BUNDESNOTARKAMMER

GESCHÄFTSFÜHRUNG

BERLIN, den 11. Mai 2018

Unser Zeichen: sb / E 22 / R 30-07

An alle
Notarkammern

Nachrichtlich an:

das Präsidium der Bundesnotarkammer

die Notarkasse

die Ländernotarkasse

das Deutsche Notarinstitut

Rundschreiben Nr. 5/2018
Datenschutz im Notariat – Inkrafttreten der Datenschutz-Grundverordnung

Sehr geehrte Damen und Herren Kolleginnen und Kollegen,

ab dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (Verordnung (EU) 2016/679)[1] in allen Mitgliedstaaten der Europäischen Union. Diese Verordnung enthält Regelungen, die auch die Notarinnen und Notare in Deutschland unmittelbar betreffen. Denn Notare sind nach allgemeiner Ansicht öffentliche Stellen der Länder und „Verantwortliche" im Sinne von Art. 4 Nr. 7 der DSGVO. Sie sind damit verpflichtet, personenbezogene Daten von natürlichen Personen als Beteiligte im notariellen Verfahren (im Folgenden auch „betroffene Person" oder „Betroffener") zu schützen.

Die aus notarieller Sicht wichtigsten Regelungen aus der DSGVO und ihre Folgen für die Praxis lassen sich überblickartig wie folgt zusammenfassen:

[1] Im Folgenden kurz DSGVO.

Sitz: Mohrenstraße 34, D-10117 Berlin, Telefon (0 30) 38 38 66 - 0, Telefax (0 30) 38 38 66 - 66, e-mail: bnotk@bnotk.de
Büro Brüssel: Avenue de Cortenbergh 172, B-1000 Bruxelles, Telefon (0032) (2) 737 90 00, Telefax (0032) (2) 737 90 09, e-mail: buero.bruessel@bnotk.de

- **Informationspflichten nach Art. 13 DSGVO**

Der Betroffene soll einen Überblick darüber erhalten, was mit seinen Daten geschieht, um von Beginn der Datenverarbeitung an über die Konsequenzen der Datenübermittlung an den Verantwortlichen informiert zu sein. Aus Art. 13 DSGVO folgt somit die Pflicht des Notars, dem Beteiligten bestimmte Informationen hinsichtlich der Verarbeitung von dessen personenbezogenen Daten zukommen zu lassen.

Die einzelnen Informationen, die dem Betroffenen zur Verfügung gestellt werden müssen, sind in Art. 13 Abs. 1 und 2 DSGVO aufgelistet.

Weitergehende Hinweise zu diesem Punkt finden Sie unter C. II. 2. dieses Rundschreibens.

- **Benennung eines Datenschutzbeauftragten, Art. 37 DSGVO**

Art. 37 DSGVO beschreibt die Pflicht des Verantwortlichen zur Benennung eines Datenschutzbeauftragten. Notare als öffentliche Stellen der Länder sind unabhängig von der Anzahl der Mitarbeiter in der notariellen Geschäftsstelle zur Bestellung eines Datenschutzbeauftragten verpflichtet. Wie die Benennungspflicht in der Praxis am besten zu erfüllen ist, hängt von der Art und der Ausstattung der jeweiligen Notarstelle ab. Grundsätzlich ergeben sich verschiedene Optionen, um der Benennungspflicht nachzukommen:
Es ist zum einen möglich, einen Mitarbeiter des Notars als „internen Datenschutzbeauftragten“ zu benennen, der über eine besondere Qualifikation im Bereich des Datenschutzrechts verfügen muss. Zum anderen besteht die Möglichkeit, einen „externen Datenschutzbeauftragten“ zu benennen. Hierfür gibt es eine Vielzahl von kommerziellen Anbietern, die unterschiedliche Angebote vorhalten.

Weitergehende Hinweise zu diesem Punkt finden Sie unter C. III. 7. dieses Rundschreibens.

- **Verzeichnis der Verarbeitungstätigkeiten**

Aus Art. 30 DSGVO ergibt sich die Pflicht des Notars zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten. Die Verzeichnisse müssen gemäß Art. 30 Abs. 3 DSGVO schriftlich geführt werden, wobei auch ein elektronisches Format verwendet werden kann.

Weitergehende Hinweise zu diesem Punkt finden Sie unter C. III. 4. dieses Rundschreibens.

- **Sicherheit der Verarbeitung und technische und organisatorische Maßnahmen**

Nach Art. 32 DSGVO ist der Notar verpflichtet, geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu treffen.

Welche Maßnahmen im konkreten Einzelfall zu treffen sind, hängt ganz wesentlich von der Struktur der jeweiligen Notarstelle ab. Hier ist insbesondere in Zusammenarbeit mit dem Datenschutzbeauftragten des Notars ein individuelles Schutzkonzept zu erarbeiten, das die Arbeitsabläufe in der jeweiligen Amtsstelle angemessen berücksichtigt.

Weitergehende Hinweise zu diesem Punkt finden Sie unter C. III. 5. dieses Rundschreibens.

Im Einzelnen:

A. Die neuen Normen des Datenschutzrechts

I. Die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung gilt unmittelbar in allen Mitgliedstaaten der Europäischen Union. Sie schafft durch Vollharmonisierung ein einheitliches europäisches Datenschutzniveau (vgl. Erwägungsgrund 10 der DSGVO). In einigen Regelungsbereichen räumt der europäische Gesetzgeber den Mitgliedstaaten jedoch die Möglichkeit ein, weitere Einzelheiten selbst oder auch abweichend zu regeln.

II. Das Bundesdatenschutzgesetz (BDSG) (neu)

Von der Möglichkeit, einzelne Regelungsbereiche selbst auszufüllen, hat der deutsche Gesetzgeber durch das neue Bundesdatenschutzgesetz (BDSG-neu) Gebrauch gemacht, das zeitgleich mit der DSGVO in Kraft tritt. Es gilt für die öffentlichen Stellen des Bundes und die öffentlichen Stellen der Länder, soweit der Datenschutz nicht durch Landesrecht geregelt ist, vgl. § 1 Abs. 1 Nr. 1 und Nr. 2 BDSG-neu.

III. Die Datenschutzgesetze der Länder

Die Datenschutzgesetze der Länder gehen im Rahmen ihres Anwendungsbereichs den Regelungen des Bundesdatenschutzgesetzes vor. Da Notare nach allgemeiner Ansicht

öffentliche Stellen der Länder sind (BGHZ 112, 178, 181), gelten für sie neben der Datenschutz-Grundverordnung die jeweiligen Landesdatenschutzgesetze.

Im Rahmen der Datenschutzgesetze wird stets der einzelne Amtsträger verpflichtet. Dies gilt auch für Notare, die in Sozietät oder Bürogemeinschaften verbunden sind. Eine gemeinsame Planung und Festlegung der organisatorischen Maßnahmen zur Umsetzung eines effektiven Datenschutzniveaus innerhalb einer Geschäftsstelle ist jedoch möglich und in der Regel auch sinnvoll. Notare, die weitere Geschäftsstellen unterhalten, haben den Datenschutz bezogen auf ihre Amtstätigkeit insgesamt sicherzustellen und müssen deswegen nicht zwischen den einzelnen Geschäftsstellen differenzieren.

B. Anwendungsbereich der Datenschutz-Grundverordnung

Gemäß Art. 2 DSGVO gilt die Datenschutz-Grundverordnung grundsätzlich für alle Datenverarbeitungsvorgänge, die sich auf personenbezogene Daten beziehen.

Der Begriff der personenbezogenen Daten ist in Art. 4 Nr. 1 DSGVO definiert. Dabei handelt es sich um *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen.* Dazu zählen etwa die Kontaktdaten der Beteiligten einschließlich ihrer Telefonnummern und E-Mail-Adressen, die Kontoangaben (IBAN) sowie die Steueridentifikationsnummer.

Unter Verarbeitung ist gem. Art. 4 Nr. 2 DSGVO jeder Umgang mit personenbezogenen Daten wie das Erheben, die Speicherung, die Verwendung, die Offenlegung durch Übermittlung, das Löschen oder die Vernichtung gemeint.

Es kommt dabei nicht darauf an, wie diese Daten verarbeitet werden: Sowohl analoge Verarbeitungsvorgänge (die handschriftliche Aufnahme personenbezogener Daten), als auch elektronische Verarbeitungen werden erfasst.

Es ist im Ergebnis davon auszugehen, dass bei sämtlichen notariellen Amtstätigkeiten jeweils personenbezogene Daten durch den Amtsträger verarbeitet werden.

C. Pflichten bei der Ausübung notarieller Amtstätigkeit

Im Folgenden werden die einzelnen aus der Datenschutz-Grundverordnung folgenden Pflichten bei der Ausübung notarieller Amtstätigkeit anhand der Grundsätze für die Verarbeitung personenbezogener Daten näher erläutert.

I. Grundsätze für die Verarbeitung personenbezogener Daten

Die Grundsätze der Datenverarbeitung regelt Art. 5 Abs. 1 DSGVO. Dabei handelt es sich in weiten Teilen um Grundsätze, die auch schon unter dem bisher geltenden Recht bei der Datenverarbeitung zu beachten waren und die die Gesamtheit der Schutzmaßnahmen prägen.

