



Informationen
des
Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-
Pfalz (LfDI)
zur Umsetzung der Datenschutz-Grundverordnung
für die Rechtsanwaltskammern

Stand: 29. Januar 2018

1. Vorbemerkung

Am 24. Mai 2016 ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) in Kraft getreten. Wirksam wird sie nach einer zweijährigen Übergangszeit zum 25. Mai 2018 werden. Mit Wirksamwerden wird sie unmittelbar in allen Mitgliedstaaten der Europäischen Union gelten. Dies wird zu einem weitgehend einheitlichen Recht bei der Verarbeitung personenbezogener Daten in der gesamten Europäischen Union führen.

In Verbindung mit dem dann in neuer Gestalt in Kraft tretenden Bundesdatenschutzgesetz (BDSG) wird damit das Datenschutzrecht in der Bundesrepublik Deutschland auf eine völlig neue Grundlage gestellt. Dies führt zu Änderungen und kann Anpassungen und Umstellungen bei den Verantwortlichen erfordern, also bei Wirtschaft, Verwaltung, Verbänden und allen anderen, die Datenverarbeitung durchführen.

Die Datenschutz-Grundverordnung führt inhaltlich nicht zu einem völlig neuen Datenschutzrecht, sondern erhält viele bewährte Prinzipien. Auch zukünftig müssen personenbezogene Daten grundsätzlich für eindeutig festgelegte Zwecke verarbeitet werden. Die betroffenen Personen haben weiterhin ein Reihe von Rechten, mit denen sie Einfluss auf die Verarbeitung ihrer personenbezogenen Daten nehmen können, z.B. Recht auf Auskunft. Die Verarbeitung personenbezogener Daten im Auftrag ist auch nach der Datenschutz-Grundverordnung möglich.

Die Datenschutz-Grundverordnung enthält aber auch Neuerungen. Das Datenschutzrecht der Europäischen Union wird zukünftig nicht lediglich für in der Europäischen Union niedergelassene Unternehmen gelten, sondern auch für außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind (Marktortprinzip). Verantwortliche sind zu umfangreicheren Information der Betroffenen und größerer Transparenz verpflichtet als bisher. Neuerungen gibt es insoweit insbesondere in Bezug auf Löschpflichten mit dem sog. Recht auf Vergessenwerden: Machen betroffene Personen einen Löschungsanspruch geltend, müssen Verantwortliche, die diese Daten öffentlich gemacht haben, andere Stellen, die diese Daten verarbeiten, über das Löschbegehren informieren.



Mit dem Recht auf Datenübertragbarkeit soll dem Einzelnen ermöglicht werden, seine personenbezogenen Daten zu übertragen. Die Verpflichtungen zu technischem und organisatorischem Datenschutz werden fortentwickelt. Insbesondere müssen Standardeinstellungen von Verfahren und Produkten so entwickelt und/oder ausgestaltet sein, dass nur die für den jeweiligen Zweck erforderlichen Daten erhoben werden (data protection by design und by default). Die Datenschutz-Grundverordnung fördert die datenschutzrechtliche Selbstregulierung der Verantwortlichen und hält hierzu mit Regeln für Codes of Conduct, Binding Corporate Rules und Zertifizierungsverfahren mehrere Instrumente bereit. Verantwortliche werden in Zukunft in vielen Bereichen verpflichtet sein, Datenschutz-Folgenabschätzungen durchzuführen.

Die Aufsichtsbehörden bekommen eine große Anzahl neuer Aufgaben zugewiesen. Auch der Bußgeldrahmen wird erheblich erweitert; in Betracht kommen Geldbußen in Höhe von bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweit erzielten Jahresumsatzes bei einem Verstoß durch ein Unternehmen. Für jedes Unternehmen wird grundsätzlich eine Datenschutzbehörde federführend zuständig sein (One stop shop). Die europaweite Zusammenarbeit der Aufsichtsbehörden in grenzüberschreitenden Fällen wurde detailliert geregelt (Kohärenzverfahren). Jede Bürgerin oder jeder Bürger kann sich mit Eingaben an die Datenschutzbehörden wenden, die dann das Verfahren wenn nötig europäisch fortführen.

