *Art. 16: Recht auf Berichtigung*
- *Art. 17: Recht auf Löschung (»Recht auf Vergessenwerden«)*
- *Art. 18: Recht auf Einschränkung der Verarbeitung (»Sperrung«)*
- *Art. 19: Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung*
- *Art. 20: Recht auf Datenübertragbarkeit*
- *Art. 21: Widerspruchsrecht*
- *Art. 22: Automatisierte Entscheidungen im Einzelfall einschließlich Profiling*
- *Art. 33 Abs. 1: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde*
- *Art. 34: Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person*

Umfangreiche Rechte von Betroffenen sind fester Bestandteil im Umgang mit personenbezogenen Daten. Inkassodienstleister treffen damit umfassende Pflichten, z. B. zur Auskunftserteilung, Berichtigung oder auch Löschung von Daten.

Der betroffenen Person stehen nachfolgende Rechte zu:

7.2.1. // Auskunftsrecht

Nach Art. 15 Abs. 1 steht der betroffenen Person ein abgestuftes Auskunftsrecht zu. Zum einen kann die betroffene Person von dem Verantwortlichen eine Bestätigung darüber verlangen, ob bei diesem sie betreffende personenbezogene Daten verarbeitet werden.

Auch eine Negativauskunft ist erforderlich, wenn der Verantwortliche keine Daten zu dieser Person verarbeitet. Im Falle der Negativauskunft werden mit dem Auskunftsersuchen personenbezogene Daten direkt beim Betroffenen erhoben, sollten seine Daten im Weiteren gespeichert werden. Daher besteht hier die Pflicht, die anfragende Person zusammen mit der Negativauskunft nach Art. 13 über die Datenspeicherung der Anfrage und Auskunft zu informieren. Als mögliche Zwecke kommen in Betracht:

- Erfüllung eigener gesetzlicher Informations-, Mitteilungs-, Auskunfts-, Aufbewahrungs- und sonstiger Pflichten
- Erfüllung eigener Identifizierungspflichten
- Abwehr von Sanktionen nach der DS-GVO und Schadensersatzansprüchen

Beispiel: Negativauskunft nach Art. 15

Wie Inkassounternehmen anfragende Personen künftig DS-GVO-konform beauskunften können, wenn diese dem Unternehmen bislang unbekannt waren, zeigt folgendes Beispiel.

Beispiel: Negativauskunft nach Art. 15

Auskunft gemäß Art. 15 Datenschutz-Grundverordnung (DS-GVO)

Sehr geehrte(r) Frau/Herr… (anfragende Person einsetzen),

um Ihrem Auskunftsantrag Genüge zu tun, teilen wir Ihnen mit, dass Sie uns bis zu Ihrer Anfrage per E-Mail am … gänzlich unbekannt waren.

Die im Rahmen des Auskunftsersuchens übermittelten Daten werden ausschließlich zum Zweck der Erteilung und des Nachweises der Auskunftserteilung gespeichert und werden nach Eintritt der Verfolgungsverjährung gelöscht.

Mit freundlichen Grüßen

Identitätsprüfung

Es muss sichergestellt werden, dass die zu beauskunftenden Daten nicht unbefugten Dritten zur Verfügung gestellt werden. Hierauf ist auch insbesondere bei mündlicher oder elektronischer Auskunftserteilung zu achten. Hat der Verantwortliche begründete Zweifel an der Identität eines Anfragenden, so kann er nach Art. 12 Abs. 6 zusätzliche Informationen zur Bestätigung der Identität nachfordern (z. B. eine Postadresse bei elektronischem Auskunftsantrag, ein Geburtsdatum, ein Aktenzeichen).

Normalerweise muss zur Identifizierung keine Ausweiskopie vom Betroffenen verlangt werden. Nur wenn gravierende Zweifel an der Identität des Anfragenden bestehen, kann eine Ausweiskopie zur Identifizierung angefordert werden. Der Betroffene ist dann aber darauf hinzuweisen, dass er alle nicht erforderlichen Angaben schwärzt bzw. unkenntlich macht. |13| Anderenfalls riskiert der Inkassodienstleister, rechtswidrig personenbezogene Daten offenzulegen.

|13| Hilfreich ist das Dokument »Personalausweis und Datenschutz« der LDI NRW, Stand: Juli 2019, abrufbar unter: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Personalausweis-und-Datenschutz/Datenschutz-und-Personalausweis-2019_07.pdf.

Wurde die Kopie des Personalausweises dem Inkassodienstleister zur Identifizierung übersandt, muss diese nach erfolgter Identifizierung gelöscht werden.

Form der Auskunftserteilung

Die Auskunftserteilung an die betroffene Person kann nach Art. 12 Abs. 1 Sätze 2 und 3 je nach Sachverhalt schriftlich, elektronisch oder – auf Wunsch der betroffenen Person – mündlich erfolgen. Als datenschutzfreundlichste Gestaltung gilt ein vom Verantwortlichen eingerichteter Fernzugriff, der der betroffenen Person Zugriff auf ihre eigenen Daten ermöglicht. Sofern ein solcher gesicherter Fernzugriff nicht angeboten werden kann, wird grundsätzlich eine Antwort per Post empfohlen. Dann ist die Gefahr minimiert, dass eine falsche Person die Auskunft erhält. Darüber hinaus ist dieser Transportweg vergleichsweise sicher.

Frist für die Auskunftserteilung

Auskunftserteilungen müssen gemäß Art. 12 Abs. 3 unverzüglich erfolgen, spätestens aber innerhalb eines Monats; nur in begründeten Ausnahmefällen kann die Monatsfrist um weitere zwei Monate überschritten werden, worüber die betroffene Person zu informieren ist (Art. 12 Abs. 3 Satz 3).

Grenzen des Auskunftsrechts

Auskünfte sind grundsätzlich kostenfrei zu erteilen. Offenkundig unbegründete oder exzessive Anträge einer betroffenen Person können zur Ablehnung oder zu einer Kostenerstattungspflicht führen (Art. 12 Abs. 5 Satz 2). Die betroffene Person muss jedoch ihr Recht in angemessenen Abständen wahrnehmen können.

Inhalt der Auskunft

Neben den über die Maske einer Inkassosoftware gespeicherten bzw. erfassten Daten sind bei der Datenauskunft vor allem noch folgende Informationen mitzuteilen:

- Verarbeitungszwecke
- Kategorien personenbezogener Daten, die verarbeitet werden
- Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig noch erhalten werden
- geplante Speicherdauer falls möglich, andernfalls die Kriterien für die Festlegung der Speicherdauer
- Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung
- Widerspruchsrecht gegen diese Verarbeitung nach Art. 21
- Beschwerderecht für die betroffene Person bei einer Aufsichtsbehörde
- Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden

Wenn eine Verarbeitung gemäß Art. 22 erfolgt, ist auch der folgende Punkt zu berücksichtigen:

- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling mit aussagekräftigen Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren

Beispiel: Positivauskunft nach Art. 15

Wie Inkassounternehmen betroffene Personen künftig DS-GVO-konform beauskunften können, wenn diese bei dem Unternehmen bezüglich einer Forderungseinzugsangelegenheit bekannt sind, zeigt folgendes Beispiel.

Beispiel: Positivauskunft nach Art. 15

Auskunft gemäß Art. 15 Datenschutz-Grundverordnung (DS-GVO)

Sehr geehrte(r) Frau/Herr… (betroffene Person einsetzen),

hiermit erteilen wir Ihnen entsprechend Ihrer Anfrage gemäß Art. 15 Abs. 1 der Datenschutz-Grundverordnung (DS-GVO) entsprechende Auskunft.

Unser Unternehmen verarbeitet Daten zu Ihrer Person.

Verarbeitungszwecke:
Die Datenverarbeitung erfolgt zum Zweck der Vertragsabwicklung bzw. Rechtsverfolgung. Weitere von uns verfolgte Zwecke der Datenverarbeitung sind das Forderungsmanagement sowie die Erfüllung von gesetzlichen Aufbewahrungspflichten.

Datenkategorien:
Wir verarbeiten nachfolgende Kategorien von Daten: Stammdaten, Kommunikationsdaten, Vertragsdaten, Forderungsdaten, ggf. Zahlungsinformationen.

Empfänger, denen personenbezogene Daten offengelegt wurden bzw. werden:

Auftraggeber:	*Muster GmbH, Musterstr. 0, 00000 Musterstadt*
Dienstleister:	*xy GmbH*
Wirtschaftsauskunfteien:	*1.) 123 Wirtschaftsauskunftei GmbH*
	2.) Wirtschaftsauskunftei für Alle AG

Dauer der Speicherung:
Personenbezogene Daten werden bis zur vollständigen Erreichung der oben genannten Zwecke verarbeitet. Hierzu gehören auch die gesetzlichen Aufbewahrungspflichten gemäß der Abgabenordnung (AO), des Handelsgesetzbuchs (HGB) und des Umsatzsteuergesetzes (UStG). Bei vollständiger Zweckerreichung werden die Daten gelöscht.

Ihre Rechte:
Ihnen stehen bei Vorliegen der gesetzlichen Voraussetzungen folgende Rechte zu: Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung.

Außerdem steht Ihnen ein Widerspruchsrecht gegen die Verarbeitung, das auf Art. 6 Abs. 1 Buchstabe f DS-GVO beruht, zu.

Beschwerderecht bei einer Datenschutzaufsichtsbehörde:
Sie haben das Recht, sich bei einer Datenschutzaufsichtsbehörde zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt. Die für unser Unternehmen zuständige Aufsichtsbehörde ist die … (Die für das Inkassounternehmen regional zuständige Datenschutzaufsichtsbehörde sollte hier genannt werden).

Datenherkunft:
Wir erhielten Sie betreffende personenbezogene Daten von folgenden Personen/Unternehmen.

Auftraggeber:	*Muster GmbH, Musterstr. 0, 00000 Musterstadt*
Adressdienstleister:	*Adressdienstleister xy GmbH*

Auskunfteien:	*1.) 123 Wirtschaftsauskunftei GmbH* *2.) Wirtschaftsauskunftei für Alle AG*	
Sonstige:	*xxx*	

Vom Auftraggeber haben wir bei Übergabe der Forderung an unser Unternehmen folgende Daten zur Erfüllung unserer Verarbeitungszwecke erhalten:

		Datenherkunft
Ursprungsgeschäfts-/ Kundennummer:	*123456789*	*Auftraggeber*
Rechnungs-/ Mandantenabrechnungs-Nr.:	*987654321*	*Auftraggeber*
Ursprungsgeschäftsart:	*Kaufvertrag*	*Auftraggeber*
Ursprungsgeschäftsdatum:	*17.09.2014*	*Auftraggeber*
Forderungsgrund:	*Forderung aus Kaufvertrag:*	*123456789*

Zudem verarbeiten wir seitdem folgende personenbezogene Daten von Ihnen:

		Datenherkunft
Inkasso-Nr.:	*00000000000 X 101*	*Inkassogesellschaft 123*
Anrede:	*Frau*	*Auftraggeber*
Name, Vorname:	*Muster, Maria*	*Auftraggeber*
Geburtsname:	*Mustermann*	*Auskunftei zu 1.)*
Geburtsdatum:	*04.02.1975*	*Auftraggeber*
Straße, Haus-Nr.:	*Mustergasse 7*	*Adressdienstleister*
PLZ, Wohnort:	*00000 Musterhausen*	*Adressdienstleister*
Voranschriften:	*Musterallee 80, 00000 Musterdorf*	*Betroffene Person*
	Musterstr. 1, 00000 Musterdorf	*Adressdienstleister*
	Musterstr. 16, 00000 Musterdorf	*Auftraggeber*
	Musterstr. 2, 00000 Musterdorf	*Adressdienstleister*
	Musterstr. 28, 00000 Musterdorf	*Auskunftei zu 2.)*
	Musterstr. 99, 00000 Musterdorf	*Auftraggeber*
Telefon:	*0123 0000-0000*	*Betroffene Person*
	0987 0000-0	*Öffentliches Telefonverzeichnis*
E-Mail:	*Muster@Muster.com*	*Betroffene Person*
Bankverbindung:	*DE72000000000000000*	*Vermögensauskunft*
Titel:	*Vollstreckungsbescheid vom 03.06.2015*	
	Az: 77 BI 123456/15, AG Musterhausen	*Gericht*
Negativmerkmale:	*Vermögensauskunft 01.01.2017*	*Auskunftei zu 1.)*
Arbeitgeber:	*Fix und Foxi GmbH Vermögensauskunft Auf dem Muster 3, 00000 Musterland*	

Aktueller Forderungsstand inkl. Zinsen beträgt:	*X €*

Zudem verarbeiten wir personenbezogene Daten von Ihnen, die Sie uns im Rahmen der Kommunikation mit uns mitgeteilt haben.