1. Grundsatz der Rechtmäßigkeit der Verarbeitung, Verarbeitung nach Treu und Glauben, Transparenz

a) Rechtmäßigkeit – Verbot mit Erlaubnisvorbehalt

Für die Verarbeitung personenbezogener Daten gilt ein Verbot mit Erlaubnisvorbehalt. Im Rahmen der notariellen Amtstätigkeit ergibt sich die Zulässigkeit der Datenverarbeitung in der Regel aus den Erlaubnistatbeständen des Art. 6 Abs. 1 lit. c) und e) DSGVO.

Gemäß Art. 6 Abs. 1 lit. e) DSGVO ist die Datenverarbeitung rechtmäßig, wenn diese für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Notare sind Träger eines öffentlichen Amtes und nehmen als solche hoheitliche Aufgaben wahr. Ihre Aufgaben liegen damit im öffentlichen Interesse.

Gemäß Art. 6 Abs. 3 Satz 1 DSGVO kann die Rechtsgrundlage für Verarbeitungen, die für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich sind, durch das Unionsrecht oder das Recht des Mitgliedstaates festgelegt werden, dem der Verantwortliche unterliegt. Für die notarielle Amtstätigkeit kommen hier insbesondere die Regelungen des notariellen Berufs- und Verfahrensrechts, namentlich der Bundesnotarordnung und des Beurkundungsgesetzes, in Betracht, da sie Regelungen zum Umgang des Notars mit personenbezogenen Daten enthalten. Auch die Vorschriften der Dienstordnung für Notarinnen und Notare konkretisieren die Amtspflichten des Notars beim Umgang mit personenbezogenen Daten. Sie sind somit relevant für die Frage, welche Verarbeitungsvorgänge für die Wahrnehmung der öffentlichen Aufgaben des Notars erforderlich sind.

Art. 6 Abs. 1 lit. c) DSGVO gestattet die Datenverarbeitung immer dann, wenn die Verarbeitung erforderlich ist, um eine rechtliche Verpflichtung, der der Verantwortliche unterliegt, zu erfüllen. Da den Notaren als externe staatliche Hoheitsträger bestimmte hoheitliche Aufgaben vom Staat übertragen worden sind, die durch besondere rechtliche Pflichten konkretisiert werden, ist jede von ihnen vorgenommene Datenver-

arbeitung zulässig, die zur Erfüllung dieser Aufgaben erforderlich ist. Wenn demnach durch den Notar Daten bei der Ausübung der Amtstätigkeit verarbeitet werden, sind (vorbehaltlich weiterer Schranken der Verarbeitung, wie zum Beispiel der Beachtung der Grundsätze der Datensparsamkeit oder der Sicherheit der Verarbeitung) die erforderlichen Datenverarbeitungsvorgänge sowohl nach nationalem Recht als auch nach der Datenschutz-Grundverordnung gestattet. Erforderlich ist insbesondere jede Datenverarbeitung, die durch das Beurkundungsgesetz vorgeschrieben wird. So folgt aus der Pflicht zur Willenserforschung und Klärung des Sachverhalts aus § 17 Abs. 1 BeurkG und der damit verbundenen umfänglichen Einschätzungsprärogative des Notars die Zulässigkeit zur Erhebung und Verarbeitung aller personenbezogenen Daten, die aus Sicht des Notars zur von den Parteien gewollten und rechtlich zutreffenden Behandlung des Sachverhalts erforderlich sind.

Lediglich ausnahmsweise, beispielsweise soweit der Notar Daten erhebt, die für die Ausübung der notariellen Amtstätigkeit nicht erforderlich sind, bedarf es der Einwilligung der Beteiligten gemäß Art. 6 Abs. 1 lit. a) DSGVO. Das dürfte angesichts der Pflicht des Notars im Rahmen des § 17 Abs. 1 BeurkG den Sachverhalt aufzuklären nur selten der Fall sein. Sollte es ausnahmsweise einer Einwilligung bedürfen, sind die Anforderungen des Art. 7 DSGVO zu beachten. Eine Einwilligung sollte nur in diesen Ausnahmefällen eingeholt werden. Andernfalls erweckt der Notar die Fehlvorstellung, dass die Zulässigkeit der Verarbeitung von der widerruflichen Einwilligung des Betroffenen abhängig ist.

Auch soweit aufgrund der genannten Tatbestände die Datenverarbeitung an sich zulässig ist, ist dies keine Rechtfertigung zur grenzenlosen Datenverarbeitung, sondern hat der Notar bei der Datenverarbeitung die nachfolgend dargestellten Grundsätze zu beachten.

b) Verarbeitung nach Treu und Glauben und Transparenzgebot

Nach Art. 5 Abs. 1 lit. a) DSGVO müssen personenbezogene Daten nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Jede Verarbeitung soll für die betroffenen Personen vorhersehbar und nachvollziehbar sein. Das schließt insbesondere eine Information der betroffenen Personen darüber ein, wer für die Datenverarbeitung verantwortlich ist, zu welchem Zweck erhobene Daten verarbeitet werden und welche Rechte den betroffenen Personen im Hinblick auf die erfolgte Datenverarbeitung zustehen (vgl. Erwägungsgrund 39 der DSGVO). Dieses abstrakte Gebot wird bei den einzelnen Informations- und Auskunftspflichten von der DSGVO wieder aufgegriffen.

2. Grundsatz der Zweckbindung

Art. 5 Abs. 1 lit. b) DSGVO normiert den sog. Grundsatz der Zweckbindung. Danach darf jede Datenerhebung nur zu einem (oder mehreren) zuvor festgelegten Zweck(en) erfolgen. Eine Weiterverarbeitung zu einem anderen Zweck als demjenigen, zu dem die Erhebung erfolgt war, ist unzulässig.

Damit soll ausgeschlossen werden, dass Daten (gewissermaßen bei Gelegenheit) gesammelt werden, um sie für erst später eintretende Zwecke verwenden zu können.

Dies bedeutet für die notariellen Verarbeitungstätigkeiten grundsätzlich, dass der Notar bereits die Erhebung von personenbezogenen Daten daran auszurichten hat, ob er diese Daten auch tatsächlich für den mit dem jeweiligen Amtsgeschäft angestrebten Zweck benötigt. Aufgrund von § 17 Abs. 1 BeurkG ist der Notar allerdings zur Aufklärung und damit einhergehenden Datenerhebung und -verarbeitung verpflichtet.

3. Grundsatz der Datenminimierung

Gemäß Art. 5 Abs. 1 lit. c) DSGVO müssen die Erhebung, aber auch jede weitere Verarbeitung von Daten, etwa deren Speicherung, auf das notwendige Maß beschränkt sein und sich an dem mit der Erhebung verfolgten Zweck orientieren. In Ergänzung zum Grundsatz der Zweckbindung soll damit erreicht werden, dass nicht nur inhaltlich, sondern auch hinsichtlich der Datenmenge eine Verarbeitung auf Vorrat nicht erfolgt.

4. Grundsatz der Datenrichtigkeit

Nach Art. 5 Abs. 1 lit. d) DSGVO müssen personenbezogene Daten – jedoch immer mit Blick auf die Zwecke ihrer Verarbeitung – sachlich richtig und auf dem neuesten Stand sein; unrichtige Daten sind unverzüglich zu berichtigen oder zu löschen.

Das bedeutet, dass der Notar durch geeignete und angemessene Maßnahmen sicherzustellen hat, dass bei ihm gespeicherte Daten korrigiert oder gelöscht werden, wenn er von deren Unrichtigkeit Kenntnis erlangt. Das gilt jedoch nur, soweit es im Hinblick auf den jeweiligen Zweck der Verarbeitung erforderlich ist. Näheres dazu siehe unter C. II. 5. und 6.

5. Grundsatz der Speicherbegrenzung

Nach Art. 5 Abs. 1 lit. e) DSGVO darf die Speicherung von personenbezogenen Daten im Grundsatz nur so lange erfolgen, wie dies für die Zwecke der Datenverarbeitung er-

forderlich ist. In Zusammenschau mit dem Grundsatz der Datenminimierung und dem Grundsatz der Zweckbindung folgt aus dem Grundsatz der Speicherbegrenzung auch, dass die Verarbeitung rechtmäßig und zweckgerichtet erhobener Daten rechtswidrig sein oder werden kann, wenn die erhobenen Daten in unzulässiger und nicht erforderlicher Weise weiterverarbeitet (zum Beispiel unnötig vervielfältigt) werden.

Beispiel:

Im Vorfeld der Beurkundung eines Testaments fragt der Notar den Beteiligten nach zahlreichen personenbezogenen Daten, unter anderem danach, wen der Beteiligte als Erben einsetzen will, wie viele Kinder der Beteiligte hat und ob er verheiratet ist. Der Beteiligte teilt im Anschluss an die Besprechung weitere Daten schriftlich mit. Sodann fertigt der Notar den Entwurf eines Testaments und versendet dieses an den Beteiligten. Die Grundsätze der Datenminimierung und der Begrenzung der Speicherung erfordern es, die Daten nicht an vielen verschiedenen Orten, sondern möglichst komprimiert und einheitlich, in der Regel zentral in der Nebenakte, abzulegen.