Dabei ist zu beachten, dass die Datenschutz-Grundverordnung trotz ihres Verordnungscharakters und der daraus folgenden unmittelbaren Geltung nicht in allen Bereichen gänzlich abschließende Regelungen trifft. Vielmehr werden sich ergänzende Regelungen sowohl auf bundes- als auch landesrechtlicher Ebene finden. Dies ist der Vielzahl vorhandener Öffnungsklauseln geschuldet. Für die Verantwortlichen des privaten Sektors – somit auch die Rechtsanwälte – finden sich einige Öffnungsklauseln, die auf bundesrechtlicher Ebene Regelungen hervorrufen. Für die Rechtsanwaltskammern als öffentliche Stellen der Länder werden sich ergänzende Regelungen in landesrechtlichen Vorschriften finden. Angesichts der Öffnungsklauseln für öffentliche Stellen in der Datenschutz-Grundverordnung wird es eine Reihe von nationalen Vorschriften in diesem Bereich geben. Dies führt dazu, dass öffentliche und nicht-öffentliche Stellen – und damit auch Rechtsanwaltskammern und die von ihnen vertretenen Rechtsanwälte – trotz eigentlich unmittelbarer und unterschiedsloser Geltung der Datenschutz-Grundverordnung für beide Arten von Stellen nicht gänzlich gleich zu behandeln sein werden.

Da die zukünftigen landesrechtlichen Regelungen in Rheinland-Pfalz derzeit noch nicht abschließend feststehen, kann in diesem Papier diesbezüglich noch keine Information erfolgen. Die Konzentration wird daher auf den sich primär aus der Datenschutz-Grundverordnung ergebenden Anforderungen liegen, flankiert durch einige Hinweise zu Regelungen des BDSG-neu, soweit diese besonders relevant im Hinblick auf die Tätigkeit von Rechtsanwälten sind.

Nach einem sogenannten Maßnahmenplan für die Rechtsanwaltskammern bzw. die von diesen vertretenen Rechtsanwälte (2.) werden in diesem Informationspapier drei Schwerpunktthemen vertieft dargestellt werden: das Verzeichnis von Verarbeitungstätigkeiten (3.), die Datenschutz-Folgenabschätzung (4.) sowie die Informationspflichten und das Auskunftsrecht (5.). Abschließen wird dieses



Informationspapier mit einigen Hinweisen zur möglichen Zusammenarbeit mit der Aufsichtsbehörde (6.).

Vorzustellen ist noch der folgende Hinweis: Soweit teilweise die Anwendbarkeit der Datenschutz-Grundverordnung bzw. des BDSG-neu auf Rechtsanwälte insgesamt diskutiert wird, ist darauf hinzuweisen, dass dies allenfalls hinsichtlich einzelner Punkte der Fall sein mag – aufgrund der Berufsgeheimnisträgereigenschaft. Allerdings gibt es insoweit jedenfalls keine vollständige Bereichsausnahme. Die Datenschutz-Grundverordnung gilt grundsätzlich sowohl für Rechtsanwälte als auch für die Rechtsanwaltskammern als öffentliche Stellen.

2. Maßnahmenplan für die Rechtsanwaltskammern bzw. die von den Rechtsanwaltskammern vertretenen Rechtsanwälte

Die Verantwortlichen bzw. die Leitungsorgane der Verantwortlichen sollten sich der Auswirkungen der Datenschutz-Grundverordnung bewusst sein.¹

Welche Auswirkungen die Datenschutz-Grundverordnung auf die einzelnen Verantwortlichen tatsächlich hat, lässt sich allerdings nicht pauschal beantworten. Dies hängt entscheidend auch vom derzeitigen datenschutzrechtlichen Standard, der bei dem Verantwortlichen vorherrscht, ab. Zunächst sollte daher der Ist-Zustand beim Verantwortlichen untersucht werden. Dabei sollte insbesondere das derzeitige Datenschutzmanagement betrachtet werden:

- die derzeitigen Datenverarbeitungsvorgänge (z.B. anhand des Verfahrensverzeichnis nach den Vorgaben des BDSG bzw. LDSG),
- die Rechtsgrundlagen der Datenverarbeitungsvorgänge,
- die Stellung und Aufgaben des ggf. bestellten Datenschutzbeauftragten,
- ggf. bestehende Auftragsverarbeitungsverhältnisse und
- vorhandene Datenschutzkonzepte (wie Rollen- und Berechtigungskonzepte, Löschkonzepte, usw.).