Wir hoffen Ihnen hiermit weitergeholfen zu haben und stehen für weitere Fragen und/oder Auskünfte auch gerne weiterhin zur Verfügung.

Mit freundlichen Grüßen

7.2.2. // Recht auf Berichtigung und Recht auf Löschung

Der Grundsatz der Richtigkeit nach Art. 5 Abs. 1 Buchstabe d bedeutet: Inkassounternehmen müssen dafür sorgen, dass falsche Daten entweder berichtigt (Art. 16) oder gelöscht (Art. 17) werden.

Aus dem Grundsatz in Art. 5 Abs. 1 Buchstabe e (»Speicherbegrenzung«) ergibt sich, dass das Inkassounternehmen jedes personenbezogene Datum zu einem bestimmten Zeitpunkt löschen muss – nämlich dann, wenn die weitere Speicherung nicht mehr erforderlich ist. |14|

Diese Erforderlichkeit muss für jede Art bzw. Kategorie personenbezogener Daten vom Inkassounternehmen im Vorfeld im Rahmen eines Sperr- und Löschkonzepts festgelegt und umgesetzt werden. Solange ein Zweck zur Datenverarbeitung vorhanden ist (z. B. zur Erfüllung der Aufbewahrungspflichten), braucht einem Löschgesuch nicht nachgekommen zu werden.

7.2.3. // Recht auf Einschränkung der Verarbeitung (»Sperrung«)

Nach Art. 18 hat der Betroffene das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung (Sperrung) zu verlangen, wenn vor allem eine der folgenden Voraussetzungen gegeben ist:

- Die Richtigkeit der personenbezogenen Daten wird vom Betroffenen bestritten, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der Daten zu überprüfen.
- Der Betroffene hat Widerspruch gegen die Verarbeitung eingelegt, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen des Betroffenen überwiegen.

7.2.4. // Recht auf Datenübertragbarkeit

Die betroffene Person kann verlangen – wenn die Verarbeitung z. B. auf Art. 6 Abs. 1 Buchstabe b beruht und zur Erfüllung eines Vertrags erforderlich ist –, dass sie ihre personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format erhält. Zudem hat sie das Recht darauf, dass der Verantwortliche diese Daten einem anderen Verantwortlichen übermittelt.

Hintergrund der Vorschrift ist, einer betroffenen Person einen leichteren Wechsel zwischen den Anbietern von sozialen Netzwerken, E-Mail- und anderen Cloud-Diensten zu ermöglichen.

Es ist davon auszugehen, dass diese Regelung für das Inkassoverfahren gegen einen Schuldner von keiner Bedeutung ist, da dieser nur selten die personenbezogenen Daten dem Inkassodienstleister direkt bereitstellt. Dieser erhält die Daten meist vom Auftraggeber oder aus anderen Quellen.

Das Merkmal »Bereitstellen von Daten« in Art. 20 ist gemäß seinem Wortlaut und in der Zusammenschau mit Art. 15 so zu verstehen, dass es sich dabei nur um die Daten handeln kann, die die betroffene Person selbst dem Verantwortlichen zur Verfügung gestellt hat. Würde der Begriff des »Bereitstellens« ausgeweitet werden bzw. angenommen, dass im Fall, dass der betroffenen Person ein Recht auf Datenübertragbarkeit nach Art. 20 bezüglich aller sie betreffenden, beim Verantwortlichen verarbeiteten personenbezogener Daten zusteht, wenn sie ggf. auch nur ein personenbezogenes Datum selbst direkt übermittelt hat, würde es zu einer Überschneidung mit Art. 15, dem Auskunftsrecht der betroffenen Person, kommen.

|14| Siehe: 6. // Löschung von personenbezogenen Daten, Seite 18.

Art. 15 sieht hingegen keine Übermittlung der Auskunft in einem »strukturierten, gängigen und maschinenlesbaren Format« vor. Aus diesem Grund kann ein weit verstandener Begriff des »Bereitstellens von Daten« nicht tragen.

Damit, dass dem Forderungsschuldner als betroffener Person seine dem Verantwortlichen selbst zur Verfügung gestellten Daten nur über die Auskunft nach Art. 15 zur Verfügung gestellt werden und nicht über Art. 20, ist auch keine Senkung des Schutzes der betroffenen Person verbunden.

7.2.5. // Widerspruchsrecht

Die betroffene Person besitzt zwar ein Recht auf Widerspruch gegen die Datenverarbeitung. Das gilt aber nur, wenn die jeweilige Datenverarbeitung auf Art. 6 Abs. 1 Buchstabe f als Rechtsgrundlage beruht. Dem Widerspruch muss nicht nachgekommen werden, wenn die Verarbeitung mit der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen begründet werden kann. Widersprüche gegen Datenverarbeitungen des Inkassodienstleisters dürften damit häufig ins Leere laufen.

7.2.6. // Automatisierte Entscheidungsfindung einschließlich Profiling

Nach Art. 22 hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden. Inkassounternehmen treffen grundsätzlich aber keine Entscheidungen, die die Rechtsposition einer betroffenen Person in irgendeiner Weise verändern, und zwar dergestalt, dass ein Recht oder ein Rechtsverhältnis begründet oder aufgehoben oder dass in ein Recht eingegriffen wird, sodass Art. 22 grundsätzlich nicht für den Inkassodienstleister maßgeblich ist.

7.2.7. // Ergänzende Mitteilungspflichten des Inkassodienstleisters

Gegebenenfalls bestehen weitere Pflichten der Inkassodienstleister als Verantwortliche:

Im Fall der Berichtigung, Löschung oder Einschränkung (»Sperrung«): Der Inkassodienstleister hat eine Pflicht zur Mitteilung über jede Berichtigung, Löschung oder Einschränkung an alle Empfänger, denen er personenbezogene Daten offengelegt hat. Zudem muss er der betroffenen Person die Empfänger mitteilen, wenn diese das verlangt (Art. 19).

Inkassodienstleister müssen Benachrichtigungspflichten, z. B. im Fall einer »Datenpanne«, beachten und teilweise innerhalb von 72 Stunden reagieren!

Meldung an die Aufsichtsbehörde bei »Datenpannen«: Der Inkassodienstleister ist im Falle einer »Datenpanne« verpflichtet, die Aufsichtsbehörde innerhalb von 72 Stunden (!) ab Bekanntwerden der Datenschutzverletzung zu benachrichtigen (Art. 33 |15|).

Im Verletzungsfall mit einem hohen Risiko für den Betroffenen: Das Inkassounternehmen trifft zudem die Pflicht zur Benachrichtigung der betroffenen Person im Fall der Verletzung des Schutzes personenbezogener Daten, sprich bei einer »Datenpanne« (Art. 34), soweit ein »hohes Risiko« für die persönlichen Rechte und Freiheiten natürlicher Personen vorliegt.

8. // UMFANGREICHE DOKUMENTATIONSPFLICHTEN

DS-GVO-Regelungen
- *Art. 5 Abs. 2: »Rechenschaftspflicht«*
- *Art. 30: Verzeichnis von Verarbeitungstätigkeiten*

Die Dokumentationspflichten lassen sich knapp zusammenfassen: Alles, was mit personenbezogenen Daten zu tun hat, muss dokumentiert werden.

Eine genaue und aktuelle Dokumentation der Datenverarbeitungen ist das A und O

Die Dokumentationspflichten der DS-GVO haben ihre Grundlage in der Rechenschaftspflicht in Art. 5 Abs. 2. Jeder Verantwortliche, somit auch der Inkassodienstleister, muss die DS-GVO-Vorgaben und -Grundsätze einhalten und sie (stets auf aktuellem Stand) nachweisen können. Die Dokumentation muss für jeden verständlich und nachvollziehbar sein.

Sofern nicht bereits schon erstellt (unter dem alten BDSG unter dem Stichwort »Verfahrensverzeichnis« bekannt), hat der Verantwortliche ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen, in dem die Anforderungen nach Art. 30 Abs. 1 berücksichtigt sein müssen.

Übrigens: Auch für Inkassounternehmen tätige Auftragsverarbeiter stehen nun, anders als vor der Einführung der DS-GVO, in der Pflicht, ein solches Verzeichnis zu führen und ihre Kunden dort mit aufzuführen. Die Anforderungen für die Auftragsverarbeiter ergeben sich auch Art. 30 Abs. 2.

Ein Nichtvorhandensein des Verzeichnisses ist bußgeldbewehrt.

Die DS-GVO sieht in vielen Regelungen eine Dokumentations- und Rechenschaftspflicht vor.

Die wichtigsten entsprechenden Pflichten ergeben sich aus den folgenden Vorschriften:

- Rechtmäßigkeit der Verarbeitung (Art. 6)
- Betroffenenrechte (Art. 13, 14, 15)
- Verzeichnis von Verarbeitungstätigkeiten (Art. 30)
- Sicherheit der Verarbeitung (Art. 32)
- Meldungen von Verletzungen des Schutzes von personenbezogenen Daten (Art. 33 »Datenpanne«)
- Datenschutz-Folgenabschätzung (Art. 35)

8.1. // EINZELNE DOKUMENTATIONSPFLICHTEN

8.1.1. // Informationen gemäß Art. 13 bis Art. 15

Es muss vor allem alles dokumentiert werden, worüber eine betroffene Person im Rahmen der Art. 13 bis Art. 15 informiert werden muss. |16|

Auf dieser Grundlage muss vor allem Folgendes beschrieben und dokumentiert werden:

- Kategorien der betroffenen Personen (z. B. Schuldner, Gläubiger, Auftraggeber, Dritte, Mitarbeiter)
- Zwecke, für die die Daten (weiter-)verarbeitet werden

|15| Siehe: 7. // Informationspflichten und Betroffenenrechte, Seite 21.
|16| Siehe: 7. // Informationspflichten und Betroffenenrechte, Seite 21.

- Rechtsgrundlage(n) für die Verarbeitung
- ggf. berechtigte Interessen in Bezug auf die Datenverarbeitung
- Datenkategorien
- Empfängerkategorien
- Herkunft der personenbezogenen Daten
- Zudem sollte unbedingt ein Berichtigungs-/Löschkonzept vorliegen, das auch Fristen für die regelmäßige Überprüfung von Speicherfristen vorsieht. |17|

8.1.2. // Technische und organisatorische Maßnahmen

Um ein angemessenes Schutzniveau gegenüber der Aufsichtsbehörde nachweisen zu können, müssen zudem die technisch-organisatorischen Maßnahmen |18| genau beschrieben werden.