6. Integrität und Vertraulichkeit der Daten

Art. 6 Abs. 1 lit. f) DSGVO beschreibt die später an anderer Stelle in der DSGVO noch weiter konkretisierte Pflicht, personenbezogene Daten in einer Weise zu verarbeiten, die eine angemessene Sicherheit und einen angemessenen Schutz vor dem Verlust und der Beschädigung gewährleistet. Hierzu gehören beispielsweise die notwendigen technischen und organisatorischen Maßnahmen (Art. 32 DSGVO). Der Notar soll die bei ihm eingesetzte Technik und die bei ihm etablierten Datenverarbeitungsprozesse so gestalten, dass die Integrität und Vertraulichkeit der Daten gewährleistet ist. Dies beinhaltet nicht nur die bereits nach § 18 BNotO bestehende Pflicht, sich einer Offenbarung von Kenntnissen über Betroffenendaten zu enthalten. Vielmehr bedeutet die Pflicht zur Wahrung der Integrität der Daten auch, dass der Notar die ihm anvertrauten Daten dahingehend zu schützen hat, dass weder durch unbefugtes Eingreifen Dritter noch durch fahrlässiges Verhalten des Notars oder seiner Mitarbeiter selbst die Daten in ihrem Bestand und ihrer Richtigkeit beeinträchtigt werden. Welche Maßnahmen konkret in der einzelnen notariellen Amtsstelle umgesetzt werden müssen, hängt von ihrer jeweiligen Struktur ab. Es ist eine Aufgabe des Datenschutzbeauftragten des Notars in Absprache mit dem Amtsträger, den Handlungsbedarf zu ermitteln und ein System zur sicheren Verarbeitung in der Geschäftsstelle zu implementieren.[2]

[2] Hierzu folgen weitere Hinweise unter C. III. 5.

7. Eingeschränkte Verarbeitungserlaubnis bei besonderen Kategorien personenbezogener Daten

Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt. Dazu zählen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Beispiele:

Der Notar zieht bei der Beurkundung eines Testaments einen zweiten Notar hinzu, da der Erblasser stark sehbehindert ist. Entsprechend der Regelung in § 22 Abs. 1 Satz 2 BeurkG vermerkt der Notar den Umstand der Hinzuziehung des zweiten Notars und der Sehbehinderung des Testierenden in der Niederschrift.

Der Notar beurkundet ein sog. „Behindertentestament" von Eheleuten betreffend ihren behinderten Sohn. Nach Aufklärung des Sachverhalts und der Erforschung des Willens der Beteiligten notiert er den Sachverhalt in der Nebenakte und nimmt ihn auch in die Niederschrift der letztwilligen Verfügung auf.

Hier werden durch Beschreibung der körperlichen Einschränkung in der Nebenakte und Niederschrift Gesundheitsdaten verarbeitet.

Gemäß Art. 9 Abs. 2 lit. g) DSGVO ist eine Verarbeitung solcher Daten zulässig, wenn dies auf der Grundlage des Rechts eines Mitgliedstaates erfolgt und dieses Recht in einem angemessenen Verhältnis zu dem verfolgten Ziel der Verarbeitung steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht und die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.

Dort, wo der Notar im Rahmen des nationalen Rechts (insbesondere zum Beispiel gemäß der Regelungen der §§ 11, 17, 22 ff., 28 BeurkG) tätig wird, um die Interessen der Rechtsuchenden zu wahren, erfolgt die Verarbeitung der Betroffenendaten aus Gründen eines erheblichen öffentlichen Interesses und ist damit gem. Art. 9 Abs. 2 lit. g) DSGVO auch ohne Einwilligung des Betroffenen zulässig. Im Bereich der notariellen Tätigkeit dient nämlich die Verarbeitung dieser besonderen Kategorien perso-

nenbezogener Daten dazu, dem Rechtsuchenden Schutz und Rechtssicherheit zu bieten, in den Fällen der §§ 11, 22 ff., 28 BeurkG insbesondere, die Beteiligten und den Rechtsverkehr allgemein vor möglichen Streitigkeiten über die Geschäftsfähigkeit eines Beteiligten zu schützen, die Beurkundung unwirksamer Rechtsgeschäfte zu verhindern und die Beweiskraft von und das Vertrauen auf den öffentlichen Glauben notarieller Urkunden insoweit zu schützen. Der Notar sorgt gerade durch die strikte Einhaltung der Vorgaben des BeurkG und der BNotO dafür, dass die Rechtsuchenden effektiven Rechtsschutz erlangen und bestmöglich sowie umfangreich beraten sind. Eben dieses Ziel erkennt auch die Datenschutz-Grundverordnung an. Aus der inhaltlichen und systematischen Verzahnung von Art. 9 Abs. 2 lit. g) und dem allgemeinen Erlaubnistatbestand des Art. 6 Abs. 1 lit. c) und lit. e) wird deutlich, dass der durch öffentliche Verfahren gewährleistete Schutz betroffener Personen auch im Rahmen der Verarbeitung ihrer personenbezogenen Daten im Sinne des Art. 9 Abs. 1 DSGVO Berücksichtigung findet. Gleichzeitig gewährt das nationale Recht durch die strafbewehrte notarielle Verschwiegenheitspflicht gemäß § 18 BNotO (vgl. auch die Parallelwertung in Art. 9 Abs. 3 DSGVO) einen angemessenen Schutz der betreffenden Daten.

Allerdings sind die Regelungen des notariellen Berufs- und Verfahrensrechts angesichts des Ausnahmecharakters des Art. 9 Abs. 2 lit. g) DSGVO und der besonderen Sensibilität der entsprechenden Beteiligtendaten verordnungskonform eng auszulegen. Der Notar muss unter dem Gesichtspunkt der Datensparsamkeit darauf achten, dass sensible Daten ausschließlich in dem Umfang verarbeitet werden, der nach dem Gesetz erforderlich ist.

II. Rechte der betroffenen Personen

Kapitel III der Datenschutz-Grundverordnung enthält die Rechte der betroffenen Personen. Im Folgenden werden einige dieser Rechte im Hinblick auf die notarielle Amtstätigkeit näher dargestellt.

1. Transparente Information der Betroffenen und Verfahren bei der Geltendmachung von Betroffenenrechten

Art. 12 DSGVO beinhaltet den Leitgedanken einer transparenten Darstellung der Betroffenenrechte durch den Verantwortlichen. Die Vorschrift enthält zum einen Regelungen zur Transparenz und zum anderen zum Verfahren der Geltendmachung der Betroffenenrechte.

a) Regelungen zur transparenten Information

Gemäß Art. 12 Abs. 1 Satz 1 DSGVO ist der Notar verpflichtet, geeignete Maßnahmen zu treffen, um die nach Artt. 13 und 14 DSGVO zu erteilenden Informationen und die nach den Artt. 15 bis 22 und 34 DSGVO zu erteilenden Mitteilungen in präziser, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Unabhängig von den Inhalten der einzelnen Auskunfts-, Mitteilungs- und Informationspflichten trägt die Vorschrift dafür Sorge, dass der Betroffene eine möglichst exakte Darstellung über die Datenverarbeitung und seiner diesbezüglichen Rechte erhält. Daneben soll die Information des Betroffenen für diesen leicht verständlich sein

Beispiel:

Der Notar möchte die Beteiligten eines Ehegattentestaments über die für die Amtstätigkeit erforderliche Datenverarbeitung informieren. Hierzu hält er einen Vordruck bereit, den er den Parteien nach einer persönlichen Vorbesprechung mitgibt. Dieser Vordruck erläutert unter anderem die Aufbewahrungsfristen für alle Aktenbestandteile sowie die Speicher- und Löschvorgänge bezüglich der personenbezogenen Daten innerhalb des Zentralen Testamentsregisters und bei den Standesämtern und Gerichten.

Hierbei ist zu beachten, dass die Informationspflicht nach Art. 12 Abs. 1 DSGVO keine juristisch exakte Darstellung der Verarbeitung in allen Einzelheiten voraussetzt. Der Notar muss vielmehr die Information so gestalten, dass der jeweilige Beteiligte nach seinem Verständnishorizont abschätzen kann, welche Bedeutung die Verarbeitung seiner Daten für ihn hat. Dementsprechend ist der Pflicht zur transparenten Information ein Gestaltungsspielraum des Verantwortlichen immanent.

b) Regelungen zum Verfahren der Informationsbereitstellung

Nach Art. 12 Abs. 2 DSGVO ist der Notar verpflichtet, den betroffenen Personen die Ausübung ihrer Rechte nach Artt. 15 bis 22 DSGVO zu erleichtern. Die einzelnen Informationspflichten werden aus Gründen der Übersichtlichkeit im Folgenden direkt bei den jeweiligen Ansprüchen und Rechten der Betroffenen dargestellt.

2. Informationspflicht im Fall der Datenerhebung bei der betroffenen Person

a) Inhalt der Informationen

Die einzelnen Informationen, die der Notar den Beteiligten zur Verfügung zu stellen hat, ergeben sich aus Art. 13 Abs. 1 und 2 DSGVO. Dazu gehören unter anderem der

Name und die Kontaktdaten des Verantwortlichen, die Kontaktdaten des Datenschutzbeauftragten, die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung und die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten. Grundsätzlich lassen sich für den Bereich der notariellen Tätigkeiten viele Datenverarbeitungsvorgänge zusammenfassen und daher auch standardisierte Informationen bereithalten.

b) Form und Zeitpunkt der Information

Datenerhebung im Sinne des Art. 13 Abs. 1 und 2 DSGVO meint den Beginn des Verarbeitungsprozesses. Gemeint ist also die erste Übermittlung durch den Betroffenen an den Notar. Bereits bei der ersten Kontaktaufnahme (zum Beispiel der Vereinbarung eines Beratungs-/Besprechungstermins) werden Daten von den Beteiligten an den Notar übermittelt. Die Daten werden bei der betroffenen Person erhoben, wenn diese dem Notar die Daten mitteilt und die Daten die mitteilende Person selbst betreffen. Die Schwierigkeit der ersten Information des Betroffenen zeigt sich an folgendem Beispiel:

Der spätere Urkundsbeteiligte ruft in der notariellen Geschäftsstelle an und vereinbart mit dem Mitarbeiter am Empfang einen Termin zur Besprechung eines Testaments. Hierzu fragt der Mitarbeiter mindestens den Namen des Mandanten und dessen Telefonnummer für spätere Rückfragen ab. Weitere Informationen (Geburtsdatum, Adresse etc.) werden dem Notar erst im persönlichen Besprechungstermin übermittelt.