Sodann ist zu prüfen, ob der bisherige Zustand den Anforderungen der Datenschutz-Grundverordnung und zusätzlich den im Rahmen der Öffnungsklauseln erlassenen nationalen Vorschriften genügt. Dabei haben die Rechtsanwälte insbesondere die Vorgaben des BDSG-neu zu beachten, während die Rechtsanwaltskammern als öffentliche Stellen den Regelungen der jeweiligen landesrechtlichen Datenschutzgesetze unterfallen.

Insbesondere sollte dabei das Augenmerk zunächst von Seiten der Rechtsanwaltskammern sowie der Rechtsanwälte auf die folgenden Punkte gelegt werden:

a. Rechtsgrundlagen

Auch künftig darf die Verarbeitung von personenbezogenen Daten nur aufgrund einer Rechtsgrundlage erfolgen. Art. 6 DS-GVO enthält eine Reihe derartiger

¹ Die im Folgenden genannten Pflichten gelten im Wesentlichen auf für Auftragsverarbeiter. Darauf soll hier allerdings nicht näher eingegangen werden.



Rechtsgrundlagen. Aufgrund von Öffnungsklauseln werden sich aber zukünftig auch weiterhin im nationalen Recht Verarbeitungsgrundlagen finden – insbesondere vermehrt in den landesrechtlichen Vorschriften für die öffentlichen Stellen der Länder. Es sollte geprüft werden, ob alle Verarbeitungsvorgänge auf eine Rechtsgrundlage – und falls ja, auf welche – gestützt werden können.

Sollte eine Verarbeitung auf Grundlage einer Einwilligung erfolgen, so ist zu prüfen, ob die Voraussetzungen des Art. 7 DS-GVO bzw. ggf. zusätzlich die ergänzender nationaler Vorschriften erfüllt sind.

b. Betroffenenrechte

Die Betroffenenrechte werden durch die Datenschutz-Grundverordnung gestärkt. Dadurch erweitern sich auch die Pflichten des Verantwortlichen insoweit.

Gegenüber dem Verantwortlichen haben die Betroffenen unter anderen das Recht auf Information nach Art. 13 und 14 DS-GVO, das Recht auf Auskunft nach Art. 15 DS-GVO, das Recht auf Berichtigung nach Art. 16 DS-GVO, das Recht auf Löschung nach Art. 17 DS-GVO, das Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO sowie das Widerspruchsrecht nach Art. 21 DS-GVO. Es sollte geprüft werden, ob Mechanismen vorhanden sind, diese Pflichten ordnungsgemäß zu erfüllen.

c. Technisch-organisatorische Maßnahmen

Die Verpflichtungen zu technischem und organisatorischem Datenschutz werden mit der Datenschutz-Grundverordnung fortentwickelt. Insbesondere müssen Standardeinstellungen von Verfahren und Produkten so ausgestaltet sein, dass nur die für den jeweiligen Zweck erforderlichen Daten erhoben werden (data protection by design und by default). Des Weiteren werden explizite Anforderungen an die Sicherheit der Verarbeitung gestellt (Art. 5, 25, 32 DS-GVO). Neue verpflichtende Instrumente zur Sicherstellung einer ausreichenden Sicherheit der Verarbeitung sind eine Risikobetrachtung der Verarbeitungstätigkeiten (Art. 25 Abs. 1, 32 Abs. 1 DS-GVO) sowie die regelmäßige Evaluation der getroffenen Maßnahmen (Art. 32 Abs. 1 lit. d DS-GVO). Dies sollte der Verantwortliche bei der Einführung neuer Prozesse beachten.