8.1.3. // Dokumentation bei der Verletzung des Schutzes personenbezogener Daten

Art. 33 schreibt ggf. eine Meldung vor, die ein Verantwortlicher gegenüber der Aufsichtsbehörde bei Verletzung des Schutzes personenbezogener Daten bzw. »Datenpannen« abgeben muss. |19| Unabhängig hiervon muss die Verletzung personenbezogener Daten stets dokumentiert werden (zu den Einzelheiten vgl. Art. 33 Abs. 5).

8.1.4. // Weisungen des Verantwortlichen

Alle Weisungen des Verantwortlichen sind zu dokumentieren. Dies betrifft Weisungen, die der Verantwortliche den ihm unterstellten Personen gibt (Art. 29), dazu gehören z. B. Arbeitsanweisungen, ggf. auch Mitarbeiterschulungen in Bezug auf die DS-GVO. Ebenso betrifft dies die Weisungen, die eine Verarbeitung beim Auftragnehmer im Rahmen eines Auftragsverarbeitungsverhältnisses (Art. 28) betreffen.

8.1.5. // Dokumentation geeigneter Garantien bei Übermittlungen in ein Drittland

Sofern personenbezogene Daten in ein Drittland übermittelt oder übergeben werden, in dem kein gleichwertiges Datenschutzniveau wie das in der Europäischen Union bzw. dem EWR oder gleichgestellten Ländern herrscht, sieht die DS-GVO eine entsprechende (erweiterte) Dokumentationspflicht vor (Art. 46 f.).

8.1.6. // Dokumentation einer Datenschutz-Folgenabschätzung

Im Fall, dass der Inkassodienstleister eine nach Art. 35 geforderte Datenschutz-Folgenabschätzung durchführen muss, |20| muss er auch eine dementsprechende Dokumentation vorweisen können. Aus dieser Dokumentation müssen die Risiken einzelner Verarbeitungsschritte hervorgehen und die Maßnahmen, die getroffen wurden, damit diese reduziert werden. |21|

8.1.7. // Dokumentation von Verarbeitungstätigkeiten

Für jeden Prozess im Unternehmen, in dem personenbezogene Daten von natürlichen Personen (z. B. von Schuldnern, Mandanten, aber auch Mitarbeitern) verarbeitet werden, muss die Verarbeitungstätigkeit dokumentiert werden.

Hilfreich könnte im Forderungsmanagement sein, vor allem auch zur Erstellung des Verzeichnisses für Verarbeitungstätigkeiten, den Ablauf eines Forderungskontos vom Zugang bis hin zur Beendigung zu prüfen und den Verlauf in mehrere logische Verarbeitungsabschnitte zu gliedern: z. B. Übernahme in die Inkassosoftware, Datenanreicherung, Zahlungsaufforderungen/Mahnungen, Anfragen bei Auskunfteien, Einmeldung bei Auskunf-

teien, Adressermittlung etc. bis hin zur Löschung der Daten. Daraus ergibt sich dann die Prozess- und ggf. auch Systembeschreibung.

Tipp

Folgende Fragen könnten dabei zur Gestaltung der jeweiligen Dokumentation/der jeweiligen Verarbeitungstätigkeit gestellt werden – entsprechend den Vorgaben aus Art. 13 bis Art. 15:

- *Wer ist für die Verarbeitung verantwortlich?*
- *Was ist der Grund (Zweck) für die Verarbeitung?*
- *Welche Daten werden verarbeitet?*
- *Woher kommen die Daten?*
- *Wie werden die Daten verarbeitet (Prozess- und Systembeschreibung sowie organisatorische Regelungen)?*
- *Wie lange werden die personenbezogenen Daten gespeichert (Sperr- und Löschkonzept)?*
- *Wer verarbeitet die Daten (interne Berechtigungskonzepte, ggf. auch Dienstleister/Auftragsverarbeiter, die dann die jeweilige Dokumentation liefern müssen)?*
- *An wen werden die Daten weitergegeben, wer erhält auf sie Zugriff?*
- *Welche Systeme und ggf. Übertragungswege werden für die Verarbeitung verwendet?*

8.2. // VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Das in Art. 30 beschriebene Verzeichnis über die Verarbeitungstätigkeiten beschreibt die in Unternehmen eingesetzten Prozesse (»Verfahren«), in denen personenbezogene Daten zu bestimmten Zwecken verarbeitet werden. Im günstigen Falle können Unternehmen dieses Verzeichnis aus vorliegenden Dokumentationen (Prozessschaubildern, Prozessbeschreibungen, Datenmodellen) erstellen. Das Verzeichnis ist auch eine gute Grundlage, um die Informationen nach Art. 13 bzw. 14 sowie die Auskünfte nach Art. 15 vorzubereiten.

8.2.1. // Notwendigkeit der Erstellung eines Verzeichnisses

Die geforderte Führung eines Verzeichnisses der Verarbeitungstätigkeiten war bereits unter dem alten BDSG als Führung eines »Verfahrensverzeichnisses« bekannt und stellt eine der wichtigsten Dokumentationspflichten der DS-GVO dar. Sie trifft sowohl den Verantwortlichen als auch den Auftragsverarbeiter. |22|

8.2.2. // Form des Verzeichnisses

Das Verzeichnis von Verarbeitungstätigkeiten ist schriftlich zu erstellen, worunter auch ein elektronisches Format fällt. Das Verzeichnis muss stets aktuell gehalten werden. Das ergibt sich aus dem Grundsatz der Richtigkeit nach Art. 5 Abs. 1 Buchstabe d.

|17| Siehe: 6. // Löschen von personenbezogenen Daten, Seite 18.

|18| Siehe: 10. // Sicherer Umgang mit personenbezogenen Daten durch technisch-organisatorische Maßnahmen (TOM), Seite 40.

|19| Siehe: 7. // Informationspflichten und Betroffenenrechte, Seite 21.

|20| Siehe: 11. // Datenschutz-Folgenabschätzung, Seite 43.

|21| Siehe: 11. // Datenschutz-Folgenabschätzung, Seite 43.

|22| Zu den Anforderungen an das Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters vgl. 14. // Auftragsverarbeitung, Seite 50.

8.2.3. // Prüfung durch die Aufsichtsbehörde

Das Verzeichnis von Verarbeitungstätigkeiten ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Ein Verzeichnis für »jedermann«, wie es im alten BDSG vorgesehen war, gibt es nicht mehr.

8.2.4. // Inhalt des Verzeichnisses

Zu dokumentieren sind alle Geschäftsprozesse (»Verarbeitungstätigkeiten«, früher auch »Verfahren«), in denen personenbezogene Daten vom Inkassounternehmen als Verantwortlichem verarbeitet werden.

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 Abs. 1 DS-GVO)

Wer führt das Verzeichnis?	Verantwortlicher, d. h. der Inkassodienstleister
Wem wird es zur Verfügung gestellt?	Aufsichtsbehörde
Welche Angaben müssen enthalten sein?	a / Name und Kontaktdaten des Verantwortlichen, ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen Name und Kontaktdaten eines etwaigen Datenschutzbeauftragten b / die Zwecke der Verarbeitung c / Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten d / die Kategorien von Empfängern, einschließlich Empfänger in Drittländern e / ggf. Übermittlungen an ein Drittland, bei Art. 49 Abs. 1 und Abs. 2 Beschreibung geeigneter Garantien f / wenn möglich, Fristen für die Löschung der verschiedenen Datenkategorien g / wenn möglich, eine allgemeine Beschreibung der technisch-organisatorischen Maßnahmen nach Art. 32 Abs. 1

Tipp

Für jeden Prozess sollte eine eigene Übersicht mit den Informationen aus Art. 30 Abs. 1 i. V. m. Art. 13 bis Art. 15 erstellt werden (auch z. B. inkl. der jeweiligen Rechtsgrundlagen). Die von Art. 30 Abs. 1 geforderten Informationen aus jeder Übersicht sollten dann in dem Verzeichnis für Verarbeitungstätigkeiten zusammen aufgeführt werden.

Gute Hilfestellungen kann man auch online abrufen. |23|

9. // VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN

9.1. // BEGRIFF

Verletzungen des Schutzes personenbezogener Daten können umgangssprachlich als »Datenpanne« bezeichnet werden. Unter einer solchen »Datenpanne« versteht man grundsätzlich den fehlerhaften Umgang mit personenbezogenen Daten. Der Begriff »Datenpanne« umfasst folgende Verletzungssituationen (Art. 4 Nr. 12):

- Vernichtung
- Verlust
- Veränderung
- unbefugte Offenlegung/Weitergabe
- unbefugter Zugang

Im Unternehmen müssen für den Fall der »Datenpanne« Prozesse etabliert und diese dokumentiert hinterlegt werden.

Beispiele

- *Übermittlung falscher Adressdaten*
- *Löschung von Datenbeständen durch unbefugte Personen*
- *Hackerangriffe*
- *Diebstahl oder Verlust von Datenträgern (z. B. Laptop, USB-Stick, Festplatte) usw.*

9.2. // AUSLÖSUNG DER MELDEPFLICHT

Eine »Datenpanne« ist der Datenschutzaufsichtsbehörde zu melden, wenn die Verletzung voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 Abs. 1 Satz 1). Führt die Verletzung voraussichtlich zu einem hohen Risiko für deren Rechte und Freiheiten, ist darüber hinaus der Betroffene zu benachrichtigen (Art. 34 Abs. 1).

Die Datenschutzbehörden haben auf der Basis der Erwägungsgründe (EG) 75 und 94 Satz 2 den Risikobegriff wie folgt definiert:

»Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.« |24|

Zu den Risiken für die Rechte und Freiheiten natürlicher Personen gehören entsprechend dem Wortlaut des EG 75 alle drohenden physischen, materiellen oder immateriellen Schäden. Hierzu zählen etwa:

- Verlust der Kontrolle über die personenbezogenen Daten
- Einschränkung der Rechte der betroffenen Person
- Diskriminierung

|23| Zum Beispiel Kurzpapier Nr. 1 der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK): https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_1.pdf und GDD-Praxishilfe DS-GVO V: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf.

|24| Kurzpapier Nr. 18 der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK): https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

- Identitätsdiebstahl oder -betrug
- finanzielle Verluste
- Rufschädigung
- wirtschaftliche oder gesellschaftliche Nachteile etc.

9.3. // RISIKOBEURTEILUNG

Derjenige, der die Daten verarbeitet, muss im Fall einer »Datenpanne« im Wege einer Risikoprognose bestimmen, ob ein Risiko und welches für die Rechte und Freiheiten natürlicher Personen besteht. Es ist unerlässlich, dass Unternehmen für diesen Fall feste Prüfungs- und Bewertungsabläufe einführen, um bestehende Meldepflichten erkennen und umsetzen zu können.

Die Risikobeurteilung im Fall einer »Datenpanne« sollte so ablaufen:

Phase 1: Risikoidentifikation

- Welche Schäden können für die Personen auf der Grundlage der zu verarbeitenden Daten entstehen?
- Durch welche Ereignisse kann es zu dem Schaden kommen?
- Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?

Phase 2: Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden

- Sowohl für die Eintrittswahrscheinlichkeit als auch für die Schwere möglicher Schäden können z. B. jeweils folgende Abstufungen verwendet werden:
  - geringfügig
  - überschaubar
  - wahrscheinlich
  - hoch/groß

Phase 3: Risikoabstufung

- Nachdem die möglichen Schäden, deren Ursachen und die Wahrscheinlichkeit des Schadenseintritts sowie die Schwere möglicher Schäden bestimmt worden sind, können diese den folgenden Risikoabstufungen zugeordnet werden:
  - geringes Risiko
  - Risiko
  - hohes Risiko

Falsche Datenübermittlung bei der Adressermittlung

Werden z. B. von einem Adressdienstleister falsche Daten übermittelt mit der Folge, dass eine falsche Person angeschrieben wird, und wird vom Inkassounternehmen sonst nichts veranlasst (z. B. eine Einmeldung bei einer Auskunftei), besteht aus unserer Sicht kein Risiko für die Rechte und Freiheiten natürlicher Personen, wenn der Fehler vermerkt wird und die Daten gelöscht werden. Die Person wird somit nicht mehr kontaktiert, die Daten nicht mehr genutzt und damit das Risiko beseitigt.