Bereits mit der Eintragung des Besprechungstermins im Kalender des Notars werden personenbezogene Daten (im Beispiel Name und Telefonnummer) verarbeitet.

Grundsätzlich müssen bereits bei Beginn des Verarbeitungsprozesses die in Art. 13 DSGVO näher bezeichneten Informationen an die Beteiligten erteilt werden (Art. 13 Abs. 1 und 2). Die Informationspflichten sind gemäß Art. 13 Abs. 4 DSGVO jedoch dahingehend eingeschränkt, dass eine Information dann nicht zu erfolgen hat, wenn die betroffene Person bereits über die Informationen bezüglich des konkreten Verarbeitungsvorgangs verfügt. Für den Beispielsfall bedeutet dies, dass eine Aufnahme der Daten zur Planung eines Besprechungstermins auch ohne vorherige Informationsübermittlung des Notars möglich ist, da der Betroffene weiß, dass seine Daten (zunächst) nur zur Planung eines von ihm gewünschten Besprechungstermins gespeichert werden.

Spätestens im Besprechungstermin hat dann jedoch eine Information gemäß Art. 13 Abs. 1 und Abs. 2 DSGVO über die Verarbeitung der in diesem Zusammenhang erho-

benen weiteren Daten zu erfolgen. Für alle Fälle notarieller Tätigkeit bietet es sich insofern regelmäßig beim Erstkontakt mit dem Beteiligten an, die erforderlichen Informationen zu erteilen. Dies kann beispielweise wie folgt erfolgen:

Im Rahmen einer Unterschriftsbeglaubigung wird dem Beteiligten nicht nur das Original mit Beglaubigungsvermerk sondern auch gleichzeitig ein Hinweisblatt zum Datenschutz ausgehändigt.

Die Beteiligten eines Grundstückskaufvertrages, die noch nicht persönlich zu diesem Geschäft an der notariellen Geschäftsstelle anwesend waren, erhalten gleichzeitig mit dem Entwurf des Vertrages das Hinweisblatt zum Datenschutz.

Grundsätzlich ist auch eine elektronische Bereitstellung der Datenschutzhinweise (zum Beispiel auf der Website des Notars) möglich. Diese kommt vorrangig in Betracht, wenn die wesentlichen Informationen auf diese Weise gewonnen wurden. Auch in weiteren Fallkonstellationen kann ein entsprechender Verweis auf Datenschutzhinweise auf der Website sachgerecht sein, etwa in der Fußzeile von Schreiben des Notars oder durch einen mündlichen Hinweis. Nur wenn die ausschließliche elektronische Bereitstellung erkennbar eine Informationsbarriere für den Beteiligten darstellt, sollte hiervon abgesehen werden.

Für das erste oben genannte Beispiel bedeutet das:

Der Mitarbeiter, der den Termin mit dem Beteiligten vereinbart, muss noch keine Informationen zur Datenverarbeitung erteilen. Der Notar muss dem Beteiligten aber zum Zeitpunkt des Besprechungstermins die entsprechenden Informationen zur Verfügung stellen.

3. Information bei anderweitiger Datenerhebung

Art. 14 DSGVO betrifft die Informationspflicht des Notars in den Fällen, in denen er die Daten nicht von den Beteiligten erhoben hat. Gemäß Art. 14 Abs. 1, 2, 3 DSGVO sind die betroffenen Personen, deren Daten nicht unmittelbar bei ihnen erhoben wurden, vom Verantwortlichen innerhalb einer angemessenen Frist, längstens jedoch innerhalb eines Monats und spätestens bei der ersten Kontaktaufnahme, über die Datenerhebung und die Verantwortlichkeit zu informieren.

Hier sind mehrere Fälle denkbar, die unterschiedlich zu behandeln sind:

Beispiel 1:

Ein Immobilienmakler nimmt Kontakt zum Notar auf und bittet im Namen der Beteiligten um Erstellung eines Grundstückskaufvertrages sowie um Kontaktaufnahme mit den Beteiligten zwecks Besprechung des weiteren Vorgehens. Dabei übermittelt er dem Notar personenbezogene Daten der Beteiligten.

Im Beispielsfall empfiehlt es sich für den Notar, den Parteien spätestens mit der Übersendung des Vertragsentwurfs die entsprechenden Datenschutzhinweise zu erteilen. Eine vorherige Information ist nicht erforderlich, da die Erstellung und Übermittlung eines Vertragsentwurfs in der Regel innerhalb einer angemessenen Frist im Sinne von Art. 14 Abs. 3 lit. a) DGSVO erfolgen dürfte.

Beispiel 2:

Der Erblasser benennt seinen Neffen als Alleinerben. Hierzu teilt er dem Notar dessen Namen, Anschrift und Geburtsdatum mit.

Gemäß Art. 14 Abs. 5 lit. d) DSGVO muss eine Information an den Betroffenen dann nicht erfolgen, wenn die Datenverarbeitung nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten dem Berufsgeheimnis unterliegt. Entsprechende Regelungen finden sich in § 29 Abs. 1 Satz 1 BDSG-neu sowie in den Landesdatenschutzgesetzen. Sofern die Landesdatenschutzgesetze hierzu keine entsprechenden Regelungen vorsehen, gilt unmittelbar die Ausnahmeregelung des Bundesdatenschutzgesetzes.

Im Beispielsfall ergibt sich aus der notariellen Pflicht zur Verschwiegenheit gemäß § 18 BNotO, dass der Notar dem Neffen nicht mitteilen muss und auch nicht darf, dass dessen personenbezogenen Daten verarbeitet wurden.

4. Auskunftsrecht der betroffenen Personen

Nach Art. 15 DSGVO haben die Beteiligten grundsätzlich einen Anspruch gegenüber dem Notar auf Mitteilung darüber, welche personenbezogenen Daten in welcher Weise konkret verarbeitet werden. Die dabei vom Verantwortlichen zu erteilende Auskunft entspricht im Wesentlichen der Information, die auch bereits nach Artt. 13 und 14 DSGVO bei Datenerhebung zu erteilen ist, geht aber insofern weiter, als auch über eine zwischenzeitlich erfolgte Weiterverarbeitung Auskunft zu erteilen ist.

Beispiel:

Der Notar erfüllt seine Verpflichtung aus Art. 13 DSGVO und teilt den Beteiligten eines Grundstückskaufvertrages mit, welche Daten er erhebt, damit der Vertrag beurkundet und vollzogen werden kann. Unter anderem teilt er dem Käufer mit, dass er dessen Daten an das Finanzamt (Grunderwerbssteuerstelle) übermitteln werde. Wenn nun der Käufer zu einem späteren Zeitpunkt den Auskunftsanspruch nach Art. 15 DSGVO geltend macht, hat der Notar weiterhin mitzuteilen, ob er die zuvor genannte Übermittlung an das Finanzamt bereits vorgenommen hat.

Nach § 29 Abs. 1 Satz 2 BDSG-neu besteht das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DSGVO nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Entsprechende Regelungen enthalten auch die Landesdatenschutzgesetze. Das bedeutet, dass eine Auskunft nicht erteilt zu werden braucht, soweit der Notar dadurch gegen seine Verschwiegenheitspflicht verstoßen würde. Sofern die Landesdatenschutzgesetze hierzu keine entsprechenden Regelungen vorsehen, gilt unmittelbar die Ausnahmeregelung des Bundesdatenschutzgesetzes.

Das Auskunftsersuchen kann vom Beteiligten grundsätzlich formlos geltend gemacht werden. Der Beteiligte kann verlangen, Auskunft in mündlicher oder elektronischer Form zu erhalten. Zu beachten ist, dass durch die Auskunftserteilung selbst ein weiterer Verarbeitungsvorgang in Gang gesetzt wird.

Beispiel:

Der Beteiligte ruft beim Notar an und verlangt unter Angabe seines Namens und einer Urkundennummer die Auskunft nach Art. 15 DSGVO in mündlicher Form. Hier muss zunächst sichergestellt werden, dass die Auskunft überhaupt dem Berechtigten erteilt wird. Der Anspruchsteller muss zur Überzeugung des Notars identifiziert werden, um dem Gebot der Vertraulichkeit der Daten zu genügen, vgl. Art. 12 Abs. 1 Satz 3 DSGVO.

Es empfiehlt sich daher, bereits mit Blick auf § 18 BNotO und § 203 StGB nur dann die Auskunft zu erteilen, wenn die Identität des Anspruchsstellers zur Überzeugung des Notars durch geeignete Mittel nachgewiesen worden ist.

Aus Gründen der Vereinfachung und Nachweisbarkeit kann sowohl für die Information nach den Artt. 13, 14 DSGVO, als auch für die Erfüllung der Auskunftsansprüche nach Art. 15 DSGVO, ein einheitliches Formular vorgehalten werden.