d. Dokumentationspflichten

Aus Art. 5 Abs. 2 DS-GVO ergibt sich für die Verantwortlichen die Rechenschaftspflicht. Daneben enthält die Datenschutz-Grundverordnung an vielen Stellen weitere Dokumentationspflichten der Verantwortlichen. Die Verantwortlichen haben in der Regel ein Verzeichnis von Verarbeitungstätigkeiten zu führen (Art. 30 DS-GVO) und sie haben in bestimmten Fällen eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 DS-GVO).

e. Datenschutzbeauftragter

Eine andere Folge der Datenschutz-Grundverordnung ist die erstmalige Einführung einer europaweiten Pflicht für alle öffentlichen Stellen und bestimmte Unternehmen zur Benennung eines Datenschutzbeauftragten (Art. 37 Abs. 1 DS-GVO). Ausgehend von



dem risikoorientierten Ansatz der Verordnung erstreckt sich die Benennungspflicht im privaten Sektor zunächst auf solche Stellen, deren Haupttätigkeit entweder in einer systematischen Überwachung von Personen oder der umfangreichen Verarbeitung besonders schutzbedürftiger Daten besteht.

Das BDSG-neu weitet diese Pflicht u.a. auf Stellen aus, bei denen in der Regel mindestens zehn Personen personenbezogene Daten automatisiert verarbeiten oder im Falle von Verarbeitungen, die einer Datenschutz-Folgenabschätzung unterliegen (§ 38 Abs. 1 BDSG-neu). Unbenommen bleibt darüber hinaus die Möglichkeit der freiwilligen Benennung eines Datenschutzbeauftragten.

Die Rechtsanwaltskammern und Rechtsanwälte sollten daher prüfen, ob künftig ein Datenschutzbeauftragter zu benennen ist. Bestand bislang eine Bestellungspflicht, so ist in der Regel auch künftig von einer Pflicht zur Benennung eines Datenschutzbeauftragten auszugehen.

Die Rechtsanwaltskammern als öffentliche Stellen sind unabhängig von weiteren Voraussetzungen verpflichtet, einen Datenschutzbeauftragten zu benennen.

Die Rechtsanwälte sollten prüfen, ob Art. 37 Abs. 1 lit. c DS-GVO oder eine der Alternativen des § 38 Abs. 1 BDSG-neu für sie einschlägig ist und demzufolge ggf. handeln.

f. Sonstiges

Darüber hinaus sollten ggf. bestehende Dienstleistungsbeziehungen, d.h. Verträge zur Auftragsverarbeitung überprüft werden. Zudem ist zu prüfen, ob Mechanismen bestehen, die zukünftigen Meldepflichten, etwa nach Art. 37 Abs. 7 DS-GVO oder Art. 33 Abs. 1 DS-GVO zu erfüllen.

3. Verzeichnis von Verarbeitungstätigkeiten

Das bisherige Verzeichnisse (nach § 10 LDSG-RLP für öffentliche Stellen des Landes Rheinland-Pfalz bzw. nach § 4g Abs. 2 und Abs. 2a BDSG für nicht-öffentliche Stellen) wird mit Art. 30 DS-GVO durch ein Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten abgelöst. Art. 30 DS-GVO verpflichtet grundsätzlich alle Verantwortlichen ein Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten zu führen. Dieses betrifft sämtliche automatisierte sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Das Verzeichnis muss die wesentlichen Angaben zum Verantwortlichen, der Art der verarbeiteten Daten, etwaigen Datenempfängern, Löschfristen und Sicherheitsmaßnahmen enthalten.

Dieses Verzeichnis von Verarbeitungstätigkeiten spielt für die Verantwortlichen eine wesentliche Rolle, um datenschutzrechtliche Vorgaben einhalten zu können. Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherzustellen.

Die Pflicht zur Führung des Verzeichnisses trifft generell alle öffentlichen Stellen – und damit auch die Rechtsanwaltskammern – sowie Unternehmen und Einrichtungen mit mehr als 250 Mitarbeitern. Unterhalb dieser Schwelle muss ein Verzeichnis der



Verarbeitungstätigkeiten geführt werden, wenn der Verantwortliche Verarbeitungen durchführt,

- die ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen (z. B. Scoring und Videoüberwachung) oder
- die nicht nur gelegentlich erfolgen (z.B. die regelmäßige Verarbeitung von Kunden- oder Beschäftigtendaten) oder
- die besondere Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO (Religionsdaten, Gesundheitsdaten, usw.) oder Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO betreffen.