9.4. // MELDEPFLICHT UND DOKUMENTATION

Im Fall der Feststellung eines voraussichtlichen Risikos für die Rechte und Freiheiten natürlicher Personen muss die Verletzung binnen 72 Stunden ab Kenntnis der Verletzung der

Aufsichtsbehörde gemeldet werden (Art. 33 Abs. 1 Satz 1). Erfolgt die Meldung später, ist ihr eine Begründung für die Verzögerung beizulegen (Art. 33 Abs. 1 Satz 2).

Besteht ein hohes Risiko, muss ferner die betroffene Person unverzüglich, d. h. ohne schuldhaftes Zögern, von der Verletzung informiert werden (Art. 34 Abs. 1).

Jede Datenschutzverletzung muss, unabhängig vom Ergebnis der Risikoanalyse, inkl. der Risikobeurteilung, dokumentiert werden. Damit kann das datenverarbeitende Unternehmen der Aufsichtsbehörde die Durchführung der Risikobeurteilung und die Einhaltung eventueller Meldepflichten nachweisen.

Tipp

Inkassounternehmen sollten außerdem Prozesse einführen (und diese auch in Arbeitsanweisungen und Richtlinien dokumentieren), damit im Fall von »Datenpannen« schnell gegenüber der Aufsichtsbehörde eine Meldung erfolgen und ggf. der Betroffene (Art. 34) informiert werden kann. Stellen Sie sicher, dass Ihre Mitarbeiter davon in Kenntnis gesetzt werden, z. B. in den Datenschutzschulungen oder durch Kenntnisnahme, dass sie die Arbeitsanweisung gelesen und verstanden haben.

Achten Sie darauf, auch mit Auftragsverarbeitern eine entsprechende Vereinbarung zu treffen, damit diese im Fall einer »Datenpanne« schnellstmöglich diese anzeigen und Sie etwaige Schäden von der betroffenen Person zügig gänzlich abwenden bzw. diese minimal halten können.

9.5. // MASSNAHMEN ZUR ABWENDUNG BZW. EINDÄMMUNG DES RISIKOS

Wenn eine »Datenpanne« aufgetreten ist, müssen Maßnahmen ergriffen werden, die in Zukunft verhindern sollen, dass eine weitere »Datenpanne« dieser Art auftritt. Die technischen und organisatorischen Anpassungen, die vorgenommen werden, um weitere »Datenpannen« zu verhindern (»Abhilfemaßnahmen«), müssen dokumentiert werden.

9.6. // INHALT DER MELDUNG

Die Benachrichtigung an den Betroffenen muss gemäß Art. 34 Abs. 2 i. V. m. Art. 33 Abs. 3 zumindest folgende Informationen enthalten:

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen der »Datenpanne«
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der »Datenpanne«, ggf. eine Beschreibung der Maßnahmen, die zur Abmilderung der möglichen nachteiligen Auswirkungen der »Datenpanne« ergriffen wurden

Die Meldung an die Aufsichtsbehörde enthält darüber hinaus noch folgende Information (Art. 33 Abs. 3):

- eine Beschreibung der Art der »Datenpanne«, soweit möglich mit Angabe der betroffenen Kategorien, der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze

10. // SICHERER UMGANG MIT PERSONENBEZOGENEN DATEN DURCH TECHNISCH-ORGANISATORISCHE MASSNAHMEN (TOM)

DS-GVO-Regelungen

- *Art. 24: Verantwortung des für die Verarbeitung Verantwortlichen*
- *Art. 25: Datenschutz durch Technikgestaltung und durch datenschutzrechtliche Voreinstellungen*
- *Art. 29: Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters*
- *Art. 32: Sicherheit der Verarbeitung*

Besondere Aufmerksamkeit gilt in der DS-GVO in der Daten- und Informationssicherheit, indem der Verantwortliche, aber auch der Auftragsverarbeiter nachweisen muss, alle möglichen organisatorischen und technischen Maßnahmen ergriffen zu haben, um ein Risiko der unbefugten Kenntnisnahme und des Verlusts personenbezogener Daten zu minimieren. Diese Verantwortung umfasst auch die sorgfältige Auswahl von geeigneten Dienstleistern in diesem Umfeld, z. B. von geeigneten Softwarelieferanten, Rechenzentrumsdienstleistern oder Cloud-Dienstleistern. |25|

10.1. // VERTRAULICHKEIT, INTEGRITÄT, VERFÜGBARKEIT UND BELASTBARKEIT

Zur Wahrung der **Vertraulichkeit** von Daten gehören Zutritts-, Zugangs-, Zugriffs- und Weitergabe-Kontrollmaßnahmen. Unter der **Zutrittskontrolle** werden die Maßnahmen verstanden, um Unbefugten das Betreten von Büros bzw. den Räumlichkeiten, in denen die Verarbeitung stattfindet (z. B. Serverraum), zu verwehren. Geeignete Maßnahmen hierfür sind u. a. Sicherheitsschlösser, Zutritt mit Zugangskarten, **Zugangskontrolle** durch Pförtner, Einsatz von Alarmanlagen, Videoüberwachung und einbruchssichere Fenster. Die Zugangskontrolle soll verhindern, dass Unbefugte die Datenverarbeitungssysteme nutzen können, um über diese an Daten des Inkassounternehmens zu gelangen, z. B. durch Sicherung aller Computer (inkl. mobiler Geräte) durch individuell geschützte Benutzerkonten, Einsatz von Firewalls und von Sicherheitssoftware. Über die **Zugriffskontrolle** soll gewährleistet werden, dass nur befugte Personen auf die Daten des Inkassounternehmens zugreifen dürfen. Zugangs- und Zugriffskontrolle sind durch Einsatz von Berechtigungssystemen zu gewährleisten. Bei der **Weitergabe von Daten** ist zu berücksichtigen, dass beim Transport der Daten Sicherheitsmaßnahmen installiert sind, damit kein Unbefugter diese einsehen und zweckentfremden kann. Zum Zuge kommen hier diverse Verschlüsselungen (z. B. verschlüsselte Hardware, verschlüsselte Internetverbindungen usw.). Bei einem physischen Transport von Daten wären geeignete Maßnahmen zu treffen (z. B. Transport von Akten in verschlossenen Containern).

Unter der **Integrität** wird die Konsistenz und Korrektheit aller Daten verstanden, die in einem oder mehreren Anwendungssystemen verarbeitet werden. Die Informationen sollen unverändert bleiben bzw. nur dann geändert bzw. gelöscht werden, wenn dies erforderlich ist. Einer Integritätsverletzung folgt nicht selten ein »Daten-GAU« (Datenverlust), wenn Informationen nicht mehr (logisch) zueinanderpassen und aus diesem Grunde kosten- und zeitintensive Bereinigungsaktivitäten von der IT-Abteilung (oder dem IT-Dienstleister) durchgeführt werden müssen.

Die **Verfügbarkeit** wird durch Sicherungsmaßnahmen der Daten und Systeme gewährleistet. Im Falle einer Zerstörung sollen diese Daten in akzeptabler Zeit wieder für die Verarbeitung zur Verfügung stehen. Die Durchführung von Back-ups gehört ebenso dazu wie

die Tests, ob ein Rückspielen der Daten zu dem gewünschten Ergebnis führt. Der Inkassodienstleister tut gut daran, seine kritischen Systeme auf den Prüfstand zu setzen und sich nach der akzeptabelsten Höchstausfallzeit zu fragen und die damit einhergehenden Gegenmaßnahmen zu ergreifen, um eine rasche Wiederherstellung zu gewährleisten.

Gleiches gilt für die **Belastbarkeit** der Systeme. Darunter wird verstanden, dass diese sich dem Datenvolumen und der Datenverarbeitung des Inkassounternehmens anpassen und auch widrige Umstände berücksichtigt werden, damit Systeme auch unter hoher Belastung weiterhin eine sichere Verarbeitung gewährleisten (z. B. bei Monats- und /oder Jahresabschlüssen).

Grundsätzlich ist hinsichtlich aller vorgenannten Sicherheitsmaßnahmen der aktuelle Stand der Technik zu berücksichtigen.

10.2. // DATENSICHERHEIT DURCH PSEUDONYMISIERUNG

Gut für die Datensicherheit: Pseudonymisierung von Daten

Die Pseudonymisierung hat in der DS-GVO einen hohen Stellenwert. Durch Pseudonymisierung werden personenbezogene Daten innerhalb einer Datenbank zentral gespeichert. Mit der pseudonymisierten Speicherung können Anforderungen der DS-GVO, wie z. B. die Berichtigung von Daten, aber auch die Löschung von Daten, sehr einfach gelöst werden, da lediglich die zentral gespeicherten Stammdaten anzupassen oder zu löschen sind. Auch der Austausch von Informationen zwischen den Mandanten und anderen Parteien, die im Besitz des Pseudonyms sind, lässt sich so organisieren, indem auf Basis einer Referenztabelle (z. B. über eine eindeutige Kontaktdaten-ID) Daten ausgetauscht werden.

10.3. // RISIKOANALYSE

Damit ein Inkassounternehmen seine technischen und organisatorischen Maßnahmen sinnvoll festlegen kann, ist es nach der DS-GVO verpflichtet, zunächst die faktischen Risiken zu analysieren, die für seine Daten bestehen. Bei einer solchen Risikoanalyse ist zu überprüfen, welche Gefahren in Bezug auf die Verarbeitung von personenbezogenen Daten beim Inkassounternehmen existieren. Die Auflistung der mit der Verarbeitung verbundenen Risiken sollte regelmäßig auf Vollständigkeit überprüft und die damit getroffenen Gegenmaßnahmen auf deren Wirksamkeit analysiert werden. Diese Risikoanalyse kann auch für eine ggf. erforderliche Datenschutz-Folgenabschätzung (Art. 35) genutzt werden.

10.4. // WEISUNGSGEBUNDENHEIT DER AN DER VERARBEITUNG BETEILIGTEN PERSONEN

Es wird grundsätzlich der Verantwortliche bzw. der Auftragsverarbeiter verpflichtet, nur solche Personen mit der Verarbeitung von Daten zu betrauen, die deren Weisung unterworfen sind. Es geht um die »unterstellten« Personen und ist sowohl für interne als auch externe Mitarbeiter maßgeblich.

|25| Siehe: 5. // Datenübertragung an außereuropäische Empfänger (Drittländer), Seite 16.

10.5. // DATENSCHUTZKONFORME TECHNIKGESTALTUNG UND DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Die meisten Inkassounternehmen dürften Standard-Inkassosoftware für die Bearbeitung ihrer Fälle nutzen. Beim Erwerb einer neuen Software bzw. bei der Analyse der aktuell im Einsatz befindlichen Software ist daher zu prüfen, inwiefern den Anforderungen aus Art. 25 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) beim Softwaredienstleister Rechnung getragen wurde. Hierüber muss eine entsprechende vertragliche Vereinbarung mit dem Anbieter getroffen werden.

Die Softwareanbieter sollten bei der Implementierung ihrer Softwarelösung bereits alle datenschutzkonformen Voreinstellungen so dokumentieren, dass Inkassounternehmen die Möglichkeit haben, diese zu prüfen und ggf. an eigene Bedürfnisse anzupassen.