Neben der Auskunft kann der Beteiligte auch verlangen, dass ihm der Notar eine Kopie der personenbezogenen Daten zur Verfügung stellt, Art. 15 Abs. 3 DSGVO. Das bedeutet, dass dem Beteiligten auf dessen Verlangen die Daten in der Form herauszugeben sind, in der sie dem Notar vorliegen. Dabei sind solche Kopien zu fertigen, die ausschließlich die Betroffenendaten abbilden. Enthalten Dokumente auch Daten anderer Personen, sind die Datensätze so zu bearbeiten, dass nur die Betroffenendaten offenbart werden (Teilkopie).

Die Regelungen über die Erteilung von Ausfertigungen und Abschriften von Urkunden des Notars einschließlich der diesbezüglichen Kostenregelungen bleiben von den Regelungen der Datenschutz-Grundverordnung, des BDSG-neu und der Landesdatenschutzgesetze unberührt.

5. Recht auf Berichtigung

Art. 16 DSGVO enthält unter den dort genannten Voraussetzungen einen Anspruch des Betroffenen gegen den Verantwortlichen auf Berichtigung unrichtiger und Vervollständigung unvollständiger Daten.

Für die in notariellen Urkunden enthaltenen Daten korrespondiert der Anspruch mit der Möglichkeit des Notars, offensichtliche Unrichtigkeiten durch einen Nachtragsvermerk nach § 44a Abs. 2 BeurkG richtigzustellen. Erst später eintretende Unrichtigkeiten sind dann vom Anspruch ausgenommen, wenn die Daten bei ihrer Erfassung richtig waren und es für die Verarbeitung gerade darauf ankommt, dass das Datum zum Zeitpunkt der Verarbeitung richtig war und welche Erklärungen die Beteiligten im Zeitpunkt der Beurkundung abgegeben haben.

Beispiel:

Frau Müller ist Partei eines Erbvertrages. Drei Jahre nach Beurkundung und Abwicklung des Vertrages verlangt Frau Müller vom Notar, die Urkunde dahingehend zu ändern, dass sie nunmehr Meier heiße, da sie nach Errichtung des Erbvertrages geheiratet und den Namen ihres Ehemannes angenommen habe. Außerdem sei ihre als Schlusserbin benannte Schwester inzwischen umgezogen, so dass deren im Erbvertrag genannte Adresse zu korrigieren sei.

Da die Urkunde den Zustand beschreiben und die Erklärungen der Beteiligten wiedergeben soll und muss, der im Zeitpunkt der Beurkundung richtig war bzw. die bei Beurkundung abgegeben wurden, scheidet ein Anspruch auf Berichtigung aus.

Anders ist der Fall zu beurteilen, in dem Daten von Anfang an unrichtig verarbeitet wurden. In diesen Fällen ist der Anspruch auf Berichtigung gegeben, die der Notar aber regelmäßig schon von sich aus vornehmen wird, wenn er die Unrichtigkeit der Daten erkennt.

Beispiel:

Im oben genannten Beispiel hat der Notar versehentlich die falsche Adresse der Beteiligten in der Nebenakte oder der Notarsoftware vermerkt. Diese ist zu berichtigen.

6. Recht auf Löschung

Unter bestimmten Voraussetzungen hat die betroffene Person gemäß Art. 17 DSGVO das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten gelöscht werden.

Im Rahmen der notariellen Amtstätigkeit ist insoweit vor allem die Regelung in Art. 17 Abs. 1 lit. a) DSGVO von Bedeutung. Danach sind personenbezogene Daten zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind. Dies kann zum einen Daten betreffen, die nicht unmittelbar in der Urkunde oder in der Nebenakte gespeichert sind. Diese sind zu löschen, sobald sie nicht mehr benötigt werden. Zum anderen normiert die Regelung zwar auch die grundsätzliche Pflicht zur Vernichtung der notariellen Akten, Bücher und Verzeichnisse. Sie gilt nach Art. 17 Abs. 3 lit. b) DSGVO jedoch nur, sofern nicht eine rechtliche Verpflichtung zur Verarbeitung in Form der Speicherung besteht. Daher besteht eine Verpflichtung zur Löschung erst nach Ablauf der Aufbewahrungsfristen. Dies gilt auch für durch den Notar verlängerte Aufbewahrungsfristen.

Beispiel:

Die Parteien errichten einen Erbvertrag. Hierzu teilen Sie dem Notar ihre dazu erforderlichen eigenen personenbezogenen Daten sowie die erforderlichen Daten der von ihnen eingesetzten Schlusserben mit. Der Notar erstellt einen Entwurf und übermittelt diesen elektronisch an die Parteien. Sodann fertigt er die Urkunde, meldet die Beurkundung an das Zentrale Testamentsregister und versendet die Ausfertigungen an die Beteiligten.

Er nimmt die Urkunde zur Urkundensammlung und archiviert die personenbezogenen Daten in der Nebenakte. Bereits bei Eingang des Beurkundungswunsches wurden außerdem Daten der Personen in der Notariatssoftware gespeichert.

Immer dann, wenn die notariellen Berufspflichten eine Speicherung gebieten, ist diese vorzunehmen und auch nach Abwicklung eines Urkundsgeschäfts keine Löschung vorzunehmen. Dies gilt im Beispielsfall namentlich für die Aufbewahrung der Daten in der Urkundensammlung, der Urkundenrolle, im Namensverzeichnis, im Erbvertragsverzeichnis sowie für die Aufbewahrung der Informationen in der Nebenakte.

Art. 17 DSGVO geht davon aus, dass ein Antrag des Betroffenen nicht erforderlich ist, um die Pflicht zur Löschung auszulösen. Auch die vom Notar verwendeten Hilfsmittel (zum Beispiel das E-Mail-Programm oder die Notariatssoftware) sind daraufhin zu überprüfen, ob die erfassten Daten noch vorgehalten werden müssen. Spätestens, wenn die gesetzlich vorgesehenen Akten und Verzeichnisse (zum Beispiel die Nebenakte) zu vernichten sind, sollte auch der Datenbestand in den unterstützenden Datenbanken gelöscht werden.

Ein Recht auf Löschung besteht gemäß Art. 17 Abs. 1 lit. b) DSGVO zudem dann, wenn eine Verarbeitung aufgrund einer Einwilligung erfolgt und die betroffene Person ihre Einwilligung widerruft und keine anderweitige Grundlage für die Verarbeitung vorliegt. Da wie oben dargestellt im Bereich notarieller Tätigkeit grundsätzlich Einwilligungen nicht erforderlich sind, dürfte dieser Fall in der notariellen Praxis kaum relevant werden.

7. Pflicht zur Folgemitteilung

Verlangt die betroffene Person die Berichtigung oder Löschung personenbezogener Daten gemäß Artt. 16, 17 DSGVO, muss der Verantwortliche gemäß Art. 19 DSGVO auch diejenigen Stellen über die Berichtigung oder Löschung der Daten informieren, gegenüber denen er diese Daten (zum Beispiel aufgrund einer gesetzlichen Pflicht) offengelegt hat.[3]

Für die Fälle der Löschungspflicht gemäß Art. 17 lit. a) DSGVO aufgrund abgelaufener Aufbewahrungsfristen dürfte die Folgemitteilungspflicht für Notare in der Regel

[3] Führt der Notar die Löschung oder Berichtigung hingegen im Hinblick auf den Grundsatz der Datenrichtigkeit (s.o. C I. 4.) aus eigenen Stücken durch, ohne dass die betroffene Person dies aktiv verlangt hat, mag eine Folgemitteilung gemäß Art. 19 im Einzelfall sinnvoll sein, eine Verpflichtung dazu besteht jedoch nicht.

keine Bedeutung haben, da in diesen Fällen für die Stellen, denen diese Daten übermittelt wurden, jeweils eigene gesetzliche Aufbewahrungsfristen gelten.

Etwas anderes gilt, wenn der Beteiligte wegen unrichtiger Datenerfassung seinen Anspruch auf Berichtigung personenbezogener Daten gemäß Art. 16 DSGVO geltend macht.

Beispiel:

Aufgrund eines Versehens lautet der Name des Käufers in der Urkunde Karl-Josef Müller. Der Käufer heißt aber tatsächlich Josef-Karl Müller. Der Käufer bemerkt dies anhand der ihm übersandten Ausfertigung des Kaufvertrages und fordert den Notar zur Korrektur auf.

Zusätzlich zu der datenschutzrechtlichen Verpflichtung zur Berichtigung des Namens in den Datensätzen des Notars hat der Notar hier auch diejenigen Stellen zu informieren, denen er im Rahmen der Abwicklung des Amtsgeschäfts den falschen Datensatz übermittelt hat. Das bedeutet zum Beispiel, dass dem Finanzamt mitzuteilen ist, dass die Veräußerungsanzeige auf den falschen Vornamen lautet.

III. Pflichten des Verantwortlichen

Ergänzend zu den Regelungen über die Ansprüche der Betroffenen und der damit korrespondierenden Pflichten des Verantwortlichen regeln die Artt. 24 – 39 DSGVO die Pflichten, die den Notar unabhängig vom konkreten Einzelfall bei der Verarbeitung personenbezogener Daten treffen.

Im Folgenden werden einzelne dieser Pflichten mit Blick auf die Amtstätigkeit des Notars näher erläutert.

1. Umfassende Verantwortung des für die Verarbeitung Verantwortlichen

Art. 24 DSGVO verpflichtet den Notar als für die Datenverarbeitung Verantwortlichen, eine Abwägung bezüglich der Risiken für ihm anvertraute personenbezogene Daten vorzunehmen und entsprechend einer vorhergehenden Risikoanalyse geeignete Maßnahmen zum Schutz der Daten in seinem Betriebsablauf zu implementieren (sog. risikobasierter Ansatz).