Für die Rechtsanwälte bzw. deren Kanzleien dürfte in der Regel zwar nicht die Schwelle von 250 Mitarbeitern überschritten sein, allerdings dürfte häufig einer der drei oben aufgeführten Fälle einschlägig sein.

Das Verzeichnis der Verantwortlichen muss folgende Angaben enthalten

- Name und Kontaktdaten des/der Verantwortlichen und deren Vertreter,
- Name und Kontaktdaten des/der Datenschutzbeauftragten des Verantwortlichen (soweit vorhanden),
- die Verarbeitungszwecke,
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
- die Kategorien von Empfängern der personenbezogenen Daten,
- Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation,
- Lösungsfristen für die verschiedenen Datenkategorien und
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Abs. 1 DS-GVO.

Es ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

Verstöße durch eine fehlende oder nicht vollständige Führung eines Verzeichnisses oder das Nichtvorlegen des Verzeichnisses nach Aufforderung durch die Aufsichtsbehörde können nach Art. 83 Abs. 4 Buchst. a DS-GVO mit einem Bußgeld sanktioniert werden (voraussichtlich allerdings nicht bei den Rechtsanwaltskammern als öffentliche Stellen des Landes Rheinland-Pfalz).

Im Gegensatz zur bisherigen Jedermann offenstehenden Möglichkeit in das Verzeichnisse Einsicht zu nehmen, ist für das Verzeichnis der Verarbeitungstätigkeiten nach DS-GVO ein solcher Anspruch nicht vorgesehen. Entsprechende Auskunftsbegehren sind für öffentliche Stellen nach dem Transparenzgesetz Rheinland-Pfalz zu behandeln. Entfallen ist weiterhin die Pflicht, die eingesetzten Verfahren der Aufsichtsbehörde zu melden. Das Verzeichnis ist jedoch der Aufsichtsbehörde auf Verlangen zur Verfügung zu stellen (siehe Art. 30 Abs. 4 DS-GVO und Erwägungsgrund 82).



Nähere Informationen bezüglich des Verzeichnisses von Verarbeitungstätigkeiten sind zu finden im Kurzpapier Nr. 1 „Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO“ der Datenschutzkonferenz (abrufbar unter: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSK_KPNr_1_Verzeichnis_Verarbeitungstaetigkeiten.pdf) sowie im Papier „Hinweise zum Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO“ (abrufbar unter: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/hinweise_verarbeitungsverzeichnis.pdf). In Kürze wird auch ein Muster für ein Verzeichnis von Verarbeitungstätigkeiten in Homepageangebot des LfDI zu finden sein.

4. Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung nach Art 35 DS-GVO ist Ausdruck des risikobasierten Ansatzes der Datenschutz-Grundverordnung. Ähnlich der bisherigen Vorabkontrolle (nach § 9 Abs. 5 LDSG-RLP für öffentliche Stellen des Landes Rheinland-Pfalz bzw. nach § 4d Abs. 5 und Abs. 6 BDSG für nicht-öffentliche Stellen) sollen auf der Grundlage einer Risikoanalyse die Folgen der Verarbeitung abgeschätzt werden, um frühzeitig Schutzmaßnahmen ergreifen zu können.

Durch die Datenschutz-Folgenabschätzung sind Verarbeitungsvorgänge, die ein hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen bergen, vorab auf ihre Folgewirkungen für deren Persönlichkeitsschutz – insbesondere des Rechts auf Achtung des Privatlebens (Art. 7 Grundrechtecharta) und dem Schutz personenbezogener Daten (Art. 8 Grundrechtecharta) – zu überprüfen. Ziel ist es, bereits frühzeitig geeignete und angemessene Gegen- und Schutzmaßnahmen in technisch-organisatorischer Hinsicht zu treffen, um die identifizierten Risiken für die Persönlichkeitsrechte der betroffenen Personen eindämmen zu können. Dazu sollen die Datenschutzerfordernungen bereits in die den Datenverarbeitungsprozessen zugrunde liegenden Konzepte integriert werden. Durch diese risikobasierte Selbsteinschätzung wird der Verantwortliche strenger in die Verantwortung genommen, als es nach geltendem Recht der Fall ist. Dies kann etwa Videoüberwachungen oder den Umgang mit Gesundheitsdaten betreffen (siehe Art. 35 Abs.3).