11. // DATENSCHUTZ-FOLGENABSCHÄTZUNG

DS-GVO-Regelung

- *Art. 35: Datenschutz-Folgenabschätzung*

Eine Abschätzung der Folgen der vorgesehenen Datenverarbeitungsvorgänge ist nach Art. 35 durchzuführen, wenn diese voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Insbesondere ist eine Datenschutz-Folgenabschätzung erforderlich, wenn

- eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen beim Verantwortlichen erfolgt, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen,

- es sich um eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 handelt oder

- eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche stattfindet.

Eine Datenschutz-Folgenabschätzung beim Verantwortlichen ist aber ferner durchzuführen, wenn dessen Datenverarbeitungen (gänzlich oder teilweise) auf der sogenannten Blacklist der Aufsichtsbehörde zu finden sind. Auf dieser Blacklist, die die Aufsichtsbehörde nach Art. 35 Abs. 4 zu erstellen hat, sind alle Verarbeitungsvorgänge aufgeführt, für die eine Datenschutz-Folgenabschätzung durchzuführen ist.

Die Datenschutzkonferenz (DSK) hat mittlerweile eine solche Blacklist |26| erstellt. Die Datenverarbeitungen bei Inkassodienstleistern werden in dieser wie folgt erwähnt:

7	Umfangreiche Erhebung und Veröffentlichung oder Übermittlung von personenbezogenen Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen	**Betrieb von Bewertungsportalen**	Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten (Online-Bewertungsportal z. B. für Ärzte, Selbstständige oder Lehrer).
		Inkassodienstleistungen – Forderungsmanagement	Ein Unternehmen verarbeitet für seine Kunden in großem Umfang personenbezogene Daten von Schuldnern, insbesondere Vertragsdaten, Rechnungsdaten und Daten über Vermögensverhältnisse von Schuldnern zur Geltendmachung von Forderungen; ggf. werden Daten an Auskunfteien übermittelt.
		Inkassodienstleistungen – Factoring	Ein Unternehmen lässt sich in großem Umfang Forderungen übertragen, um diese auf eigenes Risiko geltend zu machen. Es verarbeitet hierfür insbesondere Vertragsdaten, Rechnungsdaten, Scoringdaten und Informationen über Vermögensverhältnisse von Schuldnern; ggf. werden Daten an Auskunfteien übermittelt.

Ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss, muss im Einzelfall für die Datenverarbeitung geprüft werden

Ob und wann der jeweilige Inkassodienstleister die in der Blacklist genannten Voraussetzungen erfüllt, muss im Einzelfall genau geprüft werden. Inkassodienstleister können zu einer Datenschutz-Folgenabschätzung verpflichtet sein, wenn sie Daten an Auskunfteien übermitteln.

Im Fall, dass der Verantwortliche eine Datenschutz-Folgenabschätzung durchführen muss, ist dabei |27| der Rat des Datenschutzbeauftragten einzuholen.

12. // BETRIEBLICHER DATENSCHUTZBEAUFTRAGTER

DS-GVO-Regelungen
- *Art. 37: Benennung eines Datenschutzbeauftragten*
- *Art. 38: Stellung des Datenschutzbeauftragten*
- *Art. 39: Aufgaben des Datenschutzbeauftragten*

BDSG-Regelung
- *§ 38: Datenschutzbeauftragte nicht öffentlicher Stellen*

Zwar ist die Benennung eines Datenschutzbeauftragten für die meisten Inkassodienstleister nicht verpflichtend – es lohnt sich aber, einen (internen oder externen) Experten mit der Einhaltung und Kontrolle aller Anforderungen aus der DS-GVO zu beauftragen.

12.1. // BENENNUNGSPFLICHT

Gemäß Art. 37 Abs. 1 muss ein Verantwortlicher, somit auch ein Inkassodienstleister, einen Datenschutzbeauftragten benennen, wenn die »Kerntätigkeit« (Haupttätigkeit) des Unternehmens

- in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

- in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 bzw. 10 besteht.

Das bedeutet für Inkassounternehmen, dass ein Datenschutzbeauftragter nicht grundsätzlich bestellt werden muss, sondern es vielmehr auf ihre Kerntätigkeit (also nicht nur auf eine etwaige Nebentätigkeit des Unternehmens) ankommt.

Natürlich kann jedes Unternehmen freiwillig einen Datenschutzbeauftragten bestellen. Dies dürfte gegenüber der Behörde und Mandanten ohnehin positive Wirkung erzielen und ist schon wegen der umfassenden Dokumentationspflichten (die Dokumentationen müssen stets aktuell sein) sinnvoll für das Unternehmen selbst.

Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten bestellen.

Wenn ein Unternehmen in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, so ist gemäß § 38 BDSG ein Datenschutzbeauftragter zu benennen.

Unternehmen, die zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 verpflichtet sind, |28| müssen – unabhängig von der Zahl der Beschäftigten (!) – gemäß § 38 Abs. 1 Satz 2 BDSG immer einen Datenschutzbeauftragten benennen.

|26| Die Liste der Verarbeitungstätigkeiten, für die eine Datenschutz-Folgenabschätzung (sog. Blacklist) durchzuführen ist, ist u. a. abrufbar unter: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf.

|27| Informationen zur Durchführung der Datenschutz-Folgenabschätzung ergeben sich z. B. aus der GDD-Praxishilfe DS-GVO X, abrufbar unter: https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_10.pdf. Der Bundesverband Deutscher Inkasso-Unternehmen e. V. (BDIU) hat zudem für seine Mitgliedsunternehmen ein Template zur Durchführung der Datenschutz-Folgenabschätzung entwickelt, das beim Verband angefragt werden kann.

|28| Siehe: 11. // Datenschutz-Folgenabschätzung, Seite 43.

Die Kontaktdaten des Datenschutzbeauftragten müssen öffentlich gemacht werden – eine konkrete Namensnennung sollte aber nicht erfolgen. Anders sieht es gegenüber der Aufsichtsbehörde aus: Hier muss der Datenschutzbeauftragte namentlich benannt werden.

12.2. // STELLUNG DES DATENSCHUTZBEAUFTRAGTEN

Der Datenschutzbeauftragte ist weisungsfrei bei der Erfüllung seiner Aufgaben und berichtet unmittelbar der höchsten Managementebene. Er darf wegen der Erfüllung seiner Aufgaben weder abberufen noch benachteiligt werden.

Der Datenschutzbeauftragte ist frühzeitig in alle für den Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Ihm sind die erforderlichen Ressourcen zur Verfügung zu stellen.

Der Datenschutzbeauftragte ist zur Verschwiegenheit verpflichtet.

12.3. // AUFGABEN

Bei allen Fragen rund um den Schutz personenbezogener Daten ist der Datenschutzbeauftragte einzubeziehen

Dem Datenschutzbeauftragten obliegen (mindestens) nachfolgende Aufgaben:

- **Kontrolle:** Der Datenschutzbeauftragte überwacht die Einhaltung der DS-GVO, vor allem durch Kontrollen, die zum Nachweis dokumentiert werden müssen.

  Zudem überwacht er die Einhaltung der anderen Datenschutzvorschriften sowie der Strategien des Unternehmens in Bezug auf den Schutz personenbezogener Daten. Das kann auch die Zuweisung von Zuständigkeiten durch das Inkassounternehmen beinhalten, wie für die Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter oder zumindest diesbezügliche Überprüfungen.

- **Unterrichtung und generelle Beratung:** Der Datenschutzbeauftragte ist bezüglich aller datenschutzrechtlichen Pflichten zuständig, d. h. für die Unterrichtung und Beratung des Unternehmens sowie der Beschäftigten, die Daten verarbeiten.

- **Beratung auf Anfrage:** Außerdem gehört es zu seinen Aufgaben, eine Beratung auf Anfrage im Zusammenhang mit der ggf. durchzuführenden Datenschutz-Folgenabschätzung sowie die Überwachung ihrer Durchführung vorzunehmen.

Der Datenschutzbeauftragte ist nicht zuständig für das Führen des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30). Jedes Inkassounternehmen wird aber gut beraten sein, seinen Datenschutzbeauftragten hieran – zumindest unterstützend – zu beteiligen.

13. // ZUSAMMENARBEIT MIT AUSKUNFTEIEN

DS-GVO-Regelung
- *Art. 6: Rechtmäßigkeit der Verarbeitung*

BDSG-Regelung
- *§ 31: Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften*

Auskunfteien verarbeiten geschäftsmäßig bonitätsrelevante Daten über Unternehmen oder natürliche Personen, um sie bei entsprechendem Bedarf einem Inkassounternehmen zugänglich zu machen.

13.1. // ANFRAGEN BEI AUSKUNFTEIEN

Wie jede Datenübermittlung bedürfen auch die Anfrage bei und der Abruf von Daten einer Auskunftei einer rechtlichen Grundlage.

Rechtliche Grundlage ist grundsätzlich Art. 6 Abs. 1 Buchstabe f: Das hiernach erforderliche berechtigte Interesse des Inkassounternehmens bzw. dessen Mandanten liegt vor. Insbesondere zum Zweck der Schadensminderung (Inkassokosten als Teil des vom Schuldner zu tragenden Verzugsschadens, der dem Mandanten entstanden ist) kann es für das Inkassounternehmen bzw. den Mandanten als Dritten erforderlich sein, in Erfahrung zu bringen, wie sich die finanzielle Situation des Schuldners darstellt (Bonitätsdaten). Überdies besteht ein berechtigtes Interesse an der Information, mit welcher Wahrscheinlichkeit der Schuldner in der Lage sein wird, bestehende Verpflichtungen zu erfüllen (anhand eines Scores). Informationen können in die Steuerung des Inkassoprozesses einfließen.

Die angefragte Auskunftei kann entsprechende Auskünfte auf derselben rechtlichen Grundlage erteilen, da diese Auskünfte im Interesse des anfragenden Inkassounternehmens und des Mandanten (sowie des angefragten Schuldners selbst) liegen.

13.2. // ÜBERMITTLUNG FORDERUNGSBEZOGENER DATEN AN AUSKUNFTEIEN

Rechtsgrundlage für die Übermittlung forderungsbezogener Daten an Auskunfteien, die sogenannte Einmeldung, ist Art. 6 Abs. 1 Buchstabe f. Dabei ist das »berechtigte Interesse eines Dritten« gegeben. Nach höchstrichterlicher Rechtsprechung (BGH, NJW 2011, 2204, 2206) sind Auskunfteien und »die Erteilung von Bonitätsauskünften für das Funktionieren der Wirtschaft von erheblicher Bedeutung«.

Da Auskunfteien eingemeldete Daten zu einem vertragswidrigen Zahlungsverhalten des Schuldners (»Negativdaten«) u. a. auch zur Berechnung eines Scorewerts verwenden, ist bei der Einmeldung die Vorschrift des § 31 Abs. 2 BDSG zu beachten. Denn: Nur solche Forderungen über eine geschuldete Leistung, die trotz Fälligkeit nicht erbracht worden ist, dürfen von der Auskunftei bei der Verwendung des Wahrscheinlichkeitswerts berücksichtigt werden,

1. die durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden sind oder für die ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,

2. die nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden sind,

3. die der Schuldner ausdrücklich anerkannt hat,

4. bei denen
   a. der Schuldner nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,
   b. die erste Mahnung mindestens vier Wochen zurückliegt,
   c. der Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist und
   d. der Schuldner die Forderung nicht bestritten hat oder

5. deren zugrunde liegendes Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und bei denen der Schuldner zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist.

Die DSK hat bestätigt, dass die Erfüllung der genannten Voraussetzungen, die auch in § 31 Abs. 2 BDSG zu finden sind, im Rahmen dieser Einzelfallprüfung eine Indizwirkung für eine zulässige Einmeldung darstellt |29| und damit das vorrangige berechtigte Interesse des Verantwortlichen bzw. eines Dritten als gegeben angesehen werden kann.