Die Regelung legt abstrakt fest, dass die Anforderungen der Datenschutz-Grundverordnung grundsätzlich umfassend zu erfüllen sind. Bei der Erfüllung der Verpflichtungen kann und muss sich der Verantwortliche aber nur solcher Maßnahmen bedie-

nen, die im Hinblick auf die drohenden Risiken verhältnismäßig sind. Bei einer derartigen Abwägung sind Art, Umfang, Umstände und Zwecke der Verarbeitung und die Risiken für die Rechte und Freiheiten natürlicher Personen (regelmäßig der Betroffenen) zu berücksichtigen. Um ausgehend von dieser Risikoanalyse ein angemessenes Schutzniveau zu erreichen, ist der Verantwortliche demgemäß verpflichtet, geeignete technische und organisatorische Maßnahmen zu implementieren. Die in Erfüllung dieser Pflicht getroffenen Maßnahmen sind vom Verantwortlichen zu dokumentieren, damit das Schutzniveau nicht nur sichergestellt, sondern auch nachweisbar ist. Damit wiederholt die Regelung noch einmal die Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO, die den Verantwortlichen ebenfalls verpflichtet, die Rechtmäßigkeit der Verarbeitung nachweisen zu können. Die DSGVO sieht damit eine Pflicht vor, sowohl die Organisation der Notarstelle insgesamt, als auch die einzelne Verarbeitung personenbezogener Daten so zu gestalten, dass die möglichen Risiken und der Aufwand zu ihrer Minimierung in einem angemessenen Verhältnis stehen. Erforderlich ist also eine abstrakte Risikoanalyse bezogen auf die Vorgänge in der Geschäftsstelle sowie eine konkrete Risikoanalyse bezogen auf einzelne Datenverarbeitungsvorgänge.

2. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Art. 25 DSGVO verpflichtet den Notar, geeignete technische und organisatorische Maßnahmen zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze, wie etwa Datenminimierung, wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. Dabei hat er bereits bei der Auswahl der Systeme zur Datenverarbeitung den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Dieser risikobasierte Ansatz soll den Notar verpflichten, bereits durch die Auswahl technischer Hilfsmittel (zum Beispiel seiner Datenverarbeitungsprogramme) ein hohes Datenschutzniveau der notariellen Geschäftsstelle zu implementieren. Dabei hat er sich zwar in der Regel an den besten verfügbaren Mitteln zu orientieren (denn nur solche entsprechen dem Stand der Technik), gleichwohl hat er stets auch die anderen genannten Faktoren zu berücksichtigen. Dies betrifft für den Bereich notarieller Tätigkeit zum einen die Auswahl und richtige Bedienung der Notariatssoftware, zum anderen müssen aber auch für alle Bereiche, in denen eine Verarbeitung außerhalb einer Notariatssoftware erfolgt, Maßnahmen ergriffen werden, um ein angemessenes Schutzniveau zu gewährleisten. Dies bedingt zum Beispiel das Vorhalten eines Kon-

zeptes zur Minimierung von Daten oder auch das Vorhalten eines Konzeptes zur Löschung von Daten. Da bei der Auswahl geeigneter technischer Maßnahmen der Notar auch die Kosten für die Implementierung berücksichtigen darf, hat er nicht stets die optimale technische Lösung zu bevorzugen, wenn diese in finanzieller Hinsicht in einem Missverhältnis zu der vom Notar gewählten Lösung steht.

Neben der Auswahl geeigneter Systeme verpflichtet Art. 25 Abs. 2 DSGVO den Verantwortlichen, bei der Nutzung von IT-Systemen diejenigen Voreinstellungen zu verwenden, die einen möglichst weitgehenden Schutz personenbezogener Daten zulassen.

Beispiel:

Eine Notariatssoftware beinhaltet in der aktuellen Version keinerlei Voreinstellungen zur Löschung von personenbezogenen Daten. Der Hersteller gibt aber an, eine solche in einem künftigen Update zur Verfügung zu stellen. Selbst wenn am Markt andere Softwarehersteller bereits Software mit Löschkonzepten anbieten, ist der Notar hier nicht gezwungen, sofort den Anbieter zu wechseln. Es obliegt vielmehr seiner Einschätzung, ob sich durch den zeitweisen Einsatz einer Software ohne Löschkonzept datenschutzrechtliche Risiken erhöhen oder er auch noch auf das angekündigte Update seines Anbieters warten kann.

3. Auftragsverarbeitung

Art. 28 DSGVO regelt das Verhältnis zwischen dem für den Datenschutz Verantwortlichen und demjenigen, der im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet. Auftragsverarbeiter ist jede „*natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet*“, Art. 4 Nr. 8 DSGVO. Wann immer der Verantwortliche sich bei der Verarbeitung personenbezogener Daten der Hilfe eines Auftragsverarbeiters bedient, sind die Anforderungen des Art. 28 DSGVO zu beachten.

Insbesondere besteht nach Art. 28 Abs. 3 DSGVO die Pflicht zum Abschluss einer besonderen Vereinbarung mit dem Auftragsverarbeiter, die sicherstellt, dass ein angemessenes Datenschutzniveau auch bei Verarbeitung der Daten beim Auftragnehmer vorhanden ist. Auftragsverarbeiter sind auch Dritte, die im Rahmen der Wartung und Pflege von Hard- und Software Zugriff auf personenbezogene Daten erhalten.

Beispiel:

Der Notar hat im Rahmen der Nutzung des Programms XNotar ein technisches Problem bei der Übermittlung einer Handelsregisteranmeldung an ein Gericht.

Der von der NotarNet GmbH angebotene Service TeamViewer, mit dem sich ein Support-Mitarbeiter in Echtzeit auf den Rechner des Notars zuschalten kann, begründet eine Offenlegung von Daten gegenüber der NotarNet GmbH und stellt damit einen Fall der Auftragsdatenverarbeitung dar.

Der Vertrag mit dem Auftragsverarbeiter ist gemäß Art. 28 Abs. 3 Satz 1 DSGVO schriftlich abzuschließen, wobei das europäische Recht dafür ein elektronisches Format genügen lässt, Art. 28 Abs. 9 DSGVO.

Die wesentlichen Inhalte der erforderlichen Vereinbarung sind in Art. 28 Abs. 3 Satz 2 DSGVO festgelegt. Unter anderem ist in der Vereinbarung zu bestimmen, welche Arten von personenbezogenen Daten zu welchen Zwecken, auf welche Art und für welche Dauer verarbeitet werden. Auch muss festgehalten werden, welche Rechte und Pflichten für den Verantwortlichen im Einzelnen bestehen.

Praxishinweis:

Bereits unter der Geltung des BDSG und einiger Landesdatenschutzgesetze waren die Verantwortlichen verpflichtet, Auftragsdatenverarbeitungsvereinbarungen zu schließen. Zwar stimmt die Regelung des § 11 BDSG-alt mit der Regelung des Art. 28 Abs. 3 DSGVO in weiten Teilen überein. Gleichwohl sind die Regelungen nicht vollständig deckungsgleich, weshalb Altvereinbarungen den neuen Anforderungen regelmäßig nicht genügen dürften. Es ist daher zu empfehlen, die bestehenden Vereinbarungen anzupassen.

Klarstellend sei außerdem noch darauf hingewiesen, dass die abzuschließenden Vereinbarungen nicht deckungsgleich mit den zwingend schriftlich abzuschließenden Verschwiegenheitsvereinbarungen im Sinne des § 26a BNotO sind. Hinsichtlich der Adressaten und des Inhalts solcher Vereinbarungen wird auf das Rundschreiben Nr. 4/2018 vom 17. April 2018 der Bundesnotarkammer verwiesen.

4. Verzeichnis der Verarbeitungstätigkeiten

Art. 30 DSGVO verpflichtet den Verantwortlichen zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten. Der Begriff der Verarbeitungstätigkeit umfasst alle Verarbeitungsschritte, Vorgänge und Vorgangsreihen, die einem gemeinsamen Zweck dienen, wie etwa Beurkundungen von Kaufverträgen, Finanzbuchhaltung, Personalaktenverwaltung etc. Ein Ausnahmetatbestand von dieser Pflicht nach Art. 30 Abs. 5 1. Hs. DSGVO dürfte für Notare nicht einschlägig sein, da im Rahmen der notariellen Tätigkeit Daten gerade nicht nur gelegentlich verarbeitet werden und regelmäßig auch

eine Vielzahl von Verarbeitungen besonderer Kategorien personenbezogener Daten erfolgt (siehe oben).

Die gemäß Art. 30 DSGVO zu führenden Verzeichnisse sollen dazu dienen, die Einhaltung der Verordnung zu dokumentieren.

Gleichzeitig bergen sie aber auch das Potential, die Erfüllung der Ansprüche der Betroffenen sowie der Informationspflichten des Verantwortlichen zu erleichtern. Denn die Verzeichnisse sollen einen Überblick darüber geben, welchen Zwecken die Datenverarbeitung dient, welche Datenkategorien verarbeitet werden, an wen diese Daten ggf. übermittelt werden, welche Schutzmaßnahmen vorgehalten werden und wann die Daten zu löschen sind. Der Notar wird so auch selbst in die Lage versetzt, das bei ihm implementierte Schutzkonzept zu überprüfen und ggf. anzupassen.