Der Datenschutz-Folgenabschätzung ist die sog. Schwellwertanalyse vorangestellt, mittels der ermittelt wird, ob eine Datenverarbeitung grundsätzlich einem hohen Risiko unterliegt (siehe hierzu Erwägungsrund 75). Grundsätzlich können sich Risiken aus der Art, dem Umfang, den Umständen und dem Zweck der Datenverarbeitung ergeben. Mit Blick auf das schnelllebige Entwicklungspotenzial zukunftssträchtiger Technologien wird deren Risikopotenzial ausdrücklich hervorgehoben.

Für bestimmte Datenverarbeitungen wird eine Datenschutz-Folgenabschätzung zwingend vorgeschrieben (Art. 35 Abs. 3 DS-GVO). Hervorzuheben sind insbesondere Maßnahmen des Profilings und automatisierte Datenverarbeitungsmaßnahmen, die angesichts der automatisierten Eingriffe in das Recht auf informationelle Selbstbestimmung als besonders risikoträchtig bewertet werden. Eine Datenschutz-Folgenabschätzung ist auch durchzuführen bei umfangreichen Verarbeitungen besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DS-GVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO.



Wann eine umfangreiche Verarbeitung in diesem Sinne vorliegt, ist im Einzelfall zu entscheiden. Erwägungsgrund 91 der DS-GVO liefert diesbezüglich einige Hinweise und erwähnt in diesem Kontext insbesondere Rechtsanwält: Eine Verarbeitung personenbezogener Daten soll demzufolge nicht als umfangreich gelten, wenn die Verarbeitung personenbezogener Daten von Mandanten betrifft und durch einen einzelnen Rechtsanwalt erfolgt. Folglich kann dann eine Ausnahme von der Pflicht, eine Datenschutz-Folgenabschätzung durchführen zu müssen, bestehen.

Führt die Prognose zu dem Ergebnis, dass von der geplanten Datenverarbeitung ein hohes Risiko für die Rechte der betroffenen Person ausgeht bzw. liegt einer der in Art. 35 Abs. 3 DS-GVO ausdrücklich genannten Fälle vor, ist eine Datenschutz-Folgenabschätzung vorzunehmen. Der Mindestinhalt der Folgenabschätzung wird durch Art. 35 Abs. 7 DS-GVO festgelegt: Nach der systematischen Beschreibung der geplanten Verarbeitungsvorgänge, der Zwecke der Verarbeitung und der Erfassung der berechtigten Interessen des Verantwortlichen dazu, werden die Notwendigkeit und die Verhältnismäßigkeit der Datenverarbeitung in Bezug auf den Zweck bewertet. Des Weiteren werden die Risiken für die Rechte und Freiheiten der betroffenen Personen untersucht. Aufbauend auf dieser Analyse müssen geeignete Abhilfemaßnahmen, insbesondere Garantien, Sicherheitsvorkehrungen und Verfahren getroffen und dokumentiert werden, mit denen die identifizierten Risiken für die Rechte der betroffenen Personen eingedämmt werden können. Der interne Datenschutzbeauftragte – sofern einer benannt wurde – soll von dem Verantwortlichen einbezogen werden. Können aus vertretbaren Gründen keine geeigneten Gegenmaßnahmen getroffen werden, ist nach Art. 36 DS-GVO die zuständige Aufsichtsbehörde zu konsultieren, deren Aufgabe es nach der DS-GVO unter anderem ist, hinsichtlich der Datenschutz-Folgenabschätzung zu beraten. Eine Verletzung dieser Konsultationspflicht könnte mit empfindlichen Geldbußen geahndet werden.