Entsprechend dem Grundsatz der Transparenz der Verarbeitung (Art. 5 Abs. 1 Buchstabe a) sollte das Inkassounternehmen die betroffene Person im vorgerichtlichen Bereich rechtzeitig vor einer Einmeldung informieren.

Bezüglich der Einmeldung hat sich der Bundesverband Deutscher Inkasso-Unternehmen e. V. (BDIU) mit den folgenden Auskunfteien im Frühjahr 2018 auf folgende Texte für Einmeldeunterrichtungen verständigt und seine Mitglieder im April 2018 entsprechend informiert.

1. Bisnode Deutschland GmbH
2. Creditreform Boniversum GmbH
3. CRIF Bürgel GmbH
4. IHD Gesellschaft für Kredit- und Forderungsmanagement mbH
5. Infoscore Consumer Data GmbH
6. Regis24 GmbH
7. SCHUFA Holding AG
8. Verband der Vereine Creditreform e. V.

Texte für die Einmeldeunterrichtung – abgestimmt mit vielen Auskunfteien

Die abgestimmten Texte lauten wie folgt:

*Einmeldeunterrichtung gemäß den Anforderungen des **§ 31 Abs. 2 Satz 1 Nr. 4 BDSG** (einzusetzen frühestens mit der ersten Mahnung)*

»Wir weisen darauf hin, dass wir gemäß Art. 6 Abs. 1 Buchstabe f DS-GVO Daten über trotz Fälligkeit nicht beglichene Forderungen an eine oder mehrere Wirtschaftsauskunftei(en) übermitteln (siehe unten), wobei diese Daten dort Berücksichtigung bei der Ermittlung von Wahrscheinlichkeitswerten (Scoring) finden können. Das geschieht, soweit Sie nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden sind, die erste Mahnung mindestens vier Wochen zurückliegt und Sie die Forderung nicht bestritten haben.

*Weitere Informationen über die Wirtschaftsauskunftei(en), an die wir Daten übermitteln, erhalten Sie (mit dem beiliegenden Informationsblatt **oder**) unter www.x-Auskunftei.de (www.y-Auskunftei.de und www.z-Auskunftei.de).«*

oder

*Einmeldeunterrichtung gemäß den Anforderungen des **§ 31 Abs. 2 Satz 1 Nr. 5 BDSG***

»Wir weisen darauf hin, dass wir gemäß Art. 6 Abs. 1 Buchstabe f DS-GVO Daten über trotz Fälligkeit nicht beglichene Forderungen an eine oder mehrere Wirtschaftsauskunftei(en) übermitteln (siehe unten), wobei diese Daten dort Berücksichtigung bei der Ermittlung von Wahrscheinlichkeitswerten (Scoring) finden können. Das geschieht, soweit die geschuldete Leistung nicht erbracht worden ist und das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann.

*Weitere Informationen über die Wirtschaftsauskunftei(en), an die wir Daten übermitteln, erhalten Sie (mit dem beiliegenden Informationsblatt **oder**) unter www.x-Auskunftei.de (www.y-Auskunftei.de und www.z-Auskunftei.de).«*

Obwohl bei **titulierten Forderungen** nach der jetzigen Rechtslage keine Verpflichtung besteht, den Betroffenen vor einer Einmeldung zu informieren, ist auch hier eine Unterrichtung vor Einmeldung aus Transparenzgründen denkbar. Je älter die einzumeldende titulierte Forderung ist, desto eher sollte über eine Unterrichtung der betroffenen Person nachgedacht werden.

Ein hierzu passender Einmeldeunterrichtungstext lautet:

»Wir weisen darauf hin, dass wir gemäß Art. 6 Abs. 1 Buchstabe f DS-GVO Daten über die nicht vertragsgemäße Abwicklung von Forderungen an eine oder mehrere Wirtschaftsauskunftei(en) übermitteln (siehe unten), wobei diese Daten dort Berücksichtigung bei der Ermittlung von Wahrscheinlichkeitswerten (Scoring) finden können. Dies geschieht, soweit die vorstehend genannte Forderung trotz Fälligkeit nicht ausgeglichen wurde, die Weitergabe der Daten zur Wahrung unserer berechtigten Interessen oder der eines Dritten erforderlich ist und die Forderung durch ein rechtskräftiges Urteil oder einen Schuldtitel nach § 794 Zivilprozessordnung (z. B. Vollstreckungsbescheid) festgestellt worden ist.

Weitere Informationen über die Wirtschaftsauskunftei(en), an die wir Daten übermitteln, erhalten Sie unter www.x-Auskunftei.de (www.y-Auskunftei.de und www.z-Auskunftei.de).«

|29| Beschluss der DSK vom 23. März 2018, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20180323_dskb_einmeldungen.pdf.

14. // AUFTRAGSVERARBEITUNG

14.1. // BEGRIFF

Unter Auftragsverarbeitung versteht die DS-GVO eine besondere Verarbeitung: Dabei verbleibt die Verantwortlichkeit für die Datenverarbeitung bei dem Verantwortlichen (z. B. dem Inkassounternehmen), während die tatsächliche, physische Verarbeitung durch eine andere Stelle stattfindet, den Auftragsverarbeiter.

Anders als im bis zum 24. Mai 2018 geltenden BDSG wird mit der DS-GVO der Auftragsverarbeiter stärker in die Verantwortlichkeit mit einbezogen: Entsteht bei einer rechtswidrigen Datenverarbeitung für die betroffene Person ein Schaden, so haftet – neben dem Verantwortlichen – auch der Auftragsverarbeiter.

Verantwortlicher und Auftragsverarbeiter können wie folgt unterschieden werden:

- Der Verantwortliche legt die Zwecke und Mittel der Datenverarbeitung fest.
- Der Auftragsverarbeiter nimmt vom Auftraggeber (Verantwortlichen) dessen Weisungen entgegen und hat somit keinen Einfluss auf die Zwecke und Mittel der Verarbeitung.

Inkassounternehmen sind somit regelmäßig Verantwortliche, da sie selbst den Zweck (Forderungsmanagement) und die Mittel ihrer Inkassobearbeitung festlegen.

14.2. // AUFTRAGSVERARBEITUNGSVERHÄLTNISSE

14.2.1. // Inkasso für die öffentliche Hand

Ausnahmsweise werden Inkassodienstleister im Rahmen einer Auftragsverarbeitung tätig. Das ist dann der Fall, wenn sie als Verwaltungshelfer beim Einzug von öffentlich-rechtlichen Forderungen für die öffentliche Hand (Bund, Länder, Kommunen und andere öffentlich-rechtliche Institutionen) tätig werden.

Grund dafür ist, dass die öffentliche Hand gesetzlich gehindert sein kann, Daten zu Forderungen bzw. Schuldnern zur eigenverantwortlichen Verarbeitung an Inkassounternehmen als Verantwortliche zu übermitteln. In solchen Fällen können Inkassounternehmen als Verwaltungshelfer eingeschaltet werden, also weisungsgebunden tätig werden, sodass sie hier – entgegen der sonst üblichen rechtlichen Stellung als Verantwortlicher –»nur« Auftragsverarbeiter sind.

Wegen der Auftragsverarbeitung bedarf es bei einer Tätigkeit des Inkassounternehmens als Verwaltungshelfer keiner Rechtsgrundlage für die Weitergabe der Daten vom Auftraggeber (also die jeweilige öffentliche Institution) an den Auftragnehmer (das Inkassounternehmen) (sog. Privilegierung der Auftragsverarbeitung).

Der Verwaltungshelfer wird als Auftragsverarbeiter unselbstständig und nach Weisung eines Hoheitsträgers ohne eigene Entscheidungsbefugnis tätig.

14.2.2. // Typische Dienstleister als Auftragsverarbeiter

In der Regel wird mit folgenden Dienstleistern ein Auftragsverarbeitungsverhältnis vertraglich vereinbart:

- Druck-/Kuvertierdienstleister
- Externe Callcenter

- Entsorgungsunternehmen
- Archivierungsdienste/Posteingangsverarbeitungsdienstleister
- Softwarehersteller/IT-Dienstleister für (Fern-)Wartungstätigkeiten
- Rechenzentrumsbetrieb
- Back-up-Dienstleister
- Cloud-Dienstleister

Tipp

Achten Sie bei der Auswahl Ihrer Dienstleister/Auftragsverarbeiter auf deren Geschäftssitz. Befindet sich dieser in einem Drittland, sind ggf. weitere Voraussetzungen zu beachten. |30|

14.3. // AUFGABEN UND PFLICHTEN DES AUFTRAGSVERARBEITERS

Bei der Beauftragung eines Auftragsverarbeiters ist ein eigenständiger Vertrag oder eine entsprechende Vereinbarung als separate Anlage zu einem Vertrag zu schließen.

Vor der Übergabe personenbezogener Daten an den Auftragsverarbeiter muss der Verantwortliche prüfen, ob der Auftragsverarbeiter alle Maßnahmen zur »Sicherheit der Verarbeitung« (Art. 32) getroffen hat. Dies muss er in regelmäßigen Abständen wiederholen.

Die Durchführung der Prüfung kann durch einen Vor-Ort-Besuch beim Auftragsverarbeiter erfolgen oder durch die Vorlage geeigneter Dokumente (Sicherheitskonzepte, Auditberichte, Testberichte etc.) durch den Auftragsverarbeiter.

Besonderheit bei der Auftragsverarbeitung in einem unsicheren Drittland

Im Fall der Übermittlung an Auftragsverarbeiter in Drittländern empfiehlt sich eine gesonderte rechtliche Beratung.

Überprüfung der Auftragsverarbeitungsverträge erforderlich

Es wird ansonsten empfohlen, alle Verträge zu Auftragsverarbeitungen dahin gehend zu überprüfen, ob die nachfolgenden Regelungen darin enthalten sind. Sofern das nicht der Fall ist oder es noch keine DS-GVO-konforme vertragliche Regelung gibt, sind Verträge mit Auftragsverarbeitern zu ergänzen.

- **Beauftragung von Subunternehmern mit Vetorecht:** Der Auftragsverarbeiter darf ohne vorherige gesonderte oder allgemeine schriftliche Zustimmung des Verantwortlichen keinen weiteren Auftragsverarbeiter (Subunternehmer) einsetzen. Der Verantwortliche hat bei der Beauftragung von Subunternehmern ein Vetorecht. Der Auftragsverarbeiter hat die Verträge mit Subunternehmern so zu gestalten, dass sich diese ebenfalls den Kontrollrechten des Verantwortlichen unterwerfen.

- **Weisungsrecht des Verantwortlichen:** Art. 28 Abs. 3 Buchstabe a und Art. 29 regeln das Weisungsrecht des Verantwortlichen. Um der Dokumentationspflicht nachzukommen, sind die Weisungen grundsätzlich schriftlich zu erteilen.

- **Vertraulichkeits-/Verschwiegenheitsverpflichtung im Auftragsverhältnis:** Im Auftragsverhältnis muss eine Verpflichtung auf Datenschutz und Datensicherheit enthalten sein und mit Blick auf die Wahrung der Vertraulichkeit sowie die Verpflichtung zur Verschwiegenheit des Auftragsverarbeiters geschlossen werden.

- **Beschreibung aller technisch-organisatorischen Maßnahmen:** Die technisch-organisatorischen Maßnahmen |31| sind vertraglich festzuhalten und zu regeln.

|30| Siehe: 5. // Datenübertragung an außereuropäische Empfänger (Drittländer), Seite 16.

|31| Siehe: 10. // Sicherer Umgang mit personenbezogenen Daten durch technisch-organisatorische Maßnahmen (TOM), Seite 40.