Zwar besteht für den Betroffenen kein Recht, die Verzeichnisse der Verarbeitungstätigkeiten einzusehen. Jedoch sind die Verzeichnisse der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen. Regelmäßig dient das Verzeichnis der Verarbeitungstätigkeiten damit der Aufsichtsbehörde dazu, sich einen ersten Überblick über das Schutzniveau bei dem Verantwortlichen zu verschaffen.

Für den Bereich der notariellen Tätigkeit ergibt sich aus der Pflicht zur Führung der entsprechenden Verzeichnisse die Notwendigkeit zu prüfen, welche Verarbeitungstätigkeiten sich gemeinsam in einem Verzeichnis darstellen lassen und für welche Verarbeitungstätigkeiten sich eine Aufteilung in unterschiedliche Verzeichnisse anbietet. Regelmäßig werden sich einheitliche Lebensvorgänge in einem Verzeichnis abbilden lassen. Die Kerntätigkeiten innerhalb einer notariellen Geschäftsstelle lassen sich regelmäßig auch in einem gemeinsamen Verzeichnis abbilden.

Beispiel:

Die notarielle Tätigkeit im Zusammenhang mit der Beurkundung von Grundstückskaufverträgen bedingt die Verarbeitung personenbezogener Daten und deren Versendung an Dritte (Gerichte, Behörden etc.) sowie die Aufbewahrung in den notariellen Akten, Büchern und Verzeichnissen. Gleiches trifft auch auf die Beurkundung von Testamenten und Erbverträgen zu. Es lassen sich also fast alle vom Notar zu fertigenden Niederschriften in einem Verzeichnis abbilden. Gleichwohl steht es dem Notar frei, aus Gründen der Übersichtlichkeit für jede Art eines notariellen Amtsgeschäfts ein eigenes Verzeichnis zu führen.

Die Verzeichnisse müssen gemäß Art. 30 Abs. 3 DSGVO schriftlich geführt werden, wobei auch hier ein elektronisches Format verwendet werden kann.

5. Sicherheit der Verarbeitung

Art. 32 DSGVO bestimmt, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen (TOMs) zum Schutz personenbezogener Daten treffen muss. Hierzu können etwa Kennwörter und Kennwortrichtlinien, Zugriffs- und Berechtigungsmanagement, Verschlüsselungsmaßnahmen, Datensicherungsprozesse, mechanische Sicherungen wie Türschlösser, Rauchmelder oder Alarmsicherungen, Aktenvernichtung, Verfahrens- und Verhaltensregeln für Mitarbeiter u. v. m. zählen.

Wie in der grundlegenden Norm des Art. 24 DSGVO festgelegt, hat er dabei den Stand der Technik, die Implementierungskosten, die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Die Vorschrift beschreibt damit den risikobasierten Ansatz im Hinblick auf die technische und organisatorische Ausstattung der datenverarbeitenden Stelle. Die DSGVO verfolgt dabei das Ziel, dass die gesamte Ausstattung der datenverarbeitenden Stelle so ausgestaltet ist, dass sämtliche in ihr stattfindenden Verarbeitungsvorgänge ein effektives Schutzniveau aufweisen.

Für den Bereich der notariellen Amtstätigkeit bedeutet das zum einen, dass die Abläufe in der Notarstelle so auszugestalten sind, dass die eingangs beschriebenen Datenschutzgrundsätze eingehalten werden. Dies bedingt zum Beispiel die Sensibilisierung der Mitarbeiter für die Belange des Datenschutzes oder die Schaffung eines klaren Konzeptes bezüglich der Vergabe von Berechtigungen zum Zugriff auf Daten sowie die Sicherung der Daten gegen den unberechtigten Zugriff Dritter.

Beispiel:

Der Grundsatz der Vertraulichkeit gebietet es, dass die in den Büchern und Verzeichnissen vorhandenen personenbezogenen Daten vor einer Einsicht durch Dritte zu schützen sind. Es gehört daher zu den organisatorischen Maßnahmen, die Betriebsabläufe so zu gestalten, dass unberechtigte Dritte diese Daten nicht einsehen können. Das bedingt unter anderem eine klare Anweisung, dass sich niemand ohne Aufsicht eines Mitarbeiters in der notariellen Geschäftsstelle bewegen oder aufhalten kann, wenn dadurch eine Möglichkeit zur unberechtigten Kenntniserlangung geschaffen würde.

Daneben sind aber auch in technischer Hinsicht Maßnahmen zum Schutz personenbezogener Daten zu implementieren. Dies gebietet unter anderem die Auswahl geeigneter Datenverarbeitungsprodukte (sichere Hard- und Software), aber auch die Implementierung von Werkzeugen zur Nachvollziehbarkeit des Datenschutzes.

Beispiel:

Der Grundsatz der Vertraulichkeit gebietet es, dass nur derjenige Zugriff auf personenbezogene Daten erlangen kann, der diese Daten für seine jeweilige Tätigkeit benötigt. Es ist daher beispielsweise ein geeignetes Zugriffs-und Berechtigungskonzept zu implementieren. So muss etwa der Praktikant unter Umständen nicht mit Rechten zur Einsicht in oder zur Veränderung von Datensätzen ausgestattet sein.

Welche Maßnahmen im konkreten Einzelfall zu treffen sind, hängt ganz wesentlich von der Struktur der jeweiligen Notarstelle ab. Hier ist insbesondere in Zusammenarbeit mit dem Datenschutzbeauftragten des Notars ein individuelles Schutzkonzept zu erarbeiten, das die Arbeitsabläufe in der jeweiligen Amtsstelle angemessen berücksichtigt. Insbesondere in kleineren Einheiten mit wenigen Mitarbeitern dürften die anfallenden Tätigkeiten regelmäßig von allen Mitarbeitern wahrgenommen werden. In größeren Einheiten kann es sachgerecht sein, nicht jedem Mitarbeiter umfassende Zugriffsmöglichkeiten einzuräumen, sofern er diese zur Aufgabenerfüllung nicht benötigt.

Einen für alle notariellen Geschäftsstellen allgemeingültigen Katalog von technischen und organisatorischen Maßnahmen kann es daher nicht geben, sondern die Maßnahmen sind vom Notar anhand seiner Risikoanalyse individuell festzulegen.

6. Meldung von Verletzungen und Benachrichtigung betroffener Personen

Art. 33 DSGVO verpflichtet den Verantwortlichen, der Aufsichtsbehörde jede Verletzung des Schutzes personenbezogener Daten „unverzüglich und möglichst binnen 72 Stunden“ nach Kenntnis von der Verletzung zu melden. Dabei hat der Verantwortliche der Aufsichtsbehörde unter anderem mitzuteilen, welche Art der Verletzung erfolgt ist und welche Kategorien von Personen und Daten in welcher Anzahl betroffen sind. Daneben sind auch die wahrscheinlichen Folgen der Verletzung sowie eine Beschreibung der ergriffenen Gegenmaßnahmen mitzuteilen. Diese Pflichten bedingen indes, dass der Verantwortliche überhaupt im Stande ist, die entsprechenden Mitteilungen zu machen.

Beispiel:

In die Geschäftsräume eines Notars wird eingebrochen. Dabei wird unter anderem ein Computer entwendet, auf dem die Adressdaten der Urkundsbeteiligten des letzten Jahres gespeichert sind.

Hier ist der Notar grundsätzlich verpflichtet, der Aufsichtsbehörde mitzuteilen, dass die Daten abhandengekommen sind. Er hat diese außerdem im Einzelnen zu bezeichnen (also beispielsweise zu benennen, dass es sich um Namen, Anschriften und Telefon- und sonstige Kontaktdaten handelt). Zudem müsste er die ungefähre Anzahl der Betroffenen nennen. Eine Beschreibung möglicher Folgen der Verletzung dürfte dagegen kaum möglich sein, da dem Notar nicht bekannt ist, wie der Einbrecher mit den Daten verfahren wird. Als Beschreibung möglicher Gegenmaßnahmen dürfte eine Verbesserung der Sicherheit der Geschäftsräume für die Zukunft in Betracht kommen.

Flankiert wird die Meldepflicht des Art. 33 DSGVO von der Pflicht zur Benachrichtigung der von der Verletzung betroffenen Personen nach Art. 34 DSGVO. Hiernach hat der Verantwortliche die von der Verletzung betroffenen Personen immer dann zu informieren, wenn die Verletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten der Personen zur Folge hat. Dies dürfte bei Daten, die der notariellen Verschwiegenheitspflicht unterliegen, in aller Regel der Fall sein.

Von der Benachrichtigungspflicht bestehen indes drei wichtige Ausnahmen.

Zum einen ist gemäß Art. 34 Abs. 3 lit. a) DSGVO eine Benachrichtigung der betroffenen Person nicht erforderlich, *„wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung."*

Zum anderen besteht nach § 29 Abs. 1 Satz 3 BDSG-neu eine Benachrichtigungspflicht auch dann nicht, wenn der Notar durch die Benachrichtigung gegen seine Verschwiegenheitspflicht verstoßen würde. Dies gilt nur dann nicht, wenn das Interesse der zu benachrichtigenden Person das Geheimhaltungsinteresse ausnahmsweise überwiegt. Entsprechende Regelungen enthalten auch die Landesdatenschutzgesetze.