Nähere Hinweise zur Durchführung der Datenschutz-Folgenabschätzung sind insbesondere im Kurzpapier der Datenschutzkonferenz Nr. 5 „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“ (abrufbar unter: https://www.datenschutz.rlp.de/fileadmin/ldi/Dokumente/Orientierungshilfen/DSK_KPNr_5_Datenschutz-Folgenabschaetzung.pdf) sowie in den Leitlinien der Art. 29 Gruppe „Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (abrufbar unter: https://www.datenschutz.rlp.de/fileadmin/ldi/Dokumente/wp248rev01_de.pdf) zu finden.

5. Informationspflichten und Auskunftsrechte

Die Informationspflichten der Verantwortlichen (Art. 13 und 14 DS-GVO) und die Auskunftsrechte (Art. 15 DS-GVO) der betroffenen Personen sind in der Datenschutz-Grundverordnung detailliert geregelt.

Die Informationspflichten und Auskunftsrechte können nach Art. 23 DS-GVO unter engen Voraussetzungen u.a. durch den nationalen Gesetzgeber eingeschränkt werden, z.B. dann, wenn durch die Information oder Auskunft die nationale Sicherheit gefährdet ist oder die Rechte Dritter unverhältnismäßig eingeschränkt werden.



Bei Verstößen gegen die Bestimmungen der o.g. Artikel können die Aufsichtsbehörden nach Art. 87 Abs. 5 DS-GVO Geldbußen von bis zu 20 Millionen Euro oder bei Unternehmen von bis zu vier Prozent des Jahresumsatzes verhängen (voraussichtlich allerdings nicht bei den Rechtsanwaltskammern als öffentliche Stellen des Landes Rheinland-Pfalz).

a. Informationspflichten

Verantwortliche sind verpflichtet, die von der Verarbeitung betroffenen Personen darüber zu informieren. Dabei unterscheidet die Datenschutz-Grundverordnung danach, ob die Daten direkt bei der betroffenen Person (Art. 13 DS-GVO) oder bei Dritten erhoben worden sind (Art. 14 DS-GVO). Auch das zurzeit geltende Landesdatenschutzgesetz RLP und das Bundesdatenschutzgesetz kennen solche Informationspflichten grundsätzlich. Wurden die Daten bei Dritten erhoben, ist auch bisher die betroffene Person hierüber zu benachrichtigen. Neu und wichtig ist die Benachrichtigungspflicht im Fall der Zweckänderung, wenn also die Daten zu einem anderen Zweck verarbeitet werden sollen als zu dem Zweck, zu dem der Verantwortliche sie erlangt hat.

Grundsätzlich ist auch in Zukunft über den Verantwortlichen, über die Zweckbestimmung, die Empfänger der Daten und die Rechtsgrundlage der Verarbeitung zu informieren. Werden die Daten direkt bei der betroffenen Person erfragt, ist diese auf eine ggf. bestehende Verpflichtung zur Angabe hinzuweisen. Zudem sind zukünftig die Kontaktdaten des ggf. vorhandenen internen Datenschutzbeauftragten anzugeben. Um eine faire und transparente Verarbeitung zu gewährleisten, werden zusätzlich Angaben zur Speicherdauer, ein Hinweis auf Betroffenenrechte, die Widerrufbarkeit der Einwilligung sowie das Bestehen einer automatisierten Einzelfallentscheidung einschließlich Profiling gefordert. Von diesen Informationen kann nur unter engen Voraussetzungen abgesehen werden, z.B. wenn die betroffene Person bereits über die Angaben verfügt.

U.a. für die Rechtsanwälte wurde die Informationspflicht gemäß § 29 Abs. 2 BDSG-neu eingeschränkt, um den Schutz der ungehinderten Kommunikation zwischen Mandant und Berufsgeheimnisträger zu gewährleisten. Demzufolge besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäß Art. 13 Abs. 3 DS-GVO nicht, wenn Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Rechtsanwalt oder anderen Berufsgeheimnisträger übermittelt werden, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.

Weitere Einschränkungen der grundsätzlich bestehenden Informationspflichten befinden sich sowohl in der Datenschutz-Grundverordnung selbst als auch in den §§ 32 und 33 BDSG-neu. Inwiefern für öffentliche Stellen des Landes Rheinland-Pfalz Einschränkungen der Betroffenenrechte auf landesrechtlicher Ebene erfolgen werden, ist noch nicht gänzlich absehbar.