Tipp

Es empfiehlt sich, die technisch-organisatorischen Maßnahmen in einer Art Checkliste zusammenzufassen und für alle Auftragsverarbeiter ein Ergebnisprotokoll zu verfassen, in dem die Prüfpunkte enthalten sind und das Prüfungsergebnis festgehalten wird. Dieses Dokument sollte mit dem Auftragsverarbeiter abgestimmt werden und dient beiden Seiten als Nachweis der ordnungsgemäßen Überprüfung dieser Maßnahmen.

- **Bearbeitung von Anträgen zur Wahrung der Betroffenenrechte:** Der Verantwortliche muss die Erfüllung der Betroffenenrechte |32| vertraglich mit dem Auftragsverarbeiter regeln. Dazu muss der Auftragsverarbeiter sämtliche Anträge zu Betroffenenrechten an den Inkassodienstleister als Verantwortlichen übermitteln.

Tipp

Dokumentieren Sie alle Tätigkeiten rund um die Wahrung von Betroffenenrechten beim Auftragsverarbeiter im Rahmen einer Arbeitsanweisung/Arbeitsrichtlinie. Es sollten auch die Prozesse berücksichtigt werden, die durchgeführt werden, wenn ein Betroffener statt beim Inkassounternehmen seine Rechte beim Auftragsverarbeiter durchsetzen möchte, sodass das Inkassounternehmen in jedem Fall davon Kenntnis hat, welche Betroffenen von ihrem Informationsrecht Gebrauch machen.

- **Beendigung des Auftragsverarbeitungsverhältnisses:** Die Anforderungen an die Beendigung des Auftragsverarbeitungsverhältnisses sind bereits im Vertrag zu regeln, insbesondere in Bezug auf die Rückgabe der Daten oder den Nachweis der Löschung der im Auftrag überlassenen Daten. Darüber hinaus ist sicherzustellen, dass die Löschung auch tatsächlich stattfindet, z. B. durch die Vorlage entsprechender Löschprotokolle.

- **Nachweis der Einhaltung der vertraglichen Pflichten und Recht der Überprüfung:** Der Auftragsverarbeiter hat den Nachweis über die Einhaltung der vertraglich vereinbarten Pflichten, z. B. bestimmter Prüfpflichten, nach Art. 28 Abs. 3 zu erbringen.

  Prüfung vor Ort beim Auftragsverarbeiter ist sinnvoll und sollte dokumentiert werden!

  Inkassodienstleister sollten sich außerdem vertraglich ein eigenes Prüfrecht vor Ort einräumen lassen.

- **Informationspflicht des Auftragsverarbeiters bei Datenschutzverletzungen:** Wird beim Auftragsverarbeiter eine Datenschutzverletzung, d. h. eine »Datenpanne«, festgestellt, muss er den Inkassodienstleister davon unverzüglich in Kenntnis setzen, damit dieser rechtzeitig die Aufsichtsbehörde (Achtung: 72-Stunden-Frist ab Bekanntwerden der Verletzung nach Art. 33) und ggf. die betroffene(n) Person(en) informieren kann.

Tipp

Das Inkassounternehmen sollte im Rahmen der Erstellung von Prozessmaßnahmen gemeinsam mit dem Auftragsverarbeiter festlegen, mit welchem Kommunikationsmedium (z. B. Telefon, E-Mail) man welchen Ansprechpartner (aufseiten des Inkassounternehmens) zu informieren hat bzw. welche Eskalationswege es gibt, falls diese festgelegten Prozesse nicht durchgeführt werden können.

14.4. // VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN DES AUFTRAGSVERARBEITERS

Jeder Auftragsverarbeiter muss nach Art. 30 Abs. 2 ein Verzeichnis von Verarbeitungstätigkeiten führen.

Inhalt eines solchen Verzeichnisses des Auftragsverarbeiters sind:

- Name und Kontaktdaten des Auftragsverarbeiters; auch alle Daten der Verantwortlichen, auf deren Weisung der Auftragsverarbeiter personenbezogene Daten verarbeitet, ggf. deren Vertreter
- Name und Kontaktdaten des etwaigen Datenschutzbeauftragten
- die Kategorien von Verarbeitungen, die im Auftrag eines jeden Verantwortlichen geführt werden
- ggf. die Übermittlungen von Daten in ein Drittland
- die technisch-organisatorischen Maßnahmen in allgemeiner Art und Weise

Tipp

Das Inkassounternehmen sollte den Auftragsverarbeiter bei Erstellung des Verzeichnisses von Verarbeitungstätigkeiten unterstützen, indem es sein eigenes Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 als »Rahmendokument« zur Verfügung stellt. Hier kann das Inkassounternehmen als Verantwortlicher auf das ausgegliederte Verfahren verweisen.

Das Verzeichnis von Verarbeitungstätigkeiten des Auftragsverarbeiters nach Art. 30 Abs. 2 kann dann als eigenständiges Dokument in das Datenschutzmanagement (oder die eigene Dokumentation) beim Verantwortlichen hinzugenommen und damit als Ergänzung zum eigenen Verfahren angesehen werden.

|32| Siehe: 7. // Informationspflichten und Betroffenenrechte, Seite 21.

15. // SANKTIONEN UND AUFSICHTSMASSNAHMEN

DS-GVO-Regelungen
- *Art. 58: Befugnisse*
- *Art. 83: Allgemeine Bedingungen für die Verhängung von Geldbußen*
- *Art. 84: Sanktionen*

BDSG-Regelungen
- *§ 41: Anwendung der Vorschriften über das Bußgeld- und Strafverfahren*
- *§ 42: Strafvorschriften*

Art. 58, 83 und 84 sowie die §§ 41 ff. BDSG regeln Sanktionen bei Verstößen gegen die DS-GVO. Eine Geldbuße als eine der möglichen datenschutzaufsichtsbehördlichen Maßnahmen soll in jedem Einzelfall abschreckend sein.

15.1. // RECHTLICHE VORSCHRIFTEN

Das Strafrecht wird weiterhin von den einzelnen EU-Mitgliedstaaten geregelt, d. h., jeder Staat bestimmt seine Straftatbestände und daraus folgende Sanktionen selbst. In Deutschland ist insbesondere § 42 BDSG als einschlägiger Straftatbestand zu beachten.

Bußgeldvorschriften hingegen ergeben sich vor allem direkt aus der DS-GVO und finden sich in den Art. 83 und 84. Daneben gelten aber auch noch einschlägige nationale Bußgeldvorschriften.

15.2. // FREIHEITSSTRAFE ODER GELDSTRAFE

Freiheits- oder Geldstrafen drohen nur bei besonders schwerwiegenden Verstößen gegen die DS-GVO. Gemäß § 42 BDSG wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer wissentlich und gewerbsmäßig nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen einem Dritten übermittelt oder auf andere Art und Weise zugänglich macht, ohne hierzu berechtigt zu sein; mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind, gegen Entgelt oder in der Absicht verarbeitet oder erschleicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen. Die Taten werden nur auf Antrag des Betroffenen, des Verantwortlichen, des/der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit oder der Aufsichtsbehörde verfolgt.

15.3. // GELDBUSSE

Fast alle Vorschriften der DS-GVO sind mit empfindlichen Geldbußen und anderen Rechtsfolgen wie z. B. Gewinnabschöpfungen bewehrt.

15.3.1. // Höhe

Maximale Geldbuße kann 20 Millionen Euro bzw. 4 % des vom Unternehmen weltweit erwirtschafteten Jahresumsatzes im vorherigen Geschäftsjahr betragen

Die Geldbuße nach Art. 83 Abs. 4, Abs. 5 bzw. Abs. 6 soll verhältnismäßig ausfallen, aber dennoch abschreckend, d. h. für das Unternehmen spürbar sein. Dies ergibt sich aus Art. 83 Abs. 1.

Je nachdem, gegen welche DS-GVO-Vorschrift verstoßen wurde, beträgt die maximale Geldbuße entweder 10 bzw. 20 Millionen Euro oder 2 % bzw. 4 % des vom Unternehmen

weltweit im vorherigen Geschäftsjahr erwirtschafteten Jahresumsatzes. Dabei ist der jeweils höhere Wert von beiden Optionen ausschlaggebend. Nach herrschender Meinung ist für die Berechnung der Konzernumsatz entscheidend.

15.3.2. // Kriterien für die Sanktionierung

Die konkrete Geldbuße wird anhand der in Art. 83 Abs. 2 Buchstaben a bis k festgelegten Kriterien berechnet. Dazu gehören:

- Art, Schwere und Dauer des Verstoßes, wobei der Zweck der betreffenden Verarbeitung, die Zahl der betroffenen Personen und das Ausmaß des von ihnen erlittenen Schadens berücksichtigt werden
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
- getroffene Maßnahmen zur Minderung des entstandenen Schadens
- Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen getroffenen technischen und organisatorischen Maßnahmen
- etwaige einschlägige frühere Verstöße
- Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen
- Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind
- Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt bzw. mitgeteilt wurde
- Einhaltung von Maßnahmen, die früher angeordnet wurden
- Einhaltung von genehmigten Verhaltensregeln oder Zertifizierungsverfahren
- andere erschwerende oder mildernde Umstände im jeweiligen Fall

15.4. // WEITERE AUFSICHTSMASSNAHMEN UND SANKTIONEN

Über die Strafe oder Geldbuße hinaus kann eine Gewinnabschöpfung angeordnet werden. Unabhängig hiervon kann eine Anordnung zur Beendigung des Verstoßes in Form eines Verwaltungsakts erfolgen, der zwangsweise durchgesetzt werden kann. Es kann auch ein zeitlich begrenztes oder unbegrenztes Datenverarbeitungsverbot erlassen werden. Alle aufsichtsrechtlichen Maßnahmen sind in Art. 58 geregelt.

15.5. // DURCHSETZUNG DER SANKTIONEN UND AUFSICHTSMASSNAHMEN

Verstöße können unterschiedlich aufgedeckt werden:

- durch Überprüfung der zuständigen Aufsichtsbehörde, z. B. veranlasst durch die betroffene Person
- durch Beschwerde eines Mandanten bzw. Dritten bei der zuständigen Behörde
- durch Selbstanzeige des Unternehmens
- durch Journalismus

Das Durchsetzen von Sanktionen und Aufsichtsmaßnahmen ist Sache der Aufsichtsbehörden im entsprechenden EU-Mitgliedstaat. Bei internationalem Datenaustausch, d. h. grenzüberschreitenden Fällen, in denen der Verantwortliche und die betroffene Person in unterschiedlichen Staaten ansässig sind, ist bezüglich der Aufsichtszuständigkeit Kapitel VII der DS-GVO (Art. 60 ff.) zu beachten.

15.6. // VERSTOSSPRÄVENTION DURCH KONTROLLE UND DOKUMENTATION

Mit einer professionellen Beratung und Überprüfung kann das Risiko von Verstößen gegen die DS-GVO gesenkt werden

Professionelle Beratung, auch durch die für den Verantwortlichen zuständige Aufsichtsbehörde, und die regelmäßige Überprüfung der Einhaltung der DS-GVO helfen bei der Vorbeugung von Verstößen. Dabei sollte dringend auf eine durchgehende und lückenlose Dokumentation insbesondere von Datenquellen und -verarbeitungen geachtet werden, um im Zweifelsfall die korrekte Bearbeitung nachweisen zu können.

16. // RECHTSBEHELFE VON BETROFFENEN PERSONEN

DS-GVO-Regelungen
- *Art. 77: Recht auf Beschwerde bei einer Aufsichtsbehörde*
- *Art. 78: Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde*
- *Art. 79: Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter*
- *Art. 80: Vertretung von betroffenen Personen*
- *Art. 82: Haftung und Recht auf Schadensersatz*

BDSG-Regelung
- *§ 44: Klagen gegen den Verantwortlichen oder Auftragsverarbeiter*

Um gegen einen Verstoß gegen die DS-GVO vorgehen zu können, stehen betroffenen Personen verschiedene Rechtsbehelfe zur Verfügung – sie sind in den Art. 77 bis 82 geregelt.

16.1. // BESCHWERDERECHT BEI DER AUFSICHTSBEHÖRDE

Ist eine betroffene Person der Ansicht, es liege ein Verstoß gegen Regelungen der DS-GVO vor, kann sie bei einer Aufsichtsbehörde Beschwerde einlegen. Die Behörden stellen regelmäßig entsprechende Beschwerdeformulare bereit. Gegen Entscheidungen oder Untätigkeit der Aufsichtsbehörde kann die betroffene Person gerichtlich vorgehen.

16.2. // KLAGE GEGEN DAS UNTERNEHMEN, SCHADENSERSATZ

Betroffene können bei Verstößen gegen den Verantwortlichen der Datenverarbeitung, d. h. gegen den Mandanten bzw. das Inkassounternehmen, oder aber gegen den Auftragsverarbeiter Klage einreichen. Mögliche Klageziele sind: Schadensersatz, Unterlassung, Auskunft, Berichtigung, Löschung und/oder Feststellung. Schadensersatz kann verschuldensunabhängig verlangt werden und umfasst neben materiellen ggf. auch immaterielle Schäden, Art. 82.

16.3. // VERBÄNDE ZUR RECHTSDURCHSETZUNG

Auch wenn die betroffene Person grundsätzlich selbst Rechtsbehelfe einlegen kann, kann sie aber ebenso Einrichtungen, Organisationen oder Vereinigungen mit der Durchsetzung ihrer Rechtsbehelfe und Klageansprüche beauftragen. So können in Deutschland beispielsweise auch Verbraucherverbände die Rechte der betroffenen Person durch Klage durchsetzen. In Deutschland können Klagen wegen Verstößen gegen die DS-GVO sowohl beim Gericht am Sitz des Verantwortlichen als auch am Sitz des Betroffenen eingelegt werden. Eingeklagt werden können materielle und immaterielle Schäden des Betroffenen.

17. // AUFSICHT ÜBER UNTERNEHMEN

DS-GVO-Regelungen
- *Art. 51: Aufsichtsbehörde*
- *Art. 55: Zuständigkeit*
- *Art. 56: Zuständigkeit der federführenden Aufsichtsbehörde*
- *Art. 57: Aufgaben*
- *Art. 58: Befugnisse*
- *Art. 60: Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und den anderen betroffenen Aufsichtsbehörden*
- *Art. 63: Kohärenzverfahren*
- *Art. 68: Europäischer Datenschutzausschuss*
- *Art. 70: Aufgaben des Ausschusses*

BDSG-Regelung
- *§ 40: Aufsichtsbehörden der Länder*

Die DS-GVO regelt umfassend, welche Aufsichtsbehörden in welchem Umfang bei Verstößen zuständig sind. Für grenzüberschreitende Fälle, in denen die Beteiligten also aus unterschiedlichen (EU-)Staaten kommen, regelt die DS-GVO die Zusammenarbeit zwischen den verschiedenen nationalen Aufsichtsbehörden.

17.1. // ZUSTÄNDIGE DATENSCHUTZAUFSICHTSBEHÖRDE

In jedem EU-Mitgliedstaat gibt es eine oder mehrere unabhängige Aufsichtsbehörden, die die Anwendung der DS-GVO überwachen. In Deutschland sind das die bereits bekannten Datenschutzaufsichtsbehörden der einzelnen Bundesländer sowie die (bzw. der) Bundesdatenschutzbeauftragte. Alle Aufsichtsbehörden sind gehalten, auf eine einheitliche Anwendung der DS-GVO zu achten. Damit sollen nationale und regionale Unterschiede bei der Bewertung von datenschutzrechtlichen Fragestellungen vermieden werden.

Für den einzelnen Inkassodienstleister ist die Landesaufsichtsbehörde seiner Hauptniederlassung zuständig. Diese ist »federführend«. Geht eine Beschwerde bei einer anderen Aufsichtsbehörde ein – egal in welchem EU-Mitgliedstaat –, ist diese zwar auch zuständig, sie muss allerdings die »federführende« Aufsichtsbehörde einschalten.

Die Aufgaben sowie die Befugnisse der Aufsichtsbehörden regelt Art. 57 bzw. 58: Sie sind berechtigt, Anweisungen, Hinweise, (Ver-)Warnungen zu erteilen, Verbote auszusprechen, Zertifizierungen zu widerrufen etc. Außerdem sind sie im Fall eines Verstoßes gegen die DS-GVO berechtigt, Geldbußen nach Art. 83 zu verhängen.

17.2. // EUROPÄISCHER DATENSCHUTZAUSSCHUSS

Über den nationalen Aufsichtsbehörden steht der Europäische Datenschutzausschuss (vormals »Art.-29-Gruppe«). In ihm sitzen pro EU-Mitgliedstaat ein Vertreter der nationalen Datenschutzaufsichtsbehörden sowie der Europäische Datenschutzbeauftragte bzw. deren Vertreter.

Aufgabe des Ausschusses ist es u. a., die einheitliche Anwendung der DS-GVO herzustellen und verbindliche Entscheidungen bei Meinungsverschiedenheiten zwischen den nationalen Aufsichtsbehörden zu treffen. Darüber hinaus berät er nach Art. 70 beispielsweise die EU-Kommission, stellt Empfehlungen, Leitlinien und bewährte Verfahren bereit und fördert die Zusammenarbeit und den Austausch zwischen den einzelnen nationalen Aufsichtsbehörden.

18. // BEGRIFFE

DS-GVO-Regelung
- *Art. 4: Begriffsbestimmungen*

Die DS-GVO liefert einen umfangreichen Katalog an Begriffsdefinitionen.

Die Begriffsbestimmungen der DS-GVO befinden sich in Art. 4. Die nachstehenden Begriffe sind maßgeblich für die Inkassounternehmen.

- **Personenbezogene Daten** – alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (= betroffene Person) beziehen. Explizit ist nun auch die Online-Kennung (z. B. IP-Adressen oder Cookie-Kennung) erfasst. Auch pseudonymisierte Daten fallen unter die DS-GVO. Um personenbezogene Daten handelt es sich immer dann, wenn eine Zuordnung möglich ist. Nur bei anonymisierten Daten ist Personenbezug nicht gegeben.
  - Der Begriff umfasst alle Daten lebender natürlicher Personen (= betroffener Personen). Personenbezogene Daten von Verstorbenen unterliegen nicht der DS-GVO. Achtung: Wird im Rahmen der Inkassodienstleistung eine Forderung, die ursprünglich gegenüber einem nunmehr verstorbenen Schuldner bestand, nunmehr gegenüber seinem Erben geltend gemacht, unterliegen die entsprechenden Datenverarbeitungen weiterhin der DS-GVO.
  - Auch pseudonymisierte Daten sind personenbezogene Daten, da durch Hinzunahme weiterer Daten zu den pseudonymisierten die Zuordnung zu einer bestimmten Person weiterhin möglich ist.

- **Eine betroffene Person** ist jede natürliche Person, mit der ein Verantwortlicher, also z. B. ein Inkassounternehmen, zu tun hat oder auf die sich die Informationen, die ein Inkassounternehmen verarbeitet, sonst wie beziehen. Die meisten betroffenen Personen der Datenverarbeitungen von Inkassounternehmen sind Schuldner offener Forderungen. Aber auch die Mandanten der Inkassounternehmen, sofern es sich um Einzelpersonen handelt, sind betroffene Personen, genauso wie z. B. die Mitarbeiter im Unternehmen, Einzelfirmen sowie Betreuer, Rechtsanwälte, Arbeitgeber, Bevollmächtigte betroffene Personen sein können.

- **Verarbeitung** – jede/-r mit oder ohne Hilfe automatisierter Verfahren ausgeführte/-r Vorgang bzw. Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Der Begriff umfasst alle Vorgänge wie z. B. die Erhebung, das Speichern, das Verwenden, die Auswertung und die Offenlegung von Daten.

- **Einschränkung der Verarbeitung** – das Markieren von personenbezogenen Daten mit dem Ziel der zukünftigen Einschränkung der Verarbeitung (»Sperrung«).

- **Profiling** – jede Art automatisierter Verarbeitung personenbezogener Daten, um eine Verwendung persönlicher Aspekte, z. B. wirtschaftliche Lage, Aufenthaltsort oder Ortswechsel, zu bewerten.

- **Pseudonymisierung** – Verarbeitung personenbezogener Daten dergestalt, dass ohne Hinzuziehung zusätzlicher Informationen die Daten nicht mehr einer bestimmten betroffenen Person zugeordnet werden können. Voraussetzung ist aber, dass diese gesondert aufbewahrt und somit geschützt sind. Das Pseudonymisieren unterstützt den Verantwortlichen sowie den Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten. Die vorschriftsgemäße Pseudonymisierung ermöglicht das Nutzen von Daten innerhalb eines Unternehmens bzw. einer Unternehmensgruppe. Es sind dann aber technisch-organisatorische Maßnahmen zu ergreifen, die sicherstellen, dass keine Zuordnung/Identifizierung erfolgen kann.

- **Anonymisierung** – solche Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.
  - **Ein Verantwortlicher für die Verarbeitung** ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Bereich des Forderungsmanagements trifft genau das auf Inkassodienstleister zu. Sie entscheiden selbst über den Zweck und die Mittel der Verarbeitung. Sie sind damit Verantwortliche im Sinne der DS-GVO.
  - **Ein Auftragsverarbeiter** ist hingegen eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die im Auftrag eines Verantwortlichen personenbezogene Daten der betroffenen Person verarbeitet. Unter der DS-GVO hat der Auftragsverarbeiter künftig umfangreichere Pflichten zu erfüllen als unter der bis zum 24. Mai 2018 geltenden Fassung des BDSG.

- **Empfänger** – eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden – egal ob es sich um einen Dritten handelt oder nicht.

- **Dritter** – eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle. Ausgenommen sind damit die betroffene Person, der Verantwortliche, der Auftragsverarbeiter und Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder Auftragsverarbeiters (z. B. Mitarbeiter) befugt sind, personenbezogene Daten zu verarbeiten.

- **Gesundheitsdaten** – personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person (Achtung: nicht nur der betroffenen Person), einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Kann für Inkassounternehmen relevant sein, soweit eine Forderungsbearbeitung für Mandanten aus dem Bereich der Heilberufe erfolgt, oder wenn Mitarbeiter-/Bewerberdaten verarbeitet werden.

- **Aufsichtsbehörde** – unabhängige, staatliche Stelle zur Datenschutzaufsicht.

IMPRESSUM

Die Europäische Datenschutz-Grundverordnung – Best Practice Guide 2.0
Oktober 2019

Herausgeber
Bundesverband Deutscher Inkasso-Unternehmen e. V.
Friedrichstraße 50–55 // 10117 Berlin
Telefon +49 30.206 07 36-0
bdiu@inkasso.de // www.inkasso.de

Verfasser
BDIU-Datenschutzausschuss:
Thomas Schauf (Vorsitzender),
Sylvia Mundt (stv. Vorsitzende),
Thomas Bürck, Ingeborg Kaven-Mahler,
Nils Unverhau, Thomas Stemmer,
Prof. Dr. Ralf B. Abel
Verbandsbeauftragter für den Datenschutz des BDIU:
Dr. Gero Ziegenhorn
BDIU-Geschäftsstelle:
Daniela Gaub (Leiterin Recht)

Konzept + Gestaltung
Nolte | Kommunikation

Bildnachweis
shutterstock.com/nale