Und schließlich sieht Art. 34 Abs. 3 lit. c) DSGVO die Möglichkeit vor, von einer individuellen Benachrichtigung abzusehen, *„wenn dies mit einem unverhältnismäßigen*

Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.". Je nach Art der Verletzung ist daher im Einzelfall, ggf. in Abstimmung mit der Aufsichtsbehörde, zu bestimmen, auf welchem Wege die Information der Betroffenen erfolgen soll. Aus praktischen Gründen dürfte es sich in derartigen Fällen zudem anbieten, sich umgehend mit der zuständigen Notarkammer in Verbindung zu setzen und in Abstimmung mit dieser Kontakt zur Datenschutzaufsicht zu suchen.

7. Benennung eines Datenschutzbeauftragten

Art. 37 DSGVO beschreibt die Pflicht des Verantwortlichen zur Benennung eines Datenschutzbeauftragten. Dabei hat eine solche auf jeden Fall zu erfolgen, wenn es sich bei dem Verantwortlichen um eine öffentliche Stelle handelt, Art. 37 Abs. 1 lit. a) DSGVO. Dies ist bei Notaren, wie oben bereits ausgeführt, der Fall. In Sozietät oder Bürogemeinschaft verbundene Notare haben jeweils einen Datenschutzbeauftragten zu bestellen. Es kann sich selbstverständlich um dieselbe Person handeln.

Dem Datenschutzbeauftragten obliegen die in Art. 39 DSGVO genannten Aufgaben. Dazu zählen die Unterrichtung und Beratung des Verantwortlichen (also des Notars) und der Beschäftigten, die Überwachung der Einhaltung der datenschutzrechtlichen Regelungen sowie die Zusammenarbeit mit der Aufsichtsbehörde. Um diese Aufgaben erfüllen zu können, muss der Datenschutzbeauftragte zum einen über fundierte Kenntnisse bezüglich der Datenverarbeitungsvorgänge in der jeweiligen notariellen Geschäftsstelle verfügen. Zum anderen benötigt er auch Kenntnisse aus dem Bereich des Datenschutzrechts. Er muss die oben dargestellten Pflichten kennen und den Amtsträger im Umgang mit Ansprüchen Betroffener und bei der Kommunikation mit der Aufsichtsbehörde beraten. Er soll durch die interne Beratung des Amtsträgers zur Verwirklichung eines angemessenen Schutzstandards beitragen. Deshalb sieht Art. 37 Abs. 5 DSGVO vor, dass der Datenschutzbeauftragte auf der Grundlage seiner beruflichen Qualifikation und seines Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis zu benennen ist.

Wie die Benennungspflicht in der Praxis am besten zu erfüllen ist, hängt von der Art und der Ausstattung der jeweiligen Notarstelle ab. Grundsätzlich ergeben sich verschiedene Möglichkeiten, um der Benennungspflicht nachzukommen.

a) Interner Datenschutzbeauftragter

Zunächst besteht die Möglichkeit, einen Beschäftigten des Notars als Datenschutzbeauftragten zu benennen. Dieses Vorgehen bietet für den Notar den Vorteil, dass er einen Datenschutzbeauftragten hat, der die Abläufe an der Notarstelle sehr genau kennt. Bei der Bestellung eines internen Datenschutzbeauftragten ist allerdings darauf zu achten, dass dieser für seine Tätigkeit im Bereich des Datenschutzes auch zeitliche und sonstige Ressourcen erhält, die ihm die Erfüllung seiner Aufgaben als Datenschutzbeauftragter ermöglichen. Weiter ist der Datenschutzbeauftragte der Ansprechpartner für die Betroffenen in allen Fragen des Schutzes personenbezogener Daten. Im Bereich der Beratung des Notars hinsichtlich der Umsetzung der Vorgaben des Datenschutzes agiert der Datenschutzbeauftragte weisungsfrei. Bezüglich des Nachweises der erforderlichen Qualifikation des internen Datenschutzbeauftragten gelten aktuell noch keine einheitlichen Standards. Hier ist es möglich, dass sich der Mitarbeiter des Notars über den Besuch von Fortbildungsveranstaltungen kommerzieller Anbieter das notwendige Wissen im Bereich des Datenschutzrechts aneignet. Daneben können auch die berufsständischen Vereinigungen des Notariats ein Angebot zur Fortbildung vorhalten.

Hinsichtlich des der Benennung zugrunde liegenden Grundverhältnisses (regelmäßig des Arbeitsvertrages) ist eine weitere Besonderheit zu beachten. § 6 Abs. 4 Satz 1 BDSG-neu sieht vor, dass eine Abberufung des Datenschutzbeauftragten nur in entsprechender Anwendung des § 626 BGB zulässig ist. Das bedeutet, dass eine Beendigung der Zuweisung der Sonderstellung innerhalb der Notarstelle nur möglich ist, wenn ein wichtiger Grund hierfür vorliegt. Durch die Stellung als Datenschutzbeauftragter erfährt der Mitarbeiter außerdem einen umfassenden Kündigungsschutz. § 6 Abs. 4 Satz 2 und 3 BDSG-neu konkretisieren den Schutz des Arbeitnehmers dahingehend, dass eine Kündigung des Arbeitsverhältnisses mit dem Datenschutzbeauftragten ebenfalls eines wichtigen Grundes nach § 626 BGB bedarf. Auch nach erfolgter Abberufung oder sonstiger Beendigung der Tätigkeit als Datenschutzbeauftragter ist eine Kündigung somit innerhalb eines Jahres, mit Ausnahme der in § 626 BGB genannten Fälle, unzulässig. Die Regelungen zum Kündigungsschutz wurden auch von verschiedenen Landesgesetzgebern in die neuen Datenschutzgesetze der Länder implementiert.

Ob auch eine befristete Bestellung zum Datenschutzbeauftragten zulässig ist, ist nicht abschließend geklärt. Dafür spricht jedoch, dass das Gesetz auch die Benennung eines externen Datenschutzbeauftragten zulässt. Bei diesem erfolgt die Benennung aufgrund eines Dienstleistungsvertrages. Dass ein solcher Vertrag nicht auch auf Zeit geschlossenen werden könnte, ist nicht ersichtlich. Da das Gesetz nicht zwischen dem internen und dem externen Datenschutzbeauftragten unterscheidet, ist davon auszugehen, dass

auch eine bloß zeitweise Benennung des internen Datenschutzbeauftragten zulässig ist. Zu achten ist jedoch darauf, dass das Gesetz zwar keine Mindestdauer der Benennung nennt. Durch die Tätigkeit des Datenschutzbeauftragten soll aber ein kontinuierliches Datenschutzniveau gesichert werden, sodass die Befristung der Benennung eine sachgerechte Aufgabenerfüllung nicht vereiteln darf. Im Schrifttum wird regelmäßig eine Befristung von weniger als zwei Jahren als unzulässig erachtet[4], wobei es hinsichtlich der Dauer der Bestellung auch auf die Größe der verantwortlichen Stelle ankommen soll und entsprechend in Einzelfällen auch eine kürzere Befristung zulässig sein kann.[5]

b) Externer Datenschutzbeauftragter

Art. 37 Abs. 6 DSGVO lässt auch die Benennung eines externen Datenschutzbeauftragten zu. Das Grundverhältnis zu dieser Benennung ist ein Dienstleistungsvertrag. Hinsichtlich der Qualifikation des externen Datenschutzbeauftragten gelten die gleichen Anforderungen wie bei der internen Besetzung.

Zu beachten ist deshalb insbesondere, dass der externe Datenschutzbeauftragte neben seinen Kenntnissen aus dem Bereich des Datenschutzrechtes auch sicher im Umgang mit den Besonderheiten der Verarbeitung im Rahmen notarieller Tätigkeit sein muss. Unstreitig kann der einer Benennung zugrunde liegende Dienstleistungsvertrag jedoch auch mit einer juristischen Person geschlossen werden. Zum Datenschutzbeauftragten wäre dann ein Mitarbeiter dieser juristischen Person zu bestellen.

c) Veröffentlichung der Kontaktdaten

Nach Art. 37 Abs. 7 DSGVO sind die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen. Die Daten (E-Mail-Adresse, Anschrift, Telefonnummer) können beispielsweise auf der Homepage oder anderen Informationskanälen (insbesondere auf einem auszuhändigenden Informationsblatt im Sinne des Art. 13 DSGVO) des Notars veröffentlicht werden. Der Name des Datenschutzbeauftragten muss hingegen nicht veröffentlicht werden, da Sinn und Zweck der Veröffentlichung lediglich ist, eine Kontaktmöglichkeit für die Betroffenen und die Aufsichtsbehörde zu eröffnen. Gleichwohl dürfte sich eine namentliche Nennung des Datenschutzbeauftragten empfehlen. Dies erleichtert den Weg zum Datenschutzbeauftragten und verhindert in erster Linie, dass sich ein Betroffener direkt an die Aufsichtsbehörde wendet, was regelmäßig weiteren Verfahrensaufwand nach sich ziehen würde. Gegenüber der Auf-

---

[4] Bergt in Kühling/Buchner, DS-GVO, Art. 38, Rn. 29; Heberlein in Ehmann/Selmayr, DSGVO, Art. 37, Rn. 18; Wolff in Schantz/Wolff, Das neue Datenschutzrecht, Rn. 906 jeweils mit weiteren Nachweisen.

[5] Bergt in Kühling/Buchner, DS-GVO, a.a.O.

sichtsbehörde ist der Datenschutzbeauftragte ebenfalls zu benennen. Hierfür muss jedenfalls eine namentliche Nennung erfolgen.

Mit freundlichen Grüßen

(Dr. Nicola Hoischen)
Hauptgeschäftsführerin