Nähere Informationen zu diesem Thema sind im Kurzpapier Nr. 10 „Informationspflichten bei Dritt- und Direkterhebung“ der Datenschutzkonferenz (abrufbar unter: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSK_KPNr_10_Informationspflichten.pdf) zu finden.



b. Auskunftsrechte

Wie schon bislang haben betroffene Personen das Recht formlos und ohne Begründung von einem Verantwortlichen Auskunft über bei diesem gespeicherte personenbezogene Daten sie betreffend zu verlangen.

Um Auskunft von einem Verantwortlichen zu erhalten, kann die betroffene Person nach Art. 15 DS-GVO zunächst eine Bestätigung darüber verlangen, ob überhaupt sie betreffende personenbezogene Daten vorhanden sind. Wenn dies der Fall ist, erstreckt sich dann ihr konkretes Auskunftsrecht auf die gespeicherten Daten bzw. Datenkategorien, die Herkunft und die Empfänger der Daten sowie den Verarbeitungszweck. Dies entspricht der bisherigen Rechtslage. Zukünftig muss die Auskunft aber auch über die geplante Speicherdauer (zumindest die Kriterien für deren Festlegung), die Betroffenenrechte, das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und letztlich bei einer Datenübermittlung an ein Drittland über die geeigneten Garantien unterrichten.

Neu ist auch, dass die Auskunft grundsätzlich innerhalb einer bestimmten Frist, nämlich innerhalb eines Monats nach Eingang des Antrags, zu erteilen ist. Sie bleibt grundsätzlich kostenlos.

Informationen und Auskünfte können in jeder Form gegeben werden: schriftlich oder in anderer Form, ggf. auch elektronisch. Bei der Auskunft muss aber stets die Identität des Anfragenden nachgewiesen werden. Bei Zweifeln daran ist die Auskunft nicht zu erteilen.

Alles soll in präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache erfolgen.

§ 29 Abs. 1 S. 2 BDSG-neu enthält auch eine Einschränkung dieses Auskunftsrechts, die von besonderer Bedeutung für Rechtsanwälte sein dürfte: Demzufolge besteht das Recht auf Auskunft der betroffenen Person gemäß Art. 15 DS-GVO 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. Im Ergebnis darf dies aber jedenfalls nicht dazu führen, dass jegliche Auskunft verweigert wird.

Weitere Einschränkungen für nicht-öffentliche Stellen im nationalen Recht finden sich in § 34 BDSG-neu. Inwiefern für öffentliche Stellen des Landes Rheinland-Pfalz Einschränkungen der Betroffenenrechte auf landesrechtlicher Ebene erfolgen werden, ist noch nicht gänzlich absehbar.

Nähere Hinweise zum Auskunftsrecht der betroffenen Personen – insbesondere zum Umfang der Auskunft – finden sich im Kurzpapier Nr. 6 „Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO“ der Datenschutzkonferenz (abrufbar unter: https://www.datenschutz.rlp.de/fileadmin/ldi/Dokumente/Orientierungshilfen/DSK_KPNr_6_Auskunftsrecht.pdf).

6. Zusammenarbeit mit Aufsichtsbehörde



Die Regelung des § 29 Abs. 3 BDSG-neu zur Einschränkung der Untersuchungsbefugnisse der Aufsichtsbehörden, die möglicherweise gegen europäisches und/oder nationales Verfassungsrecht verstößt, soll hier nicht näher betrachtet werden.

Unabhängig davon empfiehlt sich allerdings sowohl für die Rechtsanwaltskammern als auch die Rechtsanwälte die unmittelbare Kontaktaufnahme mit den zuständigen Aufsichtsbehörden. Den Aufsichtsbehörden obliegt es auch, im Hinblick auf die Datenschutz-Grundverordnung beratend tätig zu werden. Dies können und sollten sowohl öffentliche als auch nicht-öffentliche Stellen nutzen. Außerdem besteht für den Verantwortlichen nach Art. 31 DS-GVO eine Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde.