

# Referentenentwurf

## des Bundesministeriums der Justiz und für Verbraucherschutz

### Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679

#### A. Problem und Ziel

Das europäische Datenschutzrecht wird durch die Verabschiedung der 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72 ) und die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) grundlegend geändert.

Durch die Neufassung des Bundesdatenschutzgesetzes (BDSG (2018)) durch das am 25. Mai 2018 in Kraft tretende Datenschutz-Anpassungs- und -Umsetzungsgesetz EU vom 30. Juni 2017 (BGBl. I S. 2097 – DSAnpUG-EU) wurde das allgemeine Datenschutzrecht des Bundes an diese europäischen Vorgaben angepasst. Das BDSG (2018) enthält einerseits, insbesondere in seinem Teil 3, Regelungen zur Umsetzung der Richtlinie (EU) 2016/680. Andererseits enthält das BDSG (2018) Regelungen zur Anpassung des nationalen Datenschutzrechts an die Datenschutz-Grundverordnung sowie zur Durchführung der Datenschutz-Grundverordnung.

Für den Bereich des Strafverfahrensrechts und des übrigen Verfahrensrechts sowie in einzelnen Bereichen des Justizverwaltungsrechts sind darüber hinaus weitere Umsetzungsmaßnahmen hinsichtlich der Richtlinie (EU) 2016/680 und Anpassungen hinsichtlich der Datenschutz-Grundverordnung vorzunehmen. Der Entwurf dient dazu, die dortigen bereichsspezifischen datenschutzrechtlichen Regelungen an die neuen Vorgaben zum Datenschutz anzupassen.

Der Entwurf dient daher der Umsetzung der Richtlinie (EU) 2016/680 und der Anpassung bereichsspezifischen Datenschutzrechts an die Datenschutz-Grundverordnung.

#### B. Lösung

Die in diesem Entwurf vorgeschlagenen Änderungen sehen im Hinblick auf die Richtlinie (EU) 2016/680 bereichsspezifische Ergänzungen vor

- in der Strafprozessordnung (StPO) und
- im Gesetz über die internationale Rechtshilfe in Strafsachen (IRG).

Darüber hinaus sind redaktionelle Anpassungen entsprechender Verweise auf das BDSG (2018) sowie an die in der Richtlinie (EU) 2016/680 bzw. im BDSG (2018) verwendeten Begriffe erforderlich innerhalb

- der Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters und
- der Eurojust-Anlaufstellen-Verordnung.

Im Hinblick auf die Datenschutz-Grundverordnung sind in dem Entwurf bereichsspezifische Anpassungen in folgenden Gesetzen und Verordnungen vorgesehen:

- Einführungsgesetz zum Gerichtsverfassungsgesetz,
- Bundesverfassungsgerichtsgesetz,
- Vorsorgeregister-Verordnung,
- Testamentsregister-Verordnung,
- Rechtsanwaltsverzeichnis- und -postfachverordnung,
- Rechtsdienstleistungsverordnung,
- Zivilprozessordnung,
- Schuldnerverzeichnisführungsverordnung,
- Schuldnerverzeichnisabdruckverordnung,
- Strafvollzugsgesetz,
- Grundbuchordnung,
- Grundbuchverfügung
- Schiffsregisterordnung,
- Verordnung zur Durchführung der Schiffsregisterordnung
- Handelsregisterverordnung
- Auslandsunterhaltsgesetz,
- Bürgerliches Gesetzbuch
- Luftfahrzeugpfandrechtsregisterverordnung und

### **C. Alternativen**

Keine.

### **D. Haushaltsausgaben ohne Erfüllungsaufwand**

Keine.

## **E. Erfüllungsaufwand**

### **E.1 Erfüllungsaufwand für Bürgerinnen und Bürger**

Keiner.

### **E.2 Erfüllungsaufwand für die Wirtschaft**

Keiner.

Davon Bürokratiekosten aus Informationspflichten

Keine.

### **E.3 Erfüllungsaufwand der Verwaltung**

#### **1. Im Rahmen der bereichsspezifischen Umsetzung der Richtlinie (EU) 2016/680**

Für die Justizbehörden und Gerichte des Bundes und der Länder kann durch die Umsetzung der Richtlinie (EU) 2016/680 in der StPO und im IRG ein Mehraufwand anfallen. Dieser Mehraufwand wird durch die Richtlinie (EU) 2016/680 selbst ausgelöst und geht hierüber nicht hinaus.

Die Anpassung der StPO und des IRG an das Datenschutzniveau der Richtlinie (EU) 2016/680 löst nur einen geringfügigen zusätzlichen Aufwand in sachlicher oder organisatorischer Hinsicht bei den zuständigen Justizbehörden und Gerichten aus. Insbesondere ist weder beim Bund noch in den Ländern die Einrichtung neuer Organisationsstrukturen erforderlich. Zu erwarten ist jedoch ein einmaliger technischer Verwirklichungsaufwand in Höhe von etwa 10 000 Euro sowie ein zusätzlicher personeller Aufwand für die Prüfungen etwaiger Auskunftersuchen auf Grund der geänderten datenschutzrechtlichen Bestimmungen. Dieser dürfte für alle Justizbehörden und Gerichte auf Bundes- und Länderebene zusammen eine Summe von rund 700 000 Euro ausmachen. Hinzu kommt ein einmaliger Einarbeitungsaufwand für die zuständigen justiziellen Stellen. Letzterer kann gegebenenfalls durch Schulungsangebote von Seiten des Bundes und der Länder verringert werden.

Für die StPO stehen hierbei zwei Änderungen im Zentrum, nämlich zum einen der Verzicht auf die Ausschlussklausel und die zeitliche Einschränkung des bisherigen § 491 StPO in Bezug auf datenschutzrechtliche Auskunftsrechte und zum anderen die Ausweitung der Protokollierungspflichten im Rahmen automatisierter Übermittlungsverfahren in den §§ 488 bzw. 493 StPO in der Entwurfsfassung.

Für das IRG geht nur das in § 77d Absatz 1 Nummer 3 des Gesetzes über die internationale Rechtshilfe in Strafsachen in der Entwurfsfassung vorgesehene Zustimmungserfordernis vor einer Datenweiterleitung durch deutsche Behörden insoweit über die Vorgaben der Richtlinie (EU) 2016/680 hinaus, als auch die Weiterleitung von personenbezogenen Daten, die aus Drittstaaten oder von internationalen Einrichtungen stammen, erfasst wird. Darüber hinaus soll eine Zustimmung auch dann erforderlich sein, wenn die Weiterleitung der Daten innerhalb der Europäischen Union erfolgt. Der umzusetzende Artikel 35 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680 erfasst dagegen ausschließlich die Weiterleitung von Daten, die von einem anderen Mitgliedstaat oder von einer Einrichtung der Europäischen Union stammen und die an Drittstaaten weitergeleitet werden sollen. Das

im IRG damit umfassend angelegte Zustimmungserfordernis entspricht allerdings der schon bisher geübten Rechtspraxis, weil der rechtshilferechtliche Spezialitätsgrundsatz zu wahren ist. Mehrkosten fallen hierfür also nicht an.

Für die grenzüberschreitende Datenübermittlung im Rahmen der strafrechtlichen Rechtshilfe gibt es im Übrigen schon jetzt internationale Vorgaben, die von den zuständigen Justizbehörden und Gerichten zu beachten sind, siehe etwa Artikel 23 des Übereinkommens vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (BGBl. 2005 II S. 650, 651). Die Aktualisierung des europäischen Datenschutzniveaus durch die Richtlinie (EU) 2016/680 löst im Grundsatz keinen zusätzlichen Aufwand in sachlicher, personeller oder organisatorischer Hinsicht bei den zuständigen Justizbehörden und Gerichten aus. Insbesondere ist weder beim Bund noch in den Ländern die Einrichtung neuer Organisationsstrukturen erforderlich.

Sollte Mehraufwand entstehen, kann dessen Höhe nicht geschätzt werden, weil das Fallaufkommen nicht vorhergesagt werden kann. Umfassende amtliche Rechtshilfestatistiken existieren weder auf Bundes- noch auf Länderebene, so dass sich bereits die Gesamtzahl aller Rechtshilfeporgänge nicht belastbar ermitteln lässt. Darüber hinaus ist nicht generell zu sagen, wie oft es innerhalb eines konkreten Rechtshilfeporgangs zu einem Austausch von personenbezogenen Daten kommt; dies hängt von den Umständen des Einzelfalls ab und divergiert entsprechend stark. Anfallen dürfte ein einmaliger Einarbeitungsaufwand für die zuständigen justiziellen Stellen, der gegebenenfalls durch Schulungsangebote von Seiten des Bundes und der Länder verringert werden kann. Dem Mehraufwand ist gegenüberzustellen, dass die zusammenhängende Regelung der im Rechtshilfeverkehr zu beachtenden allgemeinen datenschützenden Vorschriften im IRG der Rechtspraxis die Handhabbarkeit erleichtert. Dies kann sich dauerhaft entlastend für die zuständigen Justizbehörden auswirken.

Im Bereich der Zollverwaltung entsteht dem Bund im Haushaltsjahr 2018 einmaliger Erfüllungsaufwand in Höhe von rund 15 000 Euro. Der jährliche Erfüllungsaufwand für die Zollverwaltung erhöht sich ab dem Haushaltsjahr 2018 um rund 26 000 Euro.

Mehrbedarf an Sach- und Personalmitteln beim Bund soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden..

## **2. Im Rahmen der bereichsspezifischen Anpassungen an die Datenschutz-Grundverordnung**

Die gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31; L 40 vom 17.2.2017, S. 78), die durch die Verordnung (EG) Nr. 1882/2003 (ABl. L 284 vom 31.10.2003, S. 1) geändert worden ist, bereits bestehenden Betroffenenrechte, wie etwa das Auskunftsrecht, das Recht auf Berichtigung und Löschung, das Recht auf Einschränkung der Verarbeitung sowie das Widerspruchsrecht, werden durch die Datenschutz-Grundverordnung gestärkt. Mit dem vorliegenden Gesetzentwurf ist kein zusätzlicher Erfüllungsaufwand für die Verwaltung verbunden, der über die Folgen der Datenschutz-Grundverordnung hinausgeht.

## **F. Weitere Kosten**

Keine.

# Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz

## Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679<sup>1)</sup>

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

### Artikel 1

#### Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) Die Angaben zu den §§ 477 bis 480 werden wie folgt gefasst:

„§ 477 Datenübermittlung von Amts wegen

§ 478 Form der Datenübermittlung

§ 479 Übermittlungsverbote und Verwendungsbeschränkungen

§ 480 Entscheidung über die Datenübermittlung“.

b) Die Angabe zum Zweiten Abschnitt des Achten Buches wird wie folgt gefasst:

„Zweiter Abschnitt  
Regelungen zu Dateisystemen“.

c) In der Angabe zu § 486 wird das Wort „Dateien“ durch das Wort „Dateisysteme“ ersetzt.

d) In der Angabe zu § 487 werden die Wörter „einer Datei“ durch die Wörter „einem Dateisystem“ ersetzt.

e) Die Angabe zu § 489 wird wie folgt gefasst:

„§ 489 Löschung und Einschränkung der Verarbeitung von Daten“.

f) In der Angabe zu § 490 wird das Wort „Dateien“ durch das Wort „Dateisysteme“ ersetzt.

---

<sup>1)</sup> Die Artikel 1, 10, 13 und 15 dieses Gesetz dienen der Umsetzung der Richtlinie (EU) 2016/680 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

- g) In der Angabe zu § 491 wird das Wort „Betroffene“ durch die Wörter „betroffene Personen“ ersetzt.
  - h) In der Angabe zu § 494 wird das Wort „Sperrung“ durch die Wörter „Einschränkung der Verarbeitung“ ersetzt.
  - i) In der Angabe zu § 495 wird das Wort „Betroffene“ durch die Wörter „betroffene Personen“ ersetzt.
2. § 81f Absatz 2 wird wie folgt geändert:
- a) In Satz 3 werden die Wörter „des Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.
  - b) Satz 4 wird wie folgt gefasst:

„Ist der Sachverständige eine nichtöffentliche Stelle, finden die Vorschriften der 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) und des Bundesdatenschutzgesetzes auch dann Anwendung, wenn die personenbezogenen Daten nicht automatisiert verarbeitet und die Daten nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“
3. In § 97 Absatz 5 Satz 2 werden die Wörter „Absatz 2 Satz 3“ durch die Wörter durch die Wörter „Absatz 2 Satz 2“ und die Wörter „die Beteiligungsregelung in Absatz 2 Satz 3“ durch die Wörter „die Beteiligungsregelung in Absatz 2 Satz 2“ ersetzt.
4. § 100e Absatz 6 wird aufgehoben.
5. § 100f wird wie folgt geändert:
- a) In Absatz 1 werden die Wörter „der Betroffenen“ durch die Wörter „der betroffenen Personen“ ersetzt.
  - b) Absatz 4 wird wie folgt gefasst:

„(4) §§ 100d Absatz 1 und 2 sowie 100e Absatz 1, 3, 5 Satz 1 gelten entsprechend.“
6. § 100h wird wie folgt geändert:
- a) In Absatz 1 Satz 1 in dem Satzteil 1 vor Nummer 1 werden jeweils die Wörter „der Betroffenen“ durch die Wörter „der betroffenen Personen“ ersetzt.
  - b) Folgender Absatz 4 wird angefügt:

„(4) § 100d Absatz 1 und 2 gilt entsprechend.“
7. In § 100j Absatz 3 Satz 4 werden die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
8. In § 101 Absatz 8 Satz 3 werden die Wörter „der Betroffenen“ durch die Wörter „der betroffenen Personen“ und die Wörter „sie sind entsprechend zu sperren“ durch die Wörter „ihre Verarbeitung ist entsprechend einzuschränken“ ersetzt.

9. § 101a wird wie folgt geändert:
  - a) Die Absätze 4 und 5 werden aufgehoben.
  - b) Absatz 6 wird Absatz 4.
10. In § 101b Absatz 2 Nummer 8 werden die Wörter „der Betroffenen“ durch die Wörter „der betroffenen Personen“ ersetzt.
11. In § 110a Absatz 1 wird folgender Satz 5 eingefügt  
„§ 100d Absatz 1 und 2 gilt entsprechend.“
12. In § 119 Absatz 4 Satz 2 Nummer 7 werden nach dem Wort „dem“ die Wörter „oder der“ eingefügt und die Angabe „§ 38“ wird durch die Angabe „§ 40“ ersetzt.
13. § 155b wird wie folgt geändert:
  - a) Absatz 2 wird wie folgt geändert:
    - aa) In Satz 1 werden die Wörter „und nutzen“ gestrichen und die Wörter „des Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.
    - bb) Satz 2 wird wie folgt gefasst:  
„Sie darf personenbezogene Daten nur verarbeiten, soweit die betroffene Person eingewilligt hat und dies für die Durchführung des Täter-Opfer-Ausgleichs oder der Schadenswiedergutmachung erforderlich ist.“
  - b) Absatz 3 wird wie folgt gefasst:  
„(3) Ist die beauftragte Stelle eine nichtöffentliche Stelle, finden die Vorschriften der Verordnung (EU) 2016/679 und des Bundesdatenschutzgesetzes auch dann Anwendung, wenn die personenbezogenen Daten nicht automatisiert verarbeitet werden und nicht in einem Dateisystem gespeichert sind oder gespeichert werden.“
14. § 160 Absatz 4 wird aufgehoben.
15. § 161 wird wie folgt gefasst:

## „§ 161

### Allgemeine Ermittlungsbefugnis der Staatsanwaltschaft

(1) Zu den in § 160 bezeichneten Zwecken ist die Staatsanwaltschaft befugt, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen zu lassen, soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln. Die Behörden und Beamten des Polizeidienstes sind verpflichtet, dem Ersuchen oder Auftrag der Staatsanwaltschaft zu genügen, und sind in diesem Falle befugt, von allen Behörden Auskunft zu verlangen. Eine Maßnahme ist unzulässig, soweit besondere bundesgesetzliche oder entsprechende landesgesetzliche Verwendungsregelungen entgegenstehen.

(2) Zu den in § 160 bezeichneten Zwecken dürfen besondere Kategorien personenbezogener Daten nach Maßgabe des § 48 des Bundesdatenschutzgesetzes verarbeitet werden. Soweit in diesem Gesetz die Löschung personenbezogener Daten ausdrücklich angeordnet wird, findet § 58 Absatz 3 des Bundesdatenschutzgesetzes keine Anwendung.

(3) Ist eine Maßnahme nach diesem Gesetz nur bei Verdacht bestimmter Straftaten zulässig, so dürfen die auf Grund einer entsprechenden Maßnahme nach anderen Gesetzen erlangten verwertbaren personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen im Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz jeweils angeordnet werden könnte, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person.

(4) In oder aus einer Wohnung erlangte personenbezogene Daten aus einem Einsatz technischer Mittel zur Eigensicherung im Zuge nicht offener Ermittlungen auf polizeirechtlicher Grundlage dürfen unter Beachtung des Grundsatzes der Verhältnismäßigkeit in einem Strafverfahren nur verwendet werden (Artikel 13 Absatz 5 des Grundgesetzes), wenn das Amtsgericht (§ 162 Absatz 1), in dessen Bezirk die anordnende Stelle ihren Sitz hat, die Rechtmäßigkeit der Maßnahme festgestellt hat; bei Gefahr im Verzug ist die richterliche Entscheidung unverzüglich nachzuholen.“

16. Dem § 163 Absatz 1 wird folgender Satz angefügt:

„§ 161 Absatz 1 Satz 3 und Absatz 2 bis 4 gilt entsprechend.“

17. In § 163d Absatz 1 Satz 1 werden in dem Satzteil nach Nummer 2 die Wörter „einer Datei“ durch die Wörter „einem Dateisystem“ ersetzt.

18. In § 406d Absatz 2 Satz 1 Nummer 2 werden die Wörter „des Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.

19. In § 475 Absatz 1 Satz 1 werden nach dem Wort „kann“ das Komma und die Wörter „unbeschadet der Vorschrift des § 406e,“ durch die Wörter „über die Fälle des § 57 des Bundesdatenschutzgesetzes hinaus“ ersetzt.

20. § 476 Absatz 8 wird wie folgt gefasst:

„(8) Ist der Empfänger eine nichtöffentliche Stelle, finden die Vorschriften der Verordnung (EU) 2016/679 und des Bundesdatenschutzgesetzes und auch dann Anwendung, wenn die personenbezogenen Daten nicht automatisiert verarbeitet werden und nicht in einem Dateisystem gespeichert sind oder gespeichert werden.“

21. Die §§ 477 bis 480 werden wie folgt gefasst:

#### „§ 477

#### Datenübermittlung von Amts wegen

(1) Von Amts wegen dürfen personenbezogene Daten aus Strafverfahren Strafverfolgungsbehörden und Strafgerichten für Zwecke der Strafverfolgung sowie den zuständigen Behörden und Gerichten für Zwecke der Verfolgung von Ordnungswidrigkeiten übermittelt werden, soweit diese Daten aus Sicht der übermittelnden Stelle hierfür erforderlich sind.



(2) Eine von Amts wegen erfolgende Übermittlung personenbezogener Daten aus Strafverfahren ist auch zulässig, wenn die Kenntnis der Daten aus der Sicht der übermittelnden Stelle erforderlich ist für

1. die Vollstreckung von Strafen oder von Maßnahmen im Sinne des § 11 Absatz 1 Nummer 8 des Strafgesetzbuches oder die Vollstreckung oder Durchführung von Erziehungsmaßregeln oder von Zuchtmitteln im Sinne des Jugendgerichtsgesetzes,
2. den Vollzug von freiheitsentziehenden Maßnahmen oder
3. Entscheidungen in Strafsachen, insbesondere über die Strafaussetzung zur Bewährung oder deren Widerruf, oder in Bußgeld- oder Gnadensachen.

## § 478

### Form der Datenübermittlung

Auskünfte nach den §§ 474 bis 476 und Datenübermittlungen von Amts wegen nach § 477 können auch durch Überlassung von Kopien aus den Akten erfolgen.

## § 479

### Übermittlungsverbote und Verwendungsbeschränkungen

(1) Die Übermittlung personenbezogener Daten ist unzulässig, wenn ihr Zwecke des Strafverfahrens, auch die Gefährdung des Untersuchungszwecks in einem anderen Strafverfahren, oder besondere bundesgesetzliche oder entsprechende landesgesetzliche Verwendungsregelungen entgegenstehen.

(2) Ist eine Maßnahme nach diesem Gesetz nur bei Verdacht bestimmter Straftaten zulässig, so dürfen die auf Grund einer solchen Maßnahme erlangten verwertbaren personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen in anderen Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz jeweils angeordnet werden könnte, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person. Darüber hinaus dürfen verwertbare personenbezogene Daten, die durch eine Maßnahme der nach Satz 1 bezeichneten Art erlangt worden sind, ohne Einwilligung der von der Maßnahme betroffenen Personen nur verwendet werden

1. zu Zwecken der Gefahrenabwehr, soweit sie dafür durch eine entsprechende Maßnahme nach den für die zuständige Stelle geltenden Gesetzen erhoben werden könnten oder zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder für die Sicherheit oder den Bestand des Bundes oder eines Landes oder für bedeutende Vermögenswerte, soweit sich aus den Daten im Einzelfall konkrete Ansätze zur Abwehr einer solchen Gefahr erkennen lassen,
2. für Zwecke, für die eine Übermittlung nach § 18 des Bundesverfassungsschutzgesetzes zulässig ist, sowie
3. nach Maßgabe des § 476.

§ 100i Absatz 2 Satz 2 und § 108 Absatz 2 und 3 bleiben unberührt.

(3) Die Verwendung von durch eine Maßnahme nach den §§ 100b, 100c oder 100g Absatz 2, auch in Verbindung mit § 100g Absatz 3 Satz 2, erlangten verwertbaren personenbezogenen Daten ist ohne die Einwilligung der von der Maßnahme betroffenen Person neben den in Absatz 2 Satz 1 genannten Zwecken nur zulässig:

1. bei durch eine Maßnahme nach den §§ 100b oder 100c erlangten personenbezogenen Daten, auch solchen nach § 100d Absatz 5 Satz 1 zweiter Halbsatz, nur zur Abwehr einer im Einzelfall bestehenden Lebensgefahr, einer dringenden Gefahr für Leib oder Freiheit einer Person oder für die Sicherheit oder den Bestand des Bundes oder eines Landes oder einer dringenden Gefahr für Gegenstände, die von bedeutendem Wert sind, die der Versorgung der Bevölkerung dienen, die von kulturell herausragendem Wert sind oder die in § 305 des Strafgesetzbuches genannt sind,
2. bei durch eine Maßnahme nach den §§ 100b oder 100c erlangten und verwertbaren personenbezogenen Daten daneben auch zur Abwehr einer im Einzelfall bestehenden dringenden Gefahr für sonstige bedeutende Vermögenswerte und
3. bei verwertbaren, durch eine Maßnahme nach § 100g Absatz 2, auch in Verbindung mit § 100g Absatz 3 Satz 2, erlangten personenbezogenen Daten nur zur Abwehr von konkreten Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes (§ 113c Absatz 1 Nummer 2 des Telekommunikationsgesetzes).

Sind die Daten im Falle des Satzes 2 zur Abwehr der Gefahr oder für eine vorgerichtliche oder gerichtliche Überprüfung der zur Gefahrenabwehr getroffenen Maßnahmen nicht mehr erforderlich, so sind Aufzeichnungen über diese Daten von der für die Gefahrenabwehr zuständigen Stelle unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Soweit die Löschung lediglich für eine etwaige vorgerichtliche oder gerichtliche Überprüfung zurückgestellt ist, dürfen die Daten nur für diesen Zweck verwendet werden; ihre Verarbeitung ist entsprechend einzuschränken.

(4) Wenn in den Fällen der §§ 474 bis 476

1. der Angeklagte freigesprochen, die Eröffnung des Hauptverfahrens abgelehnt oder das Verfahren eingestellt wurde oder
2. die Verurteilung nicht in ein Führungszeugnis für Behörden aufgenommen wird und seit der Rechtskraft der Entscheidung mehr als zwei Jahre verstrichen sind,

dürfen Auskünfte aus den Akten und Akteneinsicht an nichtöffentliche Stellen nur gewährt werden, wenn ein rechtliches Interesse an der Kenntnis der Information glaubhaft gemacht ist und der frühere Beschuldigte kein Interesse an der Versagung hat.

(5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Abweichend hiervon trägt in den Fällen der §§ 474 bis 476 der Empfänger die Verantwortung für die Zulässigkeit der Übermittlung, soweit dieser eine öffentliche Stelle oder ein Rechtsanwalt ist. Die übermittelnde Stelle prüft in diesem Falle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass ein besonderer Anlass zu einer weitergehenden Prüfung der Zulässigkeit der Übermittlung vorliegt.

(6) § 32f Absatz 5 Satz 2 und 3 gilt mit folgenden Maßgaben entsprechend:

1. Eine Verwendung der nach den §§ 474 und 475 erlangten personenbezogenen Daten für andere Zwecke ist zulässig, wenn dafür Auskunft oder Akteneinsicht

gewährt werden dürfte und im Falle des § 475 die Stelle, die Auskunft oder Akteneinsicht gewährt hat, zustimmt;

2. eine Verwendung der nach § 477 erlangten personenbezogenen Daten für andere Zwecke ist zulässig, wenn dafür eine Übermittlung nach § 477 erfolgen dürfte.

## § 480

### Entscheidung über die Datenübermittlung

(1) Über die Übermittlungen nach den §§ 474 bis 477 entscheidet im vorbereitenden Verfahren und nach rechtskräftigem Abschluss des Verfahrens die Staatsanwaltschaft, im Übrigen der Vorsitzende des mit der Sache befassten Gerichts. Die Staatsanwaltschaft ist auch nach Erhebung der öffentlichen Klage befugt, personenbezogene Daten zu übermitteln. Die Staatsanwaltschaft kann die Behörden des Polizeidienstes, die die Ermittlungen geführt haben oder führen, ermächtigen, in den Fällen des § 475 Akteneinsicht und Auskünfte zu erteilen. Gegen deren Entscheidung kann die Entscheidung der Staatsanwaltschaft eingeholt werden. Die Übermittlung personenbezogener Daten zwischen Behörden des Polizeidienstes oder eine entsprechende Akteneinsicht ist ohne Entscheidung nach Satz 1 zulässig, sofern keine Zweifel an der Zulässigkeit der Übermittlung oder der Akteneinsicht bestehen.

(2) Aus beigezogenen Akten, die nicht Aktenbestandteil sind, dürfen Übermittlungen nur mit Zustimmung der Stelle erfolgen, um deren Akten es sich handelt; gleiches gilt für die Akteneinsicht. In den Fällen der §§ 474 bis 476 sind Auskünfte und Akteneinsicht nur zulässig, wenn der Antragsteller die Zustimmung nachweist.

(3) In den Fällen des § 475 kann gegen die Entscheidung der Staatsanwaltschaft nach Absatz 1 gerichtliche Entscheidung durch das nach § 162 zuständige Gericht beantragt werden. Die §§ 297 bis 300, 302, 306 bis 309, 311a und 473a gelten entsprechend. Die Entscheidung des Gerichts ist unanfechtbar, solange die Ermittlungen noch nicht abgeschlossen sind. Diese Entscheidungen werden nicht mit Gründen versehen, soweit durch deren Offenlegung der Untersuchungszweck gefährdet werden könnte.

(4) Die übermittelnde Stelle hat die Übermittlung und deren Zweck aktenkundig zu machen.“

22. In § 481 Absatz 3 wird die Angabe „§ 478“ durch die Angabe „§ 480“ ersetzt.

23. Die Überschrift des Zweiten Abschnitts des Achten Buches wird wie folgt gefasst:

### „Zweiter Abschnitt

### Regelungen zu Dateisystemen“.

24. § 483 wird wie folgt geändert:

- a) In Absatz 1 werden die Wörter „Dateien speichern, verändern und nutzen“ durch die Wörter „Dateisystemen verarbeiten“ ersetzt.
- b) In Absatz 3 werden die Wörter „einer Datei“ durch die Wörter „einem Dateisystem“ ersetzt.

25. § 484 wird wie folgt geändert:

- a) In Absatz 1 werden in dem Satzteil nach Nummer 5 die Wörter „Dateien speichern, verändern und nutzen“ durch die Wörter „Dateisystemen verarbeiten“ ersetzt.
- b) Absatz 2 wird wie folgt geändert:
  - aa) In Satz 1 werden die Wörter „Dateien nur speichern, verändern und nutzen“ durch die Wörter „Dateisystemen nur verarbeiten“ ersetzt.
  - bb) In Satz 2 werden die Wörter „Speicherung, Veränderung und Nutzung“ durch das Wort „Verarbeitung“ und die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
- c) In Absatz 3 Satz 2 und Absatz 4 wird jeweils das Wort „Dateien“ durch das Wort „Dateisystemen“ ersetzt.

26. In § 485 Satz 1 werden die Wörter „Dateien speichern, verändern und nutzen“ durch die Wörter „Dateisystemen verarbeiten“ ersetzt.

27. § 486 wird wie folgt geändert:

- a) In der Überschrift wird das Wort „Dateien“ durch das Wort „Dateisysteme“ ersetzt.
- b) In Absatz 1 wird das Wort „Dateien“ durch das Wort „Dateisystemen“ ersetzt.
- c) In Absatz 2 wird das Wort „Dateien“ durch das Wort „Dateisystemen“ und werden die Wörter „eines Betroffenen § 8“ durch die Wörter „einer betroffenen Person § 83“ ersetzt.

28. § 487 wird wie folgt geändert:

- a) In der Überschrift werden die Wörter „einer Datei“ durch die Wörter „einem Dateisystem“ ersetzt.
- b) In Absatz 1 Satz 2 wird die Angabe „477 Abs. 2“ durch die Wörter „§ 479 Absatz 1 und 2“ ersetzt.
- c) Absatz 2 wird wie folgt gefasst:

„(2) Außerdem kann, über die Fälle des § 57 des Bundesdatenschutzgesetzes hinaus, Auskunft aus einem Dateisystem erteilt werden, soweit nach den Vorschriften dieses Gesetzes Akteneinsicht oder Auskunft aus den Akten gewährt werden könnte. Entsprechendes gilt für Mitteilungen nach den §§ 477 und 481 Absatz 1 Satz 2 sowie für andere besondere gesetzliche Bestimmungen, die die Übermittlung personenbezogener Daten aus Strafverfahren anordnen oder erlauben.“

29. § 488 wird wie folgt geändert:

- a) In Absatz 1 Satz 1 werden die Wörter „der Betroffenen“ durch die Wörter „der betroffenen Personen“ ersetzt.
- b) Absatz 2 wird wie folgt geändert:
  - aa) Satz 1 wird durch die folgenden Sätze ersetzt:

„Bei der Festlegung zur Einrichtung eines automatisierten Abrufverfahrens haben die beteiligten Stellen zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen

1. den Anlass und den Zweck des Abrufverfahrens,
2. die Dritten, an die übermittelt wird,
3. die Art der zu übermittelnden Daten und
4. die nach § 64 des Bundesdatenschutzgesetzes erforderlichen technischen und organisatorischen Maßnahmen.“

bb) In dem neuen Satz 3 wird das Wort „Diese“ durch die Wörter „Die Festlegung“ ersetzt.

c) Absatz 3 wird wie folgt geändert:

aa) In Satz 3 werden die Wörter „zumindest durch geeignete Stichprobenverfahren“ gestrichen.

bb) Die Sätze 4 und 5 werden wie folgt gefasst:

„Im Rahmen der Protokollierung nach § 76 des Bundesdatenschutzgesetzes hat sie ergänzend zu den dort in Absatz 1 aufgeführten Daten die abgerufenen Daten, die Kennung der abrufenden Stelle und das Aktenzeichen des Empfängers zu protokollieren. Die Protokolldaten sind nach zwölf Monaten zu löschen.“

d) Folgender Absatz 4 wird angefügt:

„(4) Die Absätze 2 und 3 gelten für das automatisierte Anfrage- und Auskunftungsverfahren entsprechend.“

30. § 489 wird wie folgt gefasst:

#### „§ 489

##### Löschung und Einschränkung der Verarbeitung von Daten

(1) Zu löschen sind

1. die nach § 483 gespeicherten Daten mit der Erledigung des Verfahrens, soweit ihre Speicherung nicht nach den §§ 484 und 485 zulässig ist,
2. die nach § 484 gespeicherten Daten, soweit die dortigen Voraussetzungen nicht mehr vorliegen und ihre Speicherung nicht nach § 485 zulässig ist, und
3. die nach § 485 gespeicherten Daten, sobald ihre Speicherung zur Vorgangsverwaltung nicht mehr erforderlich ist.

(2) Als Erledigung des Verfahrens gilt die Erledigung bei der Staatsanwaltschaft oder, sofern die öffentliche Klage erhoben wurde, bei Gericht. Ist eine Strafe oder eine sonstige Sanktion angeordnet worden, ist der Abschluss der Vollstreckung oder der Erlass maßgeblich. Wird das Verfahren eingestellt und hindert die Einstellung die

Wiederaufnahme der Verfolgung nicht, so ist das Verfahren mit Eintritt der Verjährung als erledigt anzusehen.

(3) Die Frist zur Überprüfung der Notwendigkeit der Speicherung nach § 75 Absatz 4 des Bundesdatenschutzgesetzes beträgt

1. bei Beschuldigten, die zur Tatzeit das 18. Lebensjahr vollendet hatten, zehn Jahre,
2. bei Jugendlichen fünf Jahre,
3. in den Fällen des rechtskräftigen Freispruchs, der unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens und der nicht nur vorläufigen Verfahrenseinstellung drei Jahre,
4. bei nach § 484 Absatz 1 gespeicherten Daten zu Personen, die zur Tatzeit nicht strafmündig waren, zwei Jahre.

(4) Der Verantwortliche kann in der Errichtungsanordnung nach § 490 kürzere Prüffristen festlegen.

(5) Werden die Daten einer Person für ein weiteres Verfahren in dem Dateisystem gespeichert, so unterbleibt die Löschung, bis für alle Eintragungen die Löschungsvoraussetzungen vorliegen.

(6) § 58 Absatz 3 Satz 1 Nummer 1 und 3 des Bundesdatenschutzgesetzes gilt für die Löschung nach Absatz 1 entsprechend. Darüber hinaus ist anstelle der Löschung personenbezogener Daten deren Verarbeitung einzuschränken, soweit die Daten für laufende Forschungsarbeiten benötigt werden. Die Verarbeitung personenbezogener Daten ist ferner einzuschränken, soweit sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind. Nach den Sätzen 1 und 2 in ihrer Verarbeitung eingeschränkte Daten dürfen nur zu dem Zweck verwendet werden, für den ihre Löschung unterblieben ist. Sie dürfen auch verwendet werden, soweit dies zur Behebung einer bestehenden Beweisnot unerlässlich ist.

(7) Anstelle der Löschung der Daten sind die Datenträger an ein Staatsarchiv abzugeben, soweit besondere archivrechtliche Regelungen dies vorsehen.“

31. § 490 wird wie folgt geändert:

- a) In der Überschrift wird das Wort „Dateien“ durch das Wort „Dateisysteme“ ersetzt.
- b) Satz 1 wird wie folgt geändert:
  - aa) In dem Satzteil vor Nummer 1 werden die Wörter „Die speichernde Stelle“ durch die Wörter „Der Verantwortliche“ und die Wörter „jede automatisierte Datei“ durch die Wörter „jedes automatisierte Dateisystem“ ersetzt.
  - bb) In den Nummern 1 und 2 werden jeweils die Wörter „der Datei“ durch die Wörter „des Dateisystems“ ersetzt.
  - cc) In den Nummern 3 und 6 werden jeweils die Wörter „der Datei“ durch die Wörter „dem Dateisystem“ ersetzt.
- c) In Satz 2 wird das Wort „Dateien“ durch das Wort „Dateisysteme“ ersetzt.

32. § 491 wird wie folgt gefasst:

### Auskunft an betroffene Personen

Ist die betroffene Person bei einem gemeinsamen Dateisystem nicht in der Lage, den Verantwortlichen festzustellen, so kann sie sich zum Zwecke der Auskunft nach § 57 des Bundesdatenschutzgesetzes an jede beteiligte speicherungsberechtigte Stelle wenden. Über die Erteilung einer Auskunft entscheidet die ersuchte speicherungsberechtigte Stelle im Einvernehmen mit dem Verantwortlichen.“

33. In § 492 Absatz 4a Satz 2 werden die Wörter „den Betroffenen“ durch die Wörter „die betroffene Person“ ersetzt.
34. § 493 wird wie folgt geändert:
  - a) Absatz 2 Satz 1 wird wie folgt gefasst:

„Bei der Festlegung zur Einrichtung eines automatisierten Abrufverfahrens gilt § 488 Absatz 2 Satz 1 und 2 entsprechend.“
  - b) Absatz 3 Satz 3 und 4 wird wie folgt gefasst:

„Im Rahmen der Protokollierung nach § 76 des Bundesdatenschutzgesetzes hat sie ergänzend zu den dort in Absatz 1 aufgeführten Daten die abgerufenen Daten, die Kennung der abrufenden Stelle und das Aktenzeichen des Empfängers zu protokollieren. Die Protokolldaten sind nach sechs Monaten zu löschen.“
35. § 494 wird wie folgt geändert:
  - a) In der Überschrift wird das Wort „Sperrung“ durch die Wörter „Einschränkung der Verarbeitung“ ersetzt.
  - b) Die Absätze 1 und 2 werden wie folgt gefasst:

„(1) In den Fällen der §§ 58 Absatz 1 und 75 Absatz 1 des Bundesdatenschutzgesetzes teilt der Verantwortliche insbesondere der Registerbehörde die Unrichtigkeit unverzüglich mit; sie trägt die Verantwortung für die Richtigkeit und Aktualität der Daten.

(2) Die Daten sind zu löschen, sobald sich aus dem Bundeszentralregister ergibt, dass in dem Strafverfahren, aus dem die Daten übermittelt worden sind, eine nach § 20 des Bundeszentralregistergesetzes mitteilungspflichtige gerichtliche Entscheidung oder Verfügung der Strafverfolgungsbehörde ergangen ist.“
  - c) In Absatz 3 werden die Wörter „Abs. 7 und 8“ durch die Angabe „Absatz 7“ ersetzt.
  - d) Absatz 4 wird wie folgt geändert:
    - aa) In Nummer 3 werden die Wörter „der Datei“ durch die Wörter „dem Dateisystem“ ersetzt.
    - bb) In Nummer 5 wird die Angabe „§ 9“ durch die Angabe „den §§ 64, 71 und 72“ ersetzt.
36. § 495 wird wie folgt geändert:

- a) In der Überschrift wird das Wort „Betroffene“ durch die Wörter „betroffene Personen“ ersetzt.
  - b) Satz 1 wird aufgehoben.
  - c) In dem neuen Satz 1 werden nach dem Wort „Auskunft“ die Wörter „nach § 57 des Bundesdatenschutzgesetzes“ eingefügt.
  - d) In dem neuen Satz 2 werden die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
37. In § 496 Absatz 3 wird das Wort „Dateien“ durch das Wort „Dateisysteme“ ersetzt.

## Artikel 2

### Änderung des Einführungsgesetzes zum Gerichtsverfassungsgesetz

Das Einführungsgesetz zum Gerichtsverfassungsgesetz in der im Bundesgesetzblatt Teil III, Gliederungsnummer 300-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 5 Absatz 1 des Gesetzes vom 8. Oktober 2017 (BGBl. I S. 3546) geändert worden ist, wird wie folgt geändert:

1. § 13 wird wie folgt geändert:
  - a) Absatz 1 wird wie folgt geändert
    - aa) In Nummer 2 werden die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
    - bb) Nummer 3 wird wie folgt geändert:
      - aaa) Die Wörter „des Betroffenen“ werden durch die Wörter „der betroffenen Person“ ersetzt.
      - bbb) Das Wort „er“ wird durch das Wort „sie“ ersetzt.
      - ccc) Das Wort „seine“ wird durch das Wort „ihre“ ersetzt.
    - cc) Im zweiten Halbsatz werden die Wörter „der Betroffene ihm“ durch die Wörter „die betroffene Person ihr“ ersetzt.
    - dd) Absatz 2 wird wie folgt geändert:
      - aaa) In Satz 1 werden die Wörter „des Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.
      - bbb) In Satz 2 wird das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt.
2. § 14 wird wie folgt geändert:
  - a) Absatz 1 wird wie folgt geändert:



- aa) In Nummer 4 Buchstabe a werden die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ und das Wort „seines“ wird durch das Wort „ihres“ ersetzt.
  - bb) In Nummer 5 Buchstabe a werden die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
  - cc) In Nummer 6 werden die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
  - dd) In Nummer 7 werden die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
  - b) In Absatz 2 Satz 2 werden die Wörter „des Betroffenen“ durch die Wörter „der betroffenen Person“ und das Wort „ihm“ jeweils durch das Wort „ihr“ ersetzt.
3. § 18 Absatz 1 wird wie folgt geändert:
- a) In Satz 1 werden die Wörter „des Betroffenen“ jeweils durch die Wörter „der betroffenen Person“ ersetzt.
  - b) In Satz 2 werden die Wörter „des Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.
4. § 19 wird wie folgt geändert:
- a) In Absatz 1 Satz 1 wird das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt.
  - b) In Absatz 1 Satz 2 wird das Wort „Verwendung“ durch das Wort „Verarbeitung“ ersetzt.
  - c) In Absatz 2 Satz 3 wird das Wort „Verwendung“ durch das Wort „Verarbeitung“ ersetzt.
5. § 20 wird wie folgt geändert:
- a) In Absatz 1 Satz 2 werden die Wörter „den Betroffenen“ durch die Wörter „die betroffene Person“ ersetzt.
  - b) In Absatz 3 werden die Wörter „des Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.
6. § 21 wird wie folgt geändert:
- a) Absatz 1 wird wie folgt geändert:
    - aa) In Satz 1 werden die Wörter „Dem Betroffenen“ durch die Wörter „Der betroffenen Person“ ersetzt.
    - bb) In Satz 3 werden die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
  - b) Absatz 2 Satz 1 wird wie folgt gefasst:

„Die betroffene Person ist gleichzeitig mit der Übermittlung personenbezogener Daten über den Inhalt und den Empfänger zu unterrichten.“

- c) In Absatz 4 werden die Wörter „des Betroffenen“ jeweils durch die Wörter „der betroffenen Person“ ersetzt.
- d) Folgender Absatz 6 wird angefügt:

„(6) Die Absätze 1 bis 5 gelten nicht im Anwendungsbereich der 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72).“

- 7. Nach § 21 wird folgender § 21a eingefügt:

#### „§ 21a

Bei verfahrensübergreifenden Mitteilungen von Amts wegen im Sinne dieses Abschnitts gelten für Rechte und Pflichten nach den Artikeln 12 bis 15 und 19 Satz 2 der Verordnung (EU) 2016/679 die Bestimmungen des § 21 Absatz 3 bis 5 entsprechend. Rechte nach den Artikeln 18 und 21 der Verordnung (EU) 2016/679 bestehen bei verfahrensübergreifenden Mitteilungen von Amts wegen im Sinne dieses Abschnitts nicht. Die Sätze 1 und 2 gelten entsprechend für Bestimmungen des Artikels 5 der Verordnung (EU) 2016/679, die Rechten und Pflichten nach den Artikeln 12 bis 15 und 19 Satz 2 der Verordnung (EU) 2016/679 entsprechen.“

- 8. § 22 wird wie folgt geändert:

- a) In Absatz 1 Satz 2 werden die Wörter „dem Betroffenen“ durch die Wörter „der betroffenen Person“ ersetzt.
- b) In Absatz 3 Satz 3 wird das Wort „Verwendung“ durch das Wort „Verarbeitung“ ersetzt.

## Artikel 3

### Änderung des Bundesverfassungsgerichtsgesetzes

Das Bundesverfassungsgerichtsgesetz in der Fassung der Bekanntmachung vom 11. August 1993 (BGBl. I S. 1473), das zuletzt durch Artikel 2 des Gesetzes vom 8. Oktober 2017 (BGBl. I S. 3546) geändert worden ist, wird wie folgt geändert:

- 1. In § 35a werden die Wörter „die Vorschriften des Bundesdatenschutzgesetzes“ durch die Wörter „die allgemeinen datenschutzrechtlichen Vorschriften“ ersetzt.
- 2. § 35b Absatz 1 Satz 1 wird wie folgt gefasst:

„Auskunft aus oder Einsicht in Akten des Bundesverfassungsgerichts kann gewährt werden

- 1. öffentlichen Stellen, soweit dies für Zwecke der Rechtspflege erforderlich ist oder die in § 23 Absatz 1 Nummer 2, 4 bis 6 des Bundesdatenschutzgesetzes genannten Voraussetzungen vorliegen oder soweit dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der

Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,

2. Privatpersonen und anderen nichtöffentlichen Stellen, soweit die in § 25 Absatz 2 Nummer 2 des Bundesdatenschutzgesetzes genannten Voraussetzungen vorliegen. Einer Unterrichtung des Betroffenen von der Übermittlung seiner Daten bedarf es nicht; die Erteilung der Auskunft und die Gewährung der Akteneinsicht sind in der Akte zu vermerken.“
3. In § 35c wird das Wort „nutzen“ durch das Wort „verarbeiten“ ersetzt.

## Artikel 4

### Änderung der Vorsorgeregister-Verordnung

In § 6 Absatz 1 Satz 1 der Vorsorgeregister-Verordnung vom 21. Februar 2005 (BGBl. I S. 318), die zuletzt durch Artikel 3 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2426) geändert worden ist, werden die Wörter „nach § 10 Abs. 2 des Bundesdatenschutzgesetzes“ durch die Wörter „zu den technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit“ ersetzt.

## Artikel 5

### Änderung der Testamentsregister-Verordnung

Die Testamentsregister-Verordnung vom 11. Juli 2011 (BGBl. I S. 1386), die zuletzt durch Artikel 6 Absatz 1 des Gesetzes vom 1. Juni 2017 (BGBl. I S. 1396) geändert worden ist, wird wie folgt geändert:

1. In § 8 Absatz 4 werden die Wörter „(§ 19 des Bundesdatenschutzgesetzes)“ durch die Wörter „nach den datenschutzrechtlichen Vorschriften“ ersetzt.
2. § 12 wird wie folgt geändert:
  - a) Absatz 1 wird aufgehoben.
  - b) Absatz 2 wird Absatz 1 und in Satz 2 werden die Wörter „den Anforderungen von Absatz 1“ durch die Wörter „den datenschutzrechtlichen Anforderungen“ ersetzt.
  - c) Absatz 3 wird Absatz 2 und wie folgt gefasst:

„(2) Die Registerbehörde erstellt ein Sicherheitskonzept, in welchem die einzelnen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit und der Vorgaben dieser Verordnung festgelegt werden.“

## Artikel 6

### Änderung der Rechtsanwaltsverzeichnis- und -postfachverordnung

In § 18 Absatz 2 Satz 3 der Rechtsanwaltsverzeichnis- und -postfachverordnung vom 23. September 2016 (BGBl. I S. 2167), die durch Artikel 19 des Gesetzes vom 12. Mai 2017 (BGBl. I S. 1121) geändert worden ist, werden die Wörter „die für dessen Führung verantwortliche Stelle“ durch die Wörter „den für dessen Führung Verantwortlichen“ ersetzt.

## Artikel 7

### Änderung der Rechtsdienstleistungsverordnung

§ 9 Absatz 2 Satz 2 der Rechtsdienstleistungsverordnung vom 19. Juni 2008 (BGBl. I S. 1069), die zuletzt durch Artikel 7 des Gesetzes vom 12. Mai 2017 (BGBl. I S. 1121) geändert worden ist, wird wie folgt gefasst:

„Die Verantwortlichkeit für die Zulässigkeit des Abrufs trägt die abrufende Behörde.“

## Artikel 8

### Änderung der Zivilprozessordnung

Die Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel 11 Absatz 15 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 882h folgende Angabe eingefügt:  
„§ 882i Rechte der Betroffenen“.
2. In § 755 Absatz 3 wird das Wort „nutzen“ durch das Wort „verarbeiten“ ersetzt.
3. In § 802d Absatz 1 Satz 3 wird das Wort „nutzen“ durch das Wort „verarbeiten“ ersetzt.
4. § 802k wird wie folgt geändert:
  - a) In Absatz 3 Satz 3 zweiter Teilsatz werden die Wörter „die jeweiligen datenschutzrechtlichen Bestimmungen“ durch die Wörter „die datenschutzrechtlichen Vorschriften“ und das Wort „anzuwenden“ durch die Wörter „zu beachten“ ersetzt.
  - b) Folgender Absatz 5 wird angefügt:

„(5) Macht eine betroffene Person das Auskunftsrecht nach Artikel 15 Absatz 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Ra-

tes 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) in Bezug auf personenbezogene Daten geltend, die in den von den zentralen Vollstreckungsgerichten nach Absatz 1 verwalteten Vermögensverzeichnissen enthalten sind, sind der betroffenen Person im Hinblick auf die Empfänger, denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, nur die Kategorien berechtigter Empfänger mitzuteilen. Das Widerspruchsrecht gemäß Artikel 21 der Verordnung (EU) 2016/679 findet in Bezug auf die personenbezogenen Daten, die in den von den zentralen Vollstreckungsgerichten nach Absatz 1 verwalteten Vermögensverzeichnissen enthalten sind, keine Anwendung.“

5. In § 802l Absatz 2 Satz 1 werden die Wörter „zu sperren“ durch die Wörter „deren Verarbeitung einzuschränken“ ersetzt.
6. In § 850k Absatz 8 Satz 5 werden die Wörter „Erhebung, Verarbeitung und Nutzung“ durch das Wort „Verarbeitung“ ersetzt.
7. In § 882f Absatz 1 Satz 2 erster Teilsatz wird das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt.
8. In § 882g Absatz 7 Satz 1 wird die Angabe „§ 38“ durch die Angabe „§ 40“ ersetzt und werden die Wörter „und Nutzung“ gestrichen.
9. § 882h Absatz 3 wird wie folgt geändert:
  - a) In Satz 3 Nummer 4 wird das Wort „Datenverwendung“ durch das Wort „Datenverarbeitung“ ersetzt.
  - b) In Satz 4 wird das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt.
10. Nach § 882h wird folgender § 882i eingefügt:

#### „§ 882i

#### Rechte der Betroffenen

(1) Das Auskunftsrecht nach Artikel 15 Absatz 1 und das Recht auf Erhalt einer Kopie nach Artikel 15 Absatz 3 der Verordnung (EU) 2016/679 wird in Bezug auf die personenbezogenen Daten, die im Schuldnerverzeichnis und in den an das zentrale Vollstreckungsgericht übermittelten Anordnungen der Eintragung in das Schuldnerverzeichnis enthalten sind, dadurch erfüllt, dass die betroffene Person Einsicht in das Schuldnerverzeichnis über die zentrale und länderübergreifende Abfrage im Internet nach § 882h Absatz 1 Satz 2 nehmen kann. Eine Information der betroffenen Person über konkrete Empfänger, gegenüber denen die personenbezogenen Daten, die im Schuldnerverzeichnis und in den an das zentrale Vollstreckungsgericht übermittelten Anordnungen der Eintragung in das Schuldnerverzeichnis enthalten sind, offengelegt werden, erfolgt nur insoweit, als Daten zu diesen Empfängern nach den Vorschriften für Zwecke der Datenschutzkontrolle zu speichern sind.

(2) Hinsichtlich der im Schuldnerverzeichnis enthaltenen personenbezogenen Daten kann das Recht auf Berichtigung nach Artikel 16 der Verordnung (EU) 2016/679 nur unter den Voraussetzungen ausgeübt werden, die in § 882e für Löschungen von Eintragungen oder die Änderung fehlerhafter Eintragungen vorgesehen sind.

(3) Das Widerspruchsrecht gemäß Artikel 21 der Verordnung (EU) 2016/679 findet in Bezug auf die personenbezogenen Daten, die im Schuldnerverzeichnis und in den an das zentrale Vollstreckungsgericht übermittelten Anordnungen der Eintragung in das Schuldnerverzeichnis enthalten sind, keine Anwendung.“

11. In § 947 Absatz 2 Satz 2 werden die Wörter „zu sperren oder zu löschen“ durch die Wörter „zu löschen oder ist deren Verarbeitung einzuschränken“ ersetzt.

## Artikel 9

### Änderung der Schuldnerverzeichnisführungsverordnung

Die Schuldnerverzeichnisführungsverordnung vom 26. Juli 2012 (BGBl. I S. 1654), die zuletzt durch Artikel 6 des Gesetzes vom 21. November 2016 (BGBl. I S. 2591) geändert worden ist, wird wie folgt geändert:

1. In § 6 Absatz 4 Satz 2 wird das Wort „Datenschutzkontrolle“ durch das Wort „Datenschutzaufsicht“ ersetzt.
2. In § 9 Absatz 1 Satz 1 wird das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt.
3. § 10 wird wie folgt geändert:
  - a) In Absatz 1 wird das Wort „Datenverwendung“ durch das Wort „Datenverarbeitung“ ersetzt.
  - b) In Absatz 2 wird das Wort „Datenverwendung“ durch das Wort „Datenverarbeitung“ ersetzt.
  - c) In Absatz 4 Satz 4 wird das Wort „Sperrung“ durch die Wörter „Einschränkung der Verarbeitung“ ersetzt.

## Artikel 10

### Änderung der Schuldnerverzeichnisabdruckverordnung

Die Schuldnerverzeichnisabdruckverordnung vom 26. Juli 2012 (BGBl. I S. 1658), die durch Artikel 7 des Gesetzes vom 21. November 2016 (BGBl. I S. 2591) geändert worden ist, wird wie folgt geändert:

1. § 1 Absatz 3 wird wie folgt geändert:
  - a) In Nummer 3 werden die Wörter „und Nutzung“ gestrichen.
  - b) In Nummer 4 werden die Wörter „oder nutzt“ gestrichen.
2. § 4 wird wie folgt geändert:
  - a) In Absatz 1 werden die Wörter „erhoben und“ gestrichen.

- b) In Absatz 2 Satz 2 werden die Wörter „dazu erhoben, verarbeitet und genutzt“ durch das Wort „verarbeitet“ ersetzt.
3. In § 6 Absatz 2 werden in dem Satzteil vor Nummer 1 die Wörter „der anzuwendenden Vorschriften der Datenschutzgesetze“ durch die Wörter „der datenschutzrechtlichen Vorschriften“ ersetzt.
4. In § 16 Absatz 2 Satz 2 Nummer 2 werden die Wörter „erhoben, verarbeitet und genutzt“ durch das Wort „verarbeitet“ ersetzt.
5. § 17 Satz 1 wird wie folgt gefasst:
- „Der Bezieher von Abdrucken, der Einzelauskünfte im automatisierten Abrufverfahren erteilt (Auskunftsstelle), hat gemäß Artikel 24, 25 und 32 der 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) geeignete technische und organisatorische Maßnahmen zu treffen.“
6. § 18 Absatz 1 Satz 1 wird wie folgt geändert:
- a) In Nummer 1 wird das Wort „verwendet“ durch das Wort „verarbeitet“ ersetzt
- b) In Nummer 3 werden die Wörter „genutzt, insbesondere weitergegeben“ durch das Wort „verarbeitet“ ersetzt.
- c) In Nummer 5 werden die Wörter „und Nutzung“ gestrichen.

## Artikel 11

### Änderung der Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters

Die Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters vom 23. September 2005 (BGBl. I S. 2885), die zuletzt durch Artikel 2 Absatz 5 des Gesetzes vom 16. Juni 2017 (BGBl. I S. 1634) geändert worden ist, wird wie folgt geändert:

1. § 5 wird wie folgt gefasst:

#### „§ 5

#### Berichtigung, Löschung und Einschränkung der Verarbeitung

Die Berichtigung, Löschung und Einschränkung der Verarbeitung der gespeicherten Daten bestimmt sich nach § 494 Absatz 1 bis 3 der Strafprozessordnung.“

2. § 9 wird wie folgt gefasst:

„§ 9

Auskunft an betroffene Personen

(1) Für den Auskunftsanspruch betroffener Personen gilt § 57 des Bundesdatenschutzgesetzes.

(2) Über die Erteilung der Auskunft entscheidet die Registerbehörde im Einvernehmen mit der Stelle, welche die in die Auskunft aufzunehmenden personenbezogenen Daten mitgeteilt hat.“

## Artikel 12

### Änderung des Strafvollzugsgesetzes

Das Strafvollzugsgesetz vom 16. März 1976 (BGBl. I S. 581, 2088; 1977 I S. 436), das zuletzt durch Artikel 10 Absatz 7 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) In der Angabe zu dem Fünften Abschnitt werden nach dem Wort „Datenschutz“ die Wörter „beim Vollzug von Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft“ eingefügt.

b) Die Angabe zu dem Fünften Titel des Fünften Abschnitts wird wie folgt gefasst:

„Fünfter Titel

Datenschutz beim Vollzug von Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft“.

c) In der Angabe zu § 180 werden die Wörter „und Nutzung“ gestrichen.

d) Die Angaben zu den §§ 181 und 182 werden wie folgt gefasst:

„§ 181 Zweckbindung bei Übermittlungen

§ 182 Schutz besonderer Kategorien personenbezogener Daten“.

e) In der Angabe zu § 183 wird das Wort „Dateien“ durch das Wort „Dateisystemen“ ersetzt.

f) In der Angabe zu § 184 wird das Wort „Sperrung“ durch die Wörter „Einschränkung der Verarbeitung“ ersetzt.

g) In der Angabe zu § 185 werden die Wörter „den Betroffenen“ durch die Wörter „die betroffene Person“ ersetzt.

h) Die Angabe zu § 187 wird wie folgt gefasst:

„§ 187 (weggefallen)“.

2. § 86 Absatz 2 Satz 3 wird wie folgt gefasst:

„Die nach Absatz 1 erhobenen Daten dürfen nur für die in Absatz 1 und § 87 Absatz 2 genannten Zwecke und zur Verhinderung oder Verfolgung von Straftaten sowie zur



Verhinderung oder Verfolgung von Ordnungswidrigkeiten, durch welche die Sicherheit oder Ordnung der Anstalt gefährdet werden, verarbeitet werden.“

3. In § 130 werden die Wörter „(§§ 3 bis 119, 120 bis 126 sowie 179 bis 187)“ durch die Wörter „(§§ 3 bis 119 sowie 120 bis 126)“ ersetzt.
4. In der Überschrift des Fünften Abschnitts werden nach dem Wort „Datenschutz“ die Wörter „beim Vollzug von Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft“ eingefügt.
5. In § 167 Satz 1 werden die Wörter „(§§ 2 bis 121, 179 bis 187)“ durch die Wörter „(§§ 2 bis 121) und die §§ 179 bis 186“ ersetzt.
6. In § 171 werden die Wörter „(§§ 3 bis 49, 51 bis 121, 179 bis 187)“ durch die Wörter „(§§ 3 bis 49 sowie 51 bis 121)“ ersetzt.
7. Die Überschrift des Fünften Titels wird wie folgt gefasst:

#### „Fünfter Titel

Datenschutz beim Vollzug von Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft“.

8. § 179 wird wie folgt geändert:
  - a) In Absatz 1 wird das Wort „Freiheitsstrafe“ durch die Wörter „Haft nach § 171“ ersetzt.
  - b) Absatz 2 wird durch die folgenden Absätze 2 und 2a ersetzt:

„(2) Personenbezogene Daten sind bei der betroffenen Person zu erheben. Ohne ihre Mitwirkung dürfen sie nur erhoben werden,

    1. wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
    2. wenn
      - a) die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
      - b) die Erhebung bei der betroffenen Person einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Person beeinträchtigt werden.

(2a) Werden personenbezogene Daten bei der betroffenen Person aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechten, so ist die betroffene Person hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, ist sie über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären. Werden personenbezogene Daten statt bei der betroffenen Person bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Vor-

schrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.“

- c) In Absatz 3 werden nach dem Wort „für“ die Wörter „die Behandlung eines Gefangenen,“ gestrichen und werden die Wörter „einer Freiheitsstrafe“ durch die Wörter „der Haft nach § 171“ und das Wort „Betroffenen“ durch die Wörter „betroffenen Personen“ ersetzt.

- d) Absatz 4 wird wie folgt gefasst:

„(4) Die Rechte und Pflichten nach den Artikeln 13 und 14 der 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) bestehen ergänzend zu den in diesen Vorschriften genannten Ausnahmen nicht, wenn

1. bei der Erhebung personenbezogener Daten ohne Kenntnis der betroffenen Person andernfalls der Vollzug der Haft nach § 171 gefährdet wird oder
2. bei der Erhebung der Daten bei anderen Personen oder Stellen die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden berechtigten Interesses eines Dritten, geheim gehalten werden müssen.“

9. § 180 wird wie folgt geändert:

- a) In der Überschrift werden die Wörter „und Nutzung“ gestrichen.

- b) In Absatz 1 Satz 1 werden nach dem Wort „verarbeiten“ die Wörter „und nutzen“ gestrichen und werden die Wörter „der Freiheitsstrafe“ durch die Wörter „der Haft nach § 171“ ersetzt.

- c) Absatz 2 wird wie folgt gefasst:

„(2) Für die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, findet § 23 des Bundesdatenschutzgesetzes Anwendung.“

- d) Absatz 3 wird aufgehoben.

- e) Absatz 4 wird Absatz 3 und Satz 1 wird wie folgt gefasst:

„Über die in Absatz 1 und § 23 des Bundesdatenschutzgesetzes genannten Zwecke hinaus dürfen zuständigen öffentlichen Stellen personenbezogene Daten übermittelt werden, soweit dies für folgende Zwecke erforderlich ist:

1. gesetzlich angeordnete Statistiken der Rechtspflege,
2. Entscheidungen über Leistungen, die mit der Aufnahme in einer Justizvollzugsanstalt entfallen oder sich mindern,
3. dienstliche Maßnahmen der Bundeswehr im Zusammenhang mit der Aufnahme und Entlassung von Soldaten,
4. ausländerrechtliche Maßnahmen oder

5. die Durchführung der Besteuerung.“

- f) Absatz 5 wird Absatz 4 und die Sätze 2 bis 4 werden aufgehoben.
- g) Absatz 6 wird Absatz 5 und in Satz 1 werden nach den Wörtern „befugten Stellen“ das Komma durch das Wort „sowie“ und werden die Wörter „strafvollzugs-, strafvollstreckungs- und strafrechtliche Entscheidungen“ durch das Wort „Haftentscheidungen“ ersetzt.
- h) Absatz 7 wird Absatz 6 und die Wörter „nach den Absätzen 1, 2 oder 4“ werden durch die Wörter „nach den Absätzen 1 bis 3“ und die Wörter „des Betroffenen“ werden jeweils durch die Wörter „der betroffenen Person“ ersetzt und werden nach dem Wort „Verarbeitung“ die Wörter „oder Nutzung“ gestrichen.
- i) Absatz 8 wird Absatz 7 und die Wörter „in Absatz 2“ werden durch die Wörter „in § 23 Absatz 1 Nummer 3 bis 5 des Bundesdatenschutzgesetzes“ und wird nach der Angabe „121“ das Komma durch das Wort „und“ ersetzt und werden nach dem Wort „Anstalt“ die Wörter „oder nach Anhörung des Gefangenen für Zwecke der Behandlung“ und nach dem Wort „verarbeitet“ die Wörter „und genutzt“ gestrichen.
- j) Absatz 9 wird Absatz 8 und die Wörter „Absatz 2 Nr. 1 bis 3“ werden durch die Wörter „§ 23 Absatz 1 Nummer 3 und 5 des Bundesdatenschutzgesetzes“ ersetzt und werden nach dem Wort „verarbeitet“ die Wörter „oder genutzt“ gestrichen.
- k) Absatz 10 wird Absatz 9 und die Wörter „§ 182 Abs. 2, § 184 Abs. 2 und 4“ werden durch die Wörter „§ 182 Absatz 2 und § 184 Absatz 2“ ersetzt.
- l) Absatz 11 wird Absatz 10 und in Satz 3 werden die Wörter „Absätze 8 bis 10“ durch die Wörter „Absätze 7 bis 9“ ersetzt.
- m) Folgender Absatz 11 wird angefügt:

„(11) Die Unterrichtungspflicht nach Artikel 19 Satz 2 der Verordnung (EU) 2016/679 besteht nicht, soweit durch eine solche Unterrichtung der Zweck der Übermittlung der Daten gefährdet würde.“

10. § 181 wird wie folgt gefasst:

„§ 181

Zweckbindung bei Übermittlungen

(1) Von der Vollzugsbehörde an eine öffentliche Stelle übermittelte personenbezogene Daten dürfen nur zu dem Zweck verarbeitet werden, zu dessen Erfüllung sie übermittelt worden sind. Der Empfänger darf die Daten für andere Zwecke nur verarbeiten, soweit sie ihm auch für diese Zwecke hätten übermittelt werden dürfen.

(2) Die Übermittlung an eine nicht-öffentliche Stelle ist nur zulässig, wenn diese sich gegenüber der übermittelnden Vollzugsbehörde verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihr übermittelt werden. Eine Verarbeitung dieser Daten für andere Zwecke ist zulässig, wenn die Daten auch für diese Zwecke hätten übermittelt werden dürfen und die übermittelnde Vollzugsbehörde zugestimmt hat.“

11. § 182 wird wie folgt geändert:

- a) Die Überschrift wird wie folgt gefasst:

„§ 182

Schutz besonderer Kategorien personenbezogener Daten“.

- b) In Absatz 1 Satz 2 wird die Angabe „§ 180 Abs. 8 bis 10“ durch die Wörter „§ 180 Absatz 7 bis 9“ ersetzt.
- c) In Absatz 3 Satz 1 werden nach dem Wort „verarbeitet“ die Wörter „oder genutzt“ gestrichen.

12. § 183 wird wie folgt geändert:

- a) In der Überschrift wird das Wort „Dateien“ durch das Wort „Dateisystemen“ ersetzt.
- b) Absatz 2 wird wie folgt geändert:
- aa) In Satz 1 wird das Wort „Dateien“ durch das Wort „Dateisysteme“ ersetzt und werden nach dem Wort „sind“ die Wörter „nach den Artikeln 24, 25 und 32 der Verordnung (EU) 2016/679“ eingefügt.
- bb) Satz 3 wird aufgehoben.

13. § 184 wird wie folgt geändert:

- a) In der Überschrift wird das Wort „Sperrung“ durch die Wörter „Einschränkung der Verarbeitung“ ersetzt.
- b) In Absatz 1 Satz 1 wird das Wort „Dateien“ durch das Wort „Dateisystemen“ ersetzt.
- c) Absatz 2 wird wie folgt geändert:
- aa) Satz 1 wird wie folgt geändert:
- aaa) In dem Satzteil vor Nummer 1 werden die Wörter „übermittelt oder genutzt“ durch das Wort „verarbeitet“ ersetzt.
- bbb) In Nummer 4 wird das Wort „Freiheitsstrafe“ durch das Wort „Haft nach § 171“ ersetzt.
- bb) In Satz 2 wird das Wort „Freiheitsstrafe“ durch die Wörter „Haft nach § 171“ und werden die Wörter „der Betroffene“ durch die Wörter „die betroffene Person“ ersetzt.
- d) In Absatz 3 Satz 1 werden die Wörter „gesperrten Daten“ durch die Wörter „der eingeschränkten Verwendung unterliegenden Daten“ ersetzt.
- e) Die Absätze 4 und 5 werden aufgehoben.

14. § 185 wird wie folgt geändert:

- a) In der Überschrift werden die Wörter „den Betroffenen“ durch die Wörter „die betroffene Person“ ersetzt.

b) Satz 1 wird durch die folgenden Sätze ersetzt:

„Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit die Voraussetzungen einer Ausnahme nach § 34 Absatz 1 des Bundesdatenschutzgesetzes vorliegen. Steht der betroffenen Person ein Recht auf Auskunft zu, erhält sie Akteneinsicht, soweit eine Auskunft für die Wahrnehmung ihrer rechtlichen Interessen nicht ausreicht und sie hierfür auf die Einsichtnahme angewiesen ist.“

c) In dem neuen Satz 3 werden die Wörter „des Bundesbeauftragten für den Datenschutz in § 19 Abs. 5 und 6 des Bundesdatenschutzgesetzes tritt der Landesbeauftragte für den Datenschutz“ durch die Wörter „der oder des Bundesbeauftragten in § 34 Absatz 3 des Bundesdatenschutzgesetzes tritt die oder der Landesbeauftragte für den Datenschutz“ ersetzt.

15. § 187 wird aufgehoben.

## Artikel 13

### Änderung der Grundbuchordnung

Die Grundbuchordnung in der Fassung der Bekanntmachung vom 26. Mai 1994 (BGBl. I S. 1114), die zuletzt durch Artikel 11 Absatz 18 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist, wird wie folgt geändert:

1. Nach § 12c wird folgender § 12d eingefügt:

#### „§ 12d

##### Anwendung der Verordnung (EU) 2016/679

(1) Das Auskunftsrecht nach Artikel 15 Absatz 1 und das Recht auf Erhalt einer Kopie nach Artikel 15 Absatz 3 der 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) werden dadurch erfüllt, dass die betroffene Person nach Maßgabe des § 12 Absatz 1 und 2 und den dazu erlassenen Vorschriften der Grundbuchverordnung in der jeweils geltenden Fassung Einsicht in das Grundbuch, die Urkunden, auf die im Grundbuch zur Ergänzung einer Eintragung Bezug genommen ist, sowie in die noch nicht erledigten Eintragungsanträge nehmen und eine Abschrift verlangen kann, sowie dadurch, dass die betroffene Person in die nach § 12a Absatz 1 Satz 1 geführten weitere Verzeichnisse Einsicht nehmen kann. Eine Information über Empfänger, gegenüber denen die im Grundbuch oder in den Grundakten enthaltenen personenbezogenen Daten offengelegt werden, erfolgt nur zu Gunsten der Eigentümer des betroffenen Grundstücks oder dem Inhaber eines grundstücksgleichen Rechts nach Maßgabe der von § 12 Absatz 4 Satz 2 bis 4 und der Grundbuchverordnung gesetzten Grenzen.

(2) Hinsichtlich der im Grundbuch enthaltenen personenbezogenen Daten kann das Recht auf Berichtigung nach Artikel 16 der Verordnung (EU) 2016/679 nur unter den Voraussetzungen ausgeübt werden, die in den §§ 894 bis 896 des Bürgerlichen

Gesetzbuchs sowie in den §§ 22 bis 25 und 27 dieses Gesetzes für eine Berichtigung oder Löschung vorgesehen sind.

(3) Das Widerspruchsrecht gemäß Artikel 21 der Verordnung (EU) 2016/679 findet in Bezug auf die im Grundbuch und den Grundakten enthaltenen personenbezogenen Daten keine Anwendung.“

2. § 126 Absatz 1 wird wie folgt geändert:
  - a) In Satz 1 werden die Wörter „**automatisierte Datei**“ durch die Wörter „**automatisiertes Dateisystem**“ ersetzt.
  - b) Satz 2 Nummer 3 wird wie folgt gefasst:

„3. die nach den Artikeln 24, 25 und 32 der Verordnung (EU) 2016/679 erforderlichen Anforderungen erfüllt sind.“
3. In § 131 Absatz 1 Satz 1 werden die Wörter „**automatisierte Datei**“ durch die Wörter „**automatisiertes Dateisystem**“ ersetzt.
4. § 133 wird wie folgt geändert:
  - a) Absatz 5 wird wie folgt geändert:
    - aa) Satz 1 wird aufgehoben.
    - bb) In dem bisherigen Satz 2 werden die Wörter „**Unabhängig hiervon ist dem Eigentümer des Grundstücks oder dem Inhaber eines grundstücksgleichen Rechts**“ durch die Wörter „**Dem Eigentümer des Grundstücks oder dem Inhaber eines grundstücksgleichen Rechts ist**“ ersetzt.
  - b) Absatz 6 wird aufgehoben.
  - c) Absatz 7 wird Absatz 6.
5. In § 134a Absatz 1 Satz 1 werden nach den Wörtern „**Verfügung stellen**“ das Semikolon und die Wörter „**im Übrigen gelten das Bundesdatenschutzgesetz und die Datenschutzgesetze der Länder**“ gestrichen.
6. Die Anlage wird aufgehoben.

## **Artikel 14**

### **Änderung der Grundbuchverfügung**

In § 80 Absatz 1 Satz 2 der Grundbuchverfügung in der Fassung der Bekanntmachung vom 24. Januar 1995 (BGBl. I S. 114), die zuletzt durch Artikel 11 Absatz 19 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist, werden die Wörter „**nach § 133 Abs. 6 der Grundbuchordnung**“ gestrichen.

## Artikel 15

### Änderung der Schiffsregisterordnung

Die Schiffsregisterordnung in der Fassung der Bekanntmachung vom 26. Mai 1994 (BGBl. I S. 1133), die zuletzt durch Artikel 29 des Gesetzes vom 5. Juli 2017 (BGBl. I S. 2208) geändert worden ist, wird wie folgt geändert:

1. Nach § 96 wird folgender § 97 eingefügt:

#### „§ 97

(1) Das Auskunftsrecht nach Artikel 15 Absatz 1 und das Recht auf Erhalt einer Kopie nach Artikel 15 Absatz 3 der 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) werden dadurch erfüllt, dass die betroffene Person nach Maßgabe der §§ 8 und 65 und den dazu erlassenen Vorschriften der Verordnung zur Durchführung der Schiffsregisterordnung in der jeweils geltenden Fassung Einsicht in das Schiffsregister, die Urkunden, auf die im Schiffsregister zur Ergänzung einer Eintragung Bezug genommen ist, sowie in die noch nicht erledigten Eintragungsanträge nehmen und eine Abschrift verlangen kann. Eine Information über Empfänger, gegenüber denen die im Schiffsregister, in Bekanntmachungen der Eintragungen oder in den Registerakten enthaltenen personenbezogenen Daten offengelegt werden, erfolgt nicht.

(2) Hinsichtlich der im Schiffsregister enthaltenen personenbezogenen Daten kann das Recht auf Berichtigung nach Artikel 16 der Verordnung (EU) 2016/679 nur unter den Voraussetzungen ausgeübt werden, die in § 18 des Gesetzes über Rechte an eingetragenen Schiffen und Schiffsbauwerken sowie in den §§ 24, 31 und 35 dieses Gesetzes für eine Berichtigung oder Löschung vorgesehen sind.

(3) Das Widerspruchsrecht gemäß Artikel 21 der Verordnung (EU) 2016/679 findet in Bezug auf die im Schiffsregister und in den Registerakten enthaltenen personenbezogenen Daten keine Anwendung.“

2. Der bisherige § 97 wird § 98.

## Artikel 16

### Änderung der Verordnung zur Durchführung der Schiffsregisterordnung

Die Verordnung zur Durchführung der Schiffsregisterordnung in der Fassung der Bekanntmachung vom 30. November 1994 (BGBl. I S. 3631; 1995 I S. 249), die zuletzt durch Artikel 30 des Gesetzes vom 5. Juli 2017 (BGBl. I S. 2208) geändert worden ist, wird wie folgt geändert:

1. In § 58 werden die Wörter „Anlage zu § 126 Abs. 1 Satz 2 Nr. 3 der Grundbuchordnung“ durch die Wörter „Artikel 24, 25 und 32 der Verordnung (EU) 2016/679“ ersetzt.

2. In § 68 Satz 3 werden die Wörter „in Verbindung mit § 133 Abs. 6 der Grundbuchordnung“ gestrichen.

## Artikel 17

### Änderung der Handelsregisterverordnung

§ 47 Absatz 1 Satz 1 Nummer 3 der Handelsregisterverordnung vom 12. August 1937 (RMBl 1937, 515), die zuletzt durch Artikel 11 Absatz 20 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist, wird wie folgt gefasst:

- "3. die nach den Artikeln 24, 25 und 32 der Verordnung (EU) 2016/679 erforderlichen Anforderungen erfüllt sind, soweit es um personenbezogene Daten geht."

## Artikel 18

### Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen

Das Gesetz über die internationale Rechtshilfe in Strafsachen in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 3 des Gesetzes vom 27. August 2017 (BGBl. I S. 3295) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
  - a) Der Angabe zu § 73 wird folgende Angabe vorangestellt:

„Abschnitt 1

Allgemeine Regelungen“.

- b) Nach der Angabe zu § 77b werden die folgenden Angaben eingefügt:

„Abschnitt 2

Schutz personenbezogener Daten im Rechtshilfeverkehr

§ 77c Anwendungsbereich

§ 77d Übermittlung personenbezogener Daten

§ 77e Prüf-, Informations- und Protokollierungspflichten der übermittelnden Stelle

§ 77f Verfahren bei Fehlen eines Angemessenheitsbeschlusses

§ 77g Zustimmung zur Weiterleitung personenbezogener Daten

§ 77h Verwendung von übermittelten personenbezogenen Daten“.



- c) Nach der Angabe zu § 97 werden die folgenden Angaben eingefügt:

„Elfter Teil

Schutz personenbezogener Daten im Rechtshilfeverkehr innerhalb der Europäischen Union und mit den Schengen-assozierten Staaten

§ 97a Anwendungsbereich

§ 97b Übermittlung personenbezogener Daten

§ 97c Prüf-, Informations- und Protokollierungspflichten der übermittelnden Stelle“.

- d) Die Angabe zum bisherigen Elften Teil wird die Angabe zum Zwölften Teil.

2. Vor § 73 wird folgende Überschrift eingefügt:

„Abschnitt 1

Allgemeine Regelungen“.

3. Nach § 77b wird folgender Abschnitt 2 eingefügt:

„Abschnitt 2

Schutz personenbezogener Daten im Rechtshilfeverkehr

§ 77c

Anwendungsbereich

Die Vorschriften dieses Abschnitts sind auf personenbezogene Daten anzuwenden, die im Rechtshilfeverkehr übermittelt oder empfangen werden.

§ 77d

Übermittlung personenbezogener Daten

(1) Personenbezogene Daten dürfen, soweit dies gesetzlich vorgesehen ist und vorbehaltlich der Regelungen in den §§ 97a und 97b, an öffentliche Stellen anderer Staaten sowie an zwischen- oder überstaatliche Einrichtungen übermittelt werden, wenn

1. dies für die Verhütung oder Verfolgung von Straftaten oder von Ordnungswidrigkeiten oder für die Vollstreckung oder den Vollzug von strafrechtlichen Sanktionen erforderlich ist,
2. die empfangende Stelle für eine der in Nummer 1 genannten Aufgaben zuständig ist,

3. in Fällen, in denen die personenbezogenen Daten von einem anderen Staat oder von einer zwischen- oder überstaatlichen Einrichtung übermittelt wurden, dieser Staat oder die Einrichtung der Übermittlung zuvor zugestimmt oder auf das Zustimmungserfordernis ausdrücklich verzichtet hat,
4. die Europäische Kommission nach Artikel 36 Absatz 3 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) einen Beschluss zum angemessenen Datenschutzniveau des Empfängerstaats oder der empfangenden zwischen- oder überstaatlichen Einrichtung gefasst hat (Angemessenheitsbeschluss) oder die Voraussetzungen von § 77f erfüllt sind und
5. die personenbezogenen Daten in Fällen, in denen sie zu einem anderen als dem der Übermittlung zugrunde liegenden Zweck erhoben wurden, mit vergleichbaren Mitteln auch für den Übermittlungszweck erhoben werden dürften.

(2) Die Übermittlung personenbezogener Daten unterbleibt, auch unter Berücksichtigung eines besonderen öffentlichen Interesses an der Datenübermittlung, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den personenbezogenen Daten im Empfängerstaat oder bei der empfangenden zwischen- oder überstaatlichen Einrichtung nicht hinreichend gesichert ist oder sonst schutzwürdige Interessen der betroffenen Person entgegenstehen.

(3) Die Übermittlung von personenbezogenen Daten an andere als die in Absatz 1 Nummer 2 genannten zuständigen Stellen oder an nicht-öffentliche Stellen ist unter Einhaltung der übrigen Voraussetzungen des Absatzes 1 zulässig, wenn

1. dies für die Erfüllung einer der übermittelnden Stelle zugewiesenen Aufgabe unbedingt erforderlich ist,
2. die Übermittlung an die zuständige Stelle wirkungslos oder ungeeignet wäre, insbesondere, weil die Übermittlung nicht rechtzeitig durchgeführt werden könnte, und
3. die empfangende Stelle auf den Zweck der Datenübermittlung sowie darauf hingewiesen wird, dass eine Verwendung der personenbezogenen Daten nur erfolgen darf, soweit dies zur Zweckerreichung erforderlich ist.

Die zuständige Stelle ist über die Übermittlung unverzüglich zu unterrichten, es sei denn, die Unterrichtung wäre wirkungslos oder ungeeignet.

(4) Kann die nach Absatz 1 Nummer 3 erforderliche vorherige Zustimmung des betroffenen Staates nicht rechtzeitig eingeholt werden, ist die Übermittlung von personenbezogenen Daten auch ohne Zustimmung zulässig, wenn

1. die Daten von einem anderen Mitgliedstaat der Europäischen Union oder von einem Schengen-assoziierten Staat übermittelt wurden und
2. die Übermittlung erforderlich ist zur Abwehr einer gegenwärtigen und erheblichen Gefahr
  - a) für die öffentliche Sicherheit eines Staates oder

- b) für wesentliche Interessen eines Mitgliedstaates der Europäischen Union oder eines Schengen-assozierten Staates.

Die für die Erteilung der Zustimmung zuständige Stelle des betroffenen Staates ist unverzüglich zu unterrichten. Mitgliedstaaten der Europäischen Union im Sinne von Satz 1 sind solche, für welche die Richtlinie (EU) 2016/680 gilt.

(5) Die Verantwortung für die Zulässigkeit der Übermittlung von personenbezogenen Daten trägt die übermittelnde Stelle. Die Möglichkeit, die Übermittlung personenbezogener Daten mit Bedingungen zu versehen, bleibt unberührt.

### § 77e

#### Prüf-, Informations- und Protokollierungspflichten der übermittelnden Stelle

##### (1) Die übermittelnde Stelle

1. soll personenbezogene Daten vor deren Übermittlung auf Richtigkeit, Vollständigkeit und Aktualität überprüfen,
2. fügt bei der Übermittlung personenbezogener Daten nach Möglichkeit Informationen bei, die es der empfangenden Stelle gestatten, Richtigkeit, Vollständigkeit, Aktualität und Zuverlässigkeit der Daten zu beurteilen,
3. weist die empfangende Stelle bei der Übermittlung ausdrücklich darauf hin, dass die übermittelten personenbezogenen Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt wurden,
4. weist die empfangende Stelle ausdrücklich darauf hin, dass eine Weiterleitung an andere Staaten oder zwischen- oder überstaatliche Einrichtungen der vorherigen Zustimmung der übermittelnden Stelle bedarf,
5. weist die empfangende Stelle bei der Übermittlung auf Bedingungen hin, die nach deutschem Recht für die Verarbeitung der übermittelten personenbezogenen Daten gelten und einzuhalten sind, insbesondere auf Fristen, nach deren Ablauf die empfangende Stelle die übermittelten Daten zu löschen, in ihrer Verarbeitung einzuschränken oder daraufhin zu überprüfen hat, ob ihre Speicherung noch erforderlich ist,
6. unterrichtet die empfangende Stelle unverzüglich, wenn sich herausstellt, dass Daten nicht hätten übermittelt werden dürfen oder dass unrichtige Daten übermittelt wurden,
7. unterrichtet die zuständige datenschutzrechtliche Aufsichtsbehörde über Datenübermittlungen nach § 77d Absatz 3 und
8. dokumentiert jede Übermittlung von personenbezogenen Daten nach Maßgabe der innerstaatlichen Vorschriften.

(2) Absatz 1 Nummer 5 gilt entsprechend, wenn die übermittelnde Stelle die Daten von einem anderen Staat oder von einer zwischen- oder überstaatlichen Einrichtung unter Bedingungen erhalten hat, die auch von der empfangenden Stelle einzuhalten sind.

## § 77f

### Verfahren bei Fehlen eines Angemessenheitsbeschlusses

(1) Ohne Angemessenheitsbeschluss gemäß § 77d Absatz 1 Nummer 4 dürfen personenbezogene Daten übermittelt werden, wenn

1. in einem für den Empfängerstaat oder für die empfangende zwischen- oder überstaatliche Einrichtung rechtsverbindlichen Instrument geeignete Garantien zum Schutz personenbezogener Daten vorgesehen sind oder
2. die übermittelnde Stelle nach Bewertung aller relevanten Umstände zu der Auffassung gelangt, dass geeignete Garantien zum Schutz der personenbezogenen Daten bestehen.

(2) Liegen weder ein Angemessenheitsbeschluss noch geeignete Garantien gemäß Absatz 1 vor, dürfen personenbezogene Daten im Einzelfall nur übermittelt werden, wenn dies erforderlich ist

1. zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen Person,
2. zur Wahrung schutzwürdiger Interessen der betroffenen Person,
3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,
4. für die Verhütung oder Verfolgung von Straftaten oder von Ordnungswidrigkeiten oder für die Vollstreckung oder den Vollzug von strafrechtlichen Sanktionen oder
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in Nummer 4 genannten Zwecken.

(3) Die übermittelnde Stelle unterrichtet die zuständige datenschutzrechtliche Aufsichtsbehörde über Fallgruppen von Übermittlungen nach Absatz 1 Nummer 2.

## § 77g

### Zustimmung zur Weiterleitung personenbezogener Daten

Wird die übermittelnde Stelle von der empfangenden Stelle um eine Zustimmung zur Weiterleitung der übermittelten personenbezogenen Daten an andere Staaten oder andere zwischen- oder überstaatliche Einrichtungen gebeten, kann die Zustimmung erteilt werden, wenn eine entsprechende unmittelbare Datenübermittlung gemäß § 77d zulässig wäre.

## § 77h

### Verwendung von übermittelten personenbezogenen Daten

(1) Personenbezogene Daten, die von öffentlichen Stellen anderer Staaten oder von zwischen- oder überstaatlichen Einrichtungen übermittelt wurden, dürfen, soweit dies gesetzlich vorgesehen ist, für andere Zwecke als diejenigen, für die sie übermit-

telt wurden, nur verwendet werden, wenn die übermittelnde Stelle zuvor zugestimmt hat.

(2) Bedingungen für die Verwendung der personenbezogenen Daten, auf die die übermittelnde Stelle hingewiesen hat, sind zu beachten.

(3) Werden personenbezogene Daten ohne Ersuchen übermittelt, prüft die empfangende Stelle unverzüglich, ob die Daten für den Zweck, für den sie übermittelt wurden, benötigt werden.“

4. § 83c Absatz 4 Satz 3 wird wie folgt gefasst:

„Ist die Einhaltung des Termins aufgrund von Umständen unmöglich, die sich dem Einfluss der beteiligten Staaten entziehen, so ist ein neuer Termin zu vereinbaren, nach dem die Übergabe binnen zehn Tagen zu erfolgen hat.“

5. Nach dem Zehnten Teil wird folgender Elfter Teil eingefügt:

## „Elfter Teil

### Schutz personenbezogener Daten im Rechtshilfeverkehr innerhalb der Europäischen Union und mit den Schengen-assozierten Staaten

#### § 97a

##### Anwendungsbereich

(1) Die Vorschriften dieses Teils sind anzuwenden auf personenbezogene Daten, die an Mitgliedstaaten der Europäischen Union, für welche die Richtlinie (EU) 2016/680 gilt, oder an Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union übermittelt oder von diesen empfangen werden.

(2) Schengen-assozierte Staaten stehen den Mitgliedstaaten der Europäischen Union bei der Anwendung dieses Teils gleich.

(3) Soweit dieser Teil keine besonderen Regelungen enthält, sind die Bestimmungen des Abschnitts 2 des Siebenten Teils anzuwenden.

#### § 97b

##### Übermittlung personenbezogener Daten

§ 77d gilt mit der Maßgabe, dass keine Anwendung finden

1. Absatz 1 Nummer 2, auch in Verbindung mit Absatz 3 und § 77e Absatz 1 Nummer 7, und
2. Absatz 1 Nummer 4 in Verbindung mit § 77f.

§ 97c

Prüf-, Informations- und Protokollierungspflichten der übermittelnden Stelle

Zusätzlich zu den in § 77e genannten Pflichten gilt, dass der Stelle eines anderen Mitgliedstaates der Europäischen Union, von der oder an die personenbezogene Daten übermittelt wurden, bei einer Verletzung des Schutzes der personenbezogenen Daten unverzüglich die in § 65 Absatz 3 des Bundesdatenschutzgesetzes genannten Informationen mitzuteilen sind.“

6. Der bisherige Elfte Teil wird der Zwölfte Teil.

## Artikel 19

### Änderung des Fünften Gesetzes zur Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen

Artikel 1 des Fünften Gesetzes zur Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen vom 1. Juni 2017 (BGBl. I S. 1414) wird wie folgt geändert:

1. Nummer 1 wird wie folgt geändert:
  - a) In Buchstabe a werden die Angabe „97“ durch die Angabe „97c“, die Wörter „Elfter Teil“ durch die Wörter „Zwölfter Teil“ und die Wörter „Elften Teils“ durch die Wörter „Zwölften Teils“ ersetzt.
  - b) In Buchstabe b werden die Wörter „Elften Teil“ durch die Wörter „Zwölften Teil“ und die Wörter „Zwölften Teil“ durch die Wörter „Dreizehnten Teil“ ersetzt.
2. In Nummer 3 werden die Wörter „Zehnten und Elften Teil“ durch die Wörter „Zehnten und Zwölften Teil“ ersetzt.
3. Nummer 4 wird aufgehoben.
4. In Nummer 5 werden die Wörter „Zehnten Teil“ durch die Wörter „Elften Teil“, jeweils die Wörter „Elfter Teil“ durch die Wörter „Zwölfter Teil“ und die Wörter „Elften Teils“ durch die Wörter „Zwölften Teils“ ersetzt.
5. In Nummer 6 werden die Wörter „Elfte Teil“ durch die Wörter „Zwölfte Teil“ und die Wörter „Zwölfter Teil“ durch die Wörter „Dreizehnter Teil“ ersetzt.

## Artikel 20

### Änderung der Eurojust-Anlaufstellen-Verordnung

Die Eurojust-Anlaufstellen-Verordnung vom 17. Dezember 2004 (BGBl. I S. 3520), die zuletzt durch Artikel 167 der Verordnung vom 31. August 2015 (BGBl. I S. 1474) geändert worden ist, wird wie folgt geändert:

1. § 2 Absatz 3 Satz 2 wird wie folgt gefasst:

„§ 64 des Bundesdatenschutzgesetzes bleibt unberührt.“

2. In § 5 Absatz 1 werden die Wörter „§ 485 Satz 1, § 487 Abs. 6, § 489 Abs. 1 und 2 Satz 1, 2 Nr. 3 sowie § 491 Abs. 1 und 2 der Strafprozessordnung“ durch die Wörter „§ 485 Satz 1, § 487 Absatz 6, 489 Absatz 1 Nummer 3 sowie § 491 der Strafprozessordnung“ ersetzt.

## Artikel 21

### Änderung des Auslandsunterhaltsgesetzes

Das Auslandsunterhaltsgesetz vom 23. Mai 2011 (BGBl. I S. 898), das zuletzt durch Artikel 5 des Gesetzes vom 20. November 2015 (BGBl. I S. 2018) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht werden in der Angabe zu § 19 die Wörter „und Löschung“ gestrichen.
2. § 19 wird wie folgt geändert.
  - a) In der Überschrift werden die Wörter „und Löschung“ gestrichen.
  - b) Die Absatzbezeichnung „(1)“ wird gestrichen.
  - c) Absatz 2 wird aufgehoben.

## Artikel 22

### Änderung des Bürgerlichen Gesetzbuchs

Das Bürgerliche Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 1 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2787) geändert worden ist, wird wie folgt geändert:

1. § 55a Absatz 1 Satz 2 wird wie folgt geändert:
  - a) In Nummer 2 wird das Komma durch das Wort „und“ ersetzt.
  - b) Nummer 3 wird wie folgt gefasst:

„3. die nach den Artikeln 24, 25 und 32 der Verordnung (EU) 2016/679 erforderlichen Anforderungen erfüllt sind.“
2. Nach § 79 wird folgender § 79a eingefügt:

„§ 79a

Anwendung der Verordnung (EU) 2016/679 im Registerverfahren

(1) Die Rechte nach Artikel 15 der 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) werden nach § 79 und den dazu erlassenen Vorschriften der Vereinsregisterverordnung durch Einsicht in das Register oder den Abruf von Registerdaten über das länderübergreifende Informations- und Kommunikationssystem gewährt. Das Registergericht ist nicht verpflichtet, Personen, deren personenbezogene Daten im Vereinsregister oder in den Registerakten gespeichert sind, über die Offenlegung dieser Daten an Dritte Auskunft zu gewähren.

(2) Das Recht auf Berichtigung nach Artikel 16 der Verordnung (EU) 2016/679 kann für personenbezogene Daten, die im Vereinsregister oder den Registerakten gespeichert sind, nur unter den Voraussetzungen und in dem Verfahren ausgeübt werden, die im Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit sowie der Vereinsregisterverordnung für eine Löschung oder Berichtigung von Eintragungen geregelt sind.

(3) Das Widerspruchsrecht nach Artikel 21 der Verordnung (EU) 2016/679 ist auf personenbezogene Daten, die im Vereinsregister und in den Registerakten gespeichert sind, nicht anzuwenden.“

3. § 1563 wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

„§ 1563

Registereinsicht; Anwendung der Verordnung (EU) 2016/679 im Registerverfahren“.

b) Der Wortlaut wird Absatz 1.

c) Die folgenden Absätze 2 und 3 werden angefügt:

„(2) Die Rechte nach Artikel 15 der Verordnung (EU) 2016/679 werden nach Absatz 1 durch Einsicht in das Register gewährt. Das Registergericht ist nicht verpflichtet, Personen, deren personenbezogene Daten im Güterrechtsregister oder in den Registerakten gespeichert sind, über die Offenlegung dieser Daten an Dritte Auskunft zu gewähren.

(3) Im Übrigen gilt § 79a Absatz 2 und 3 entsprechend.“

## Artikel 23

### Änderung der Luftfahrzeugpfandrechtsregisterverordnung

In § 11 Absatz 2 der Luftfahrzeugpfandrechtsregisterverordnung vom 2. März 1999 (BGBl I S. 279), die zuletzt durch Artikel 4 Absatz 12 des Gesetzes vom 11. August 2009



(BGBl. I S. 2713) geändert worden ist, werden die Wörter „Anlage zu § 126 Abs. 1 Satz 2 Nr. 3 der Grundbuchordnung“ durch die Wörter „Artikel 24, 25 und 32 der Verordnung (EU) 2016/679“ ersetzt.

## Artikel 24

### Folgeänderungen

(1) In § 28a Absatz 4 Satz 1 des Bundespolizeigesetzes vom 19. Oktober 1994 (BGBl. I S. 2978, 2979), das zuletzt durch Artikel 1 des Gesetzes vom 5. Mai 2017 (BGBl. I S. 1066) geändert worden ist, werden die Wörter „§ 161 Absatz 2 und 3“ gestrichen.

(2) In § 8 Absatz 2 Satz 1 des Anti-Doping-Gesetzes vom 10. Dezember 2015 (BGBl. I S. 2210), das zuletzt durch Artikel 6 Absatz 5 des Gesetzes vom 13. April 2017 (BGBl. I S. 872) geändert worden ist, werden die Wörter „§ 477 Absatz 1, 2 und 5 sowie § 478 Absatz 1 und 2“ durch die Wörter „Die § 478, 479 Absatz 2 und 6 sowie § 480 Absatz 1 und 2“ ersetzt.

(3) In § 59 Absatz 1 Nummer 3 des IStGH-Gesetzes vom 21. Juni 2002 (BGBl. I S. 2144), das zuletzt durch Artikel 13 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202) geändert worden ist, wird die Angabe „§ 477 Abs. 2 Satz 2“ durch die Wörter „§ 479 Absatz 2 Satz 1“ ersetzt.

(4) In § 17 Absatz 1 Satz 3 des Schwarzarbeitsbekämpfungsgesetzes vom 23. Juli 2004 (BGBl. I S. 1842), das zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2739) geändert worden ist, werden die Wörter „§ 478 Abs. 1 Satz 1 und 2“ durch die Wörter „§ 480 Absatz 1 Satz 1 und 2“ ersetzt.

(5) Das Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), das zuletzt durch Artikel 5 des Gesetzes vom 27. August 2017 (BGBl. I S. 3295) geändert worden ist, wird wie folgt geändert:

1. § 49a wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Satz 1 wird wie folgt geändert:

aaa) In Nummer 3 wird die Angabe „§ 479 Abs. 2“ durch die Angabe „§ 477 Absatz 2“ ersetzt.

bbb) In dem Satzteil nach Nummer 3 wird die Angabe „§ 478 Abs. 1“ durch die Angabe „§ 480 Absatz 1“ ersetzt.

bb) Satz 2 wird wie folgt gefasst.

„Die §§ 478, 479 Absatz 1, 2 und 6 sowie 480 Absatz 1 und 2 der Strafprozessordnung gelten sinngemäß.“

b) Absatz 5 Satz 1 wird wie folgt gefasst:

„§ 481 der Strafprozessordnung ist sinngemäß anzuwenden.“

2. § 49b wird wie folgt geändert:

- a) Vor dem Satzteil vor Nummer 1 wird die Angabe „bis 478“ durch die Wörter „bis 476, 478 bis 481“ ersetzt.
- b) In Nummer 2 wird die Angabe „, § 480“ gestrichen.
- c) In Nummer 3 wird die Angabe „§ 477 Abs. 2 Satz 1“ durch die Angabe „§ 479 Absatz 1“ ersetzt.
- d) In Nummer 4 wird nach der Angabe „und 3“ das Komma und die Angabe „§ 477 Abs. 3 Nr. 2“ durch die Angabe „§ 479 Absatz 4 Nummer 2“ ersetzt.
- e) In Nummer 5 wird die Angabe „§ 478 Abs. 3 Satz 1“ durch die Angabe „§ 480 Absatz 3 Satz 1“ ersetzt.

(6) In § 3 Absatz 2 Satz 2 des ZIS-Ausführungsgesetzes vom 31. März 2004 (BGBl. I S. 482), das zuletzt durch Artikel 8 Absatz 9 des Gesetzes vom 3. Dezember 2015 (BGBl. I S. 2178) geändert worden ist, werden die Wörter „§ 478 Absatz 1 Satz 1 und 2“ durch die Wörter „§ 480 Absatz 1 Satz 1 und 2“ ersetzt.

## **Artikel 25**

### **Inkrafttreten**

Dieses Gesetz tritt am 25. Mai 2018 in Kraft.

## **Begründung**

### **A. Allgemeiner Teil**

#### **I. Zielsetzung und Notwendigkeit der Regelungen**

Die Mitgliedstaaten sind verpflichtet, bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften zu erlassen, die erforderlich sind, um der Richtlinie (EU) 2016/680 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) (Richtlinie (EU) 2016/680) nachzukommen.

Darüber hinaus wird ab dem 25. Mai 2018 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) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein. Ziel der Datenschutz-Grundverordnung, die grundsätzlich auch für die Tätigkeit der Gerichte und der Justizbehörden gilt (vgl. den dortigen Artikel 2 und Erwägungsgrund 20), ist ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten in allen Mitgliedstaaten (Erwägungsgrund 10). Der Unionsgesetzgeber hat sich für die Handlungsform einer Verordnung entschieden, damit innerhalb der Union ein gleichmäßiges Datenschutzniveau für natürliche Personen gewährleistet ist (Erwägungsgrund 13). Die Datenschutz-Grundverordnung sieht eine Reihe von Öffnungsklauseln für den nationalen Gesetzgeber vor. Zugleich enthält die Datenschutz-Grundverordnung konkrete, an die Mitgliedstaaten gerichtete, Regelungsaufträge. Dies erfordert es, das allgemeine wie auch das bereichsspezifische nationale Datenschutzrecht auf die Vereinbarkeit mit der Datenschutz-Grundverordnung zu überprüfen und soweit nötig anzupassen.

Diesen Zwecken dient bereits die Neufassung des Bundesdatenschutzgesetzes (BDSG (2018)) durch das am 25. Mai 2018 in Kraft tretende Datenschutz-Anpassungs- und -Umsetzungsgesetz EU vom 30. Juni 2017 (BGBl. I S. 2097) (DSAnpUG-EU) zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680. Die hierin vorgesehenen allgemeinen datenschutzrechtlichen Bestimmungen, die auch für die gerichtlichen Verfahrensordnungen und die Gerichte den subsidiär geltenden datenschutzrechtlichen Rahmen bilden (vgl. § 1 Absatz 2 BDSG (2018)), sind unter Berücksichtigung der Besonderheiten des jeweiligen Verfahrensrechts bereichsspezifisch zu modifizieren.

Der vorliegende Entwurf dient der Umsetzung der Richtlinie (EU) 2016/680 vom 27. April 2016 sowie der bereichsspezifischen Modifikation des Strafverfahrensrechts im Zuge der Anpassung an die Datenschutzgrundverordnung.

#### **II. Wesentlicher Inhalt des Entwurfs**

Der Entwurf sieht folgende Gesetzesänderungen vor:

## **1. Gesetzesänderungen im Anwendungsbereich der Richtlinie (EU) 2016/680**

Im Anwendungsbereich der Richtlinie (EU) 2016/680 werden die zu deren Umsetzung geschaffenen Regelungen des DSAnpUG-EU zum 3. Teil des BDSG (2018) bereichsspezifisch ergänzt.

Der Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60 – im Folgenden: Rb Datenschutz), wird durch Artikel 59 der Richtlinie (EU) 2016/680 aufgehoben. Die Bundesregierung hatte zur Umsetzung des Rb Datenschutz einen Gesetzentwurf vorgelegt (Bundestagsdrucksache 18/6285), der angesichts der im Mai 2016 erfolgten Verkündung der Richtlinie (EU) 2016/680 und ihrer beabsichtigten zügigen Umsetzung nicht mehr zur Beratung im Deutschen Bundestag aufgerufen wurde. Eine Umsetzung des Rb Datenschutz erschien nicht mehr sachgerecht, weil die Richtlinie (EU) 2016/680 abweichende Vorgaben enthält, beispielsweise mit Blick auf die Zulässigkeit einer Zweckänderung.

Die Richtlinie (EU) 2016/680 gilt – anders als noch der Rb Datenschutz – nicht nur für grenzüberschreitende, sondern auch für rein innerstaatliche Sachverhalte. Daraus ergibt sich ein anderer Umsetzungsansatz als seinerzeit beim Rb Datenschutz (siehe insoweit Bundestagsdrucksache 18/6285, S. 10 ff.). Die erforderlichen Anpassungen erfolgen im Grundsatz im nationalen Datenschutzrecht und in den Verfahrensordnungen.

Wie sich aus § 1 Absatz 2 Satz 1 BDSG (2018) ergibt, hat das BDSG (2018) im Verhältnis zu bereichsspezifischen datenschutzrechtlichen Vorschriften den Charakter eines „Auf-fanggesetzes“: Spezifische Rechtsvorschriften des Bundes genießen gegenüber den Vorschriften des BDSG (2018) grundsätzlich Vorrang. Liegt keine bereichsspezifische Datenschutzregelung für einen vergleichbaren Sachverhalt vor, so kommen die Vorschriften des BDSG (2018) zur Anwendung. Bei einer nur teilweisen Regelung oder im Falle des Schweigens eines bereichsspezifischen Gesetzes kommt es maßgeblich darauf an, ob die spezifischen Regelungen des jeweiligen Gesetzes für einen bestimmten Bereich insgesamt umfassend und damit abschließend die Datenverarbeitung regeln sollen. Wenn dies nicht der Fall ist, kann subsidiär auf die Vorschriften des BDSG (2018) zurückgegriffen werden.

### **a) Strafprozessordnung (StPO) (Artikel 1)**

Innerhalb der StPO werden die in Teil 3 des BDSG (2018) vorgesehenen Bestimmungen zur Umsetzung der Richtlinie (EU) 2016/680 berücksichtigt und bereichsspezifisch ergänzt bzw. die bereits vorhandenen bereichsspezifischen Sonderregelungen angepasst.

Dem mit dem Entwurf verfolgten Ansatz entsprechend verbleibt ein sehr weitreichender Anwendungsspielraum für die Regelungen in Teil 3 des BDSG (2018). Diese sollen für den Bereich des Strafverfahrens grundsätzlich technikneutral zur Anwendung kommen, d. h. unabhängig davon, ob personenbezogene Daten elektronisch oder in Papierakten verarbeitet werden.

D. h. für die Anwendungspraxis, dass Ausgangspunkt für die Bestimmung der datenschutzrechtlichen Pflichten immer Teil 3 des BDSG (2018) sein wird und dann ergänzend zu prüfen ist, ob bereichsspezifische Sonderregelungen bestehen. Hieraus ergibt sich für die Praxis also ein neuartiges Regelungsgefüge, so dass es zweckmäßig erscheint, ihr hierzu nähere Hinweise im Rahmen einer Überarbeitung der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) an die Hand zu geben. Allgemein lässt sich Folgendes ausführen:

Soweit die StPO eigene datenschutzrechtliche Vorschriften enthält, treten sie ergänzend neben die allgemeinen Regelungen des BDSG (2018). So enthält das BDSG (2018) bei-

spielsweise allgemeine Vorgaben für die Anforderungen an die datenschutzrechtliche Einwilligung einer betroffenen Person (§ 51 BDSG (2018)). Unter welchen Umständen die Einwilligung der betroffenen Person aber gerade im Strafverfahren für die Verarbeitung personenbezogener Daten maßgeblich sein kann, ergibt sich aber aus der StPO selbst (z. B. aus § 161 Absatz 3 der Strafprozessordnung in der Entwurfsfassung (StPO-E)). Ähnlich verhält es sich mit der Verarbeitung besonderer Kategorien personenbezogener Daten im Strafverfahren: Dass diese grundsätzlich auch im Strafverfahren erfolgen darf, ergibt sich aus der StPO (§ 161 Absatz 2 StPO-E), ergänzende Anforderungen an die Verarbeitung sind in § 48 BDSG (2018) geregelt.

Ein weiteres Beispiel ist die im Entwurf vorgesehene Regelung zu automatisierten Verfahren für Datenübermittlungen in § 488 StPO-E, die, etwa zur Protokollierung, punktuell ergänzende bereichsspezifische Regelungen enthält, soweit diese über die Anforderungen des BDSG (2018) hinausgehen.

Ähnlich verhält es sich bei den sonstigen bereichsspezifischen Sonderregelungen zu Löschungspflichten in Bezug auf personenbezogene Daten innerhalb der StPO. Diese finden sich z. B. in den § 81h Absatz 3 Satz 3, § 98b Absatz 3 Satz 2, § 100d Absatz 2 Satz 2, Absatz 3 Satz 2, § 100g Absatz 4 Satz 3, § 160a Absatz 1 Satz 3, § 163d Absatz 4 Satz 2 und § 479 Absatz 3 StPO-E. Auch die Regelungen zur Löschung elektronischer Aktenkopien (§ 499 der Strafprozessordnung in der Fassung des Gesetzesentwurfs zur Einführung der elektronischen Akte in Strafsachen und zur weiteren Förderung des elektronischen Rechtsverkehrs, Bundestagsdrucksache 18/9416) sowie zur Aufbewahrung und Speicherung von Akten (vgl. für den Bund das Justizaktenaufbewahrungsgesetz in der Fassung des o. g. Gesetzesentwurfs) stellen insofern bereichsspezifische Regelungen zu Löschungspflichten bzgl. personenbezogener Daten dar.

Aus ihnen ergeben sich zwar besondere rechtliche Verpflichtungen zur Löschung im Sinne von § 75 Absatz 2 BDSG (2018). § 75 BDSG (2018) findet im Übrigen aber grundsätzlich Anwendung, wie z. B. die durch den Verweis in § 75 Absatz 3 BDSG (2018) erfassten Mitteilungspflichten des § 58 Absatz 5 BDSG (2018). Eine Einschränkung ist insofern lediglich in § 161 Absatz 2 StPO-E vorgesehen, wonach die Ausnahmeregel des § 58 Absatz 3 BDSG (2018), auf welche § 75 Absatz 3 BDSG (2018) verweist, nicht zur Anwendung kommt, soweit die Löschung personenbezogener Daten innerhalb der StPO ausdrücklich angeordnet wird.

Die vorgenannten bereichsspezifischen Sonderregelungen zu Löschungspflichten verdrängen auch die weiteren in § 75 BDSG (2018) geregelten Berichtigungs- und Löschungspflichten grundsätzlich nicht. Für letztere ist allerdings nur ein sehr begrenzter praktischer Anwendungsbereich zu erwarten. Dies gilt insbesondere für die in § 75 Absatz 2 BDSG (2018) erwähnte Pflicht zur Löschung, wenn die Verarbeitung personenbezogener Daten unzulässig ist. Dass einmal erhobene Daten innerhalb eines Strafverfahrens nicht verwendet werden dürfen, kann in strafprozessualer Hinsicht z. B. durch die rechtswidrige Erhebung der Daten begründet sein. Soweit nicht ausdrücklich anders vorgesehen (vgl. z. B. § 100g Absatz 4 Satz 3 StPO) steht dies jedoch nicht jeder Form der weiteren technischen Verarbeitung entgegen. In der Regel wird die weitere Verarbeitung in der Verfahrensakte schon aus Gründen der Aktenwahrheit, -klarheit und -vollständigkeit geboten sein oder es werden zumindest die durch § 75 Absatz 3 Satz 1 BDSG (2018) in Bezug genommenen Ausnahmetatbestände des § 58 Absatz 3 BDSG (2018) eingreifen.

Auch die bereichsspezifischen Sonderregelungen zur Berichtigung und Löschung personenbezogener Daten und zur Einschränkung ihrer Verarbeitung in Dateisystemen werden entsprechend überarbeitet. Die §§ 489 und 494 StPO sehen in ihrer bisherigen Fassung umfassende Regelungen zur Berichtigung, Löschung bzw. Einschränkung der Verarbeitung vor. Diese wurden nun den Vorgaben der Richtlinie (EU) 2016/680 (insbesondere Artikel 7 Absatz 3 und Artikel 16 Absatz 3) entsprechend angepasst. Dabei soll aus rechtssystematischer Sicht im Hinblick auf die Regelungen im 3. Teil des BDSG (2018)

nur das an dieser Stelle geregelt werden, was einer besonderen Behandlung im Strafverfahren bedarf. Im Übrigen gelten die Vorschriften des Bundesdatenschutzgesetzes (insbesondere § 75 BDSG (2018)).

Schließlich wird auch eine bisherige Sonderregelung zum allgemeinen datenschutzrechtlichen Auskunftsanspruch aufgehoben. So wird die bisher in § 491 Absatz 1 Satz 1 StPO vorgesehene und in § 495 Absatz 1 Satz 1 StPO auch für das Zentrale Staatsanwaltschaftliche Verfahrensregister in Bezug genommene Ausschlussklausel zu datenschutzrechtlichen Auskunftsansprüchen bei Dateisystemen dahingehend abgeändert, dass das allgemeine Auskunftsrecht des Bundesdatenschutzgesetzes Anwendung finden soll und nicht mehr durch andere, in der StPO geregelte Auskunfts- oder Akteneinsichtsrechte verdrängt wird. Zum Zwecke der Klarstellung, dass der in § 57 BDSG (2018) geregelte Auskunftsanspruch auch im Übrigen, d. h. auch bei personenbezogenen Daten außerhalb von Dateisystemen im Sinne des 8. Buches, nicht durch die in der StPO vorgesehenen Auskunftsrechte ausgeschlossen wird, wird zudem auch ein entsprechender Hinweis in § 475 Absatz 1 StPO-E aufgenommen.

Darüber hinaus erfolgen redaktionelle Anpassungen an die in der Richtlinie (EU) 2016/680 bzw. dem BDSG (2018) verwendeten Begriffe.

Anlässlich der Richtlinienumsetzung werden die Regelungen zur verfahrensübergreifenden Weitergabe bzw. verfahrensübergreifenden Verarbeitung von Daten systematisch überarbeitet und in den §§ 161 und 479 StPO-E gebündelt.

Der Regelungsgehalt der bisherigen Vorschriften bleibt hierbei jedoch in seiner Grundstruktur unverändert und wird den Vorgaben der Richtlinie (EU) 2016/680 angepasst.

Zusätzlich wird in § 479 Absatz 2 Satz 2 Nummer 2 StPO-E die Verwendung strafprozessual erhobener personenbezogener Daten zu Zwecken der Gefahrenabwehr neu geregelt, um den Anforderungen des Bundesverfassungsgerichts (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09) zum Grundsatz der hypothetischen Neuerhebung umfassend Rechnung zu tragen.

## **b) Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) (Artikel 18)**

Die Regelungen zu grenzüberschreitenden Sachverhalten im IRG können auf die Verfahrensvorschriften der StPO und des Gesetzes über Ordnungswidrigkeiten (OWiG), sowie das BDSG (2018) ganz überwiegend Bezug nehmen; gesonderter Umsetzungsbedarf im IRG entsteht damit nur punktuell.

Umsetzungsbedarf im IRG lösen vor allem die Artikel 7, 9 (allgemeine Grundsätze bezüglich Speicherfristen und Unterscheidungen bei personenbezogenen Daten) und die Artikel 35 bis 39 (Regelungen zur Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen) der Richtlinie (EU) 2016/680 aus. Schon bisher sind bereichsspezifische und allgemeine datenschützende Vorschriften im Rechtshilfeverfahren zu beachten. Ergänzend dazu sollen im IRG künftig für den Rechtshilfeverkehr mit Drittstaaten und internationalen Organisationen sowie auch für den Rechtshilfeverkehr innerhalb der Europäischen Union bereichsspezifische Vorschriften für den grenzüberschreitenden Datenaustausch gelten. Die Schengen-assoziierten Staaten werden den Mitgliedstaaten der Europäischen Union in datenschutzrechtlicher Hinsicht gleichgestellt.

Artikel 35 der Richtlinie (EU) 2016/680 führt die einzelnen Voraussetzungen für die Übermittlung personenbezogener Daten an Drittstaaten und an internationale Organisationen auf. Die Vorgaben werden mit den §§ 77d, 77g und 97b des Gesetzes über die internationale Rechtshilfe in Strafsachen in der Entwurfsfassung (IRG-E) umgesetzt.

Artikel 36 der Richtlinie (EU) 2016/680 ergänzt Artikel 35 Absatz 1 Buchstabe d der Richtlinie (EU) 2016/680 und sieht vor, dass personenbezogene Daten an Drittstaaten und an internationale Organisationen übermittelt werden dürfen, wenn ein sogenannter Angemessenheitsbeschluss der Europäischen Kommission vorliegt. Die Regelung wird mit § 77d Absatz 1 Nummer 4 IRG-E umgesetzt.

Artikel 37 und Artikel 38 der Richtlinie (EU) 2016/680 regeln die Voraussetzung einer Datenübermittlung an Drittstaaten oder internationale Organisationen in Fällen, in denen es an einem Angemessenheitsbeschluss der Europäischen Kommission fehlt. Die Umsetzung erfolgt durch § 77f IRG-E.

Artikel 39 der Richtlinie (EU) 2016/680 regelt Fälle, in denen eine Datenübermittlung abweichend von Artikel 35 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/680 direkt an in Drittstaaten niedergelassene Empfänger möglich ist, die nicht die zuständigen Strafverfolgungsbehörden oder Gerichte sind. Nach Artikel 39 Absatz 1 Buchstabe d der Richtlinie (EU) 2016/680 ist dies der zuständigen Behörde im Drittstaat unverzüglich mitzuteilen. Die Vorgaben werden mit § 77d Absatz 3 und § 77e Absatz 1 Nummer 7 IRG-E umgesetzt.

Darüber hinaus soll durch die Änderung des IRG auch den Anforderungen entsprochen werden, die nach der Rechtsprechung des Bundesverfassungsgerichts an die Datenübermittlung ins Ausland auf der Grundlage des Bundeskriminalamtgesetzes (BKAG) zu stellen sind (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09), soweit diese verfassungsgerichtlichen Vorgaben auf die justizielle Rechtshilfe in Strafsachen nach dem IRG übertragbar sind. Geregelt werden insoweit etwa die Voraussetzungen für eine Zweckänderung (§ 77d Absatz 1 Nummer 5 IRG-E), eine Hinweispflicht auf die Zweckbindung übermittelter personenbezogener Daten (§ 77e Absatz 1 Nummer 3 IRG-E) und Protokollierungspflichten (§ 77e Absatz 1 Nummer 8 IRG-E). Im Zusammenhang mit den im BKAG vorgesehenen Regelungen zur Übermittlung von personenbezogenen Daten an ausländische Behörden hält das Bundesverfassungsgericht auch Berichtspflichten gegenüber Parlament und Öffentlichkeit für erforderlich, um ausreichende Transparenz und Kontrolle zu gewährleisten (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 354 in Verbindung mit Rn. 142 f.). Diese auf die polizeiliche Rechtshilfe nach dem BKAG zugeschnittene Aussage löst indes keinen Anpassungsbedarf im IRG aus. § 101b enthält mit Blick auf verdeckte Ermittlungsmaßnahmen bereits Berichtspflichten für das (auch grenzüberschreitende) Strafverfahren. Hinzu kommt, dass die Verfahren der justiziellen Rechtshilfe in Strafsachen bereits eine ausreichende Transparenz und Kontrolle sicherstellen: Hier sind zum einen stets justizielle Behörden und Gerichte beteiligt. Zum anderen sind im Rahmen der justiziellen Rechtshilfe nicht nur die strafprozessualen Vornahmehandlungen gerichtlich überprüfbar, sondern auch die – positiven oder negativen – Bewilligungsentscheidungen, die eine Vornahmehandlung erst ermöglichen.

Die neuen Vorschriften ergänzen die schon bisher vorhandenen datenschützenden Regelungen des IRG, beispielsweise die §§ 61a, 61b Absatz 3 und 4 IRG sowie die §§ 92b, 92c und 93 Absatz 3 und 4 IRG. Soweit das IRG also bereits datenschützende Standards enthält, die strenger sind als die der neu eingefügten Normen, bleiben erstere zu beachten. Dies kann insbesondere bei § 61a Absatz 2 Buchstabe c IRG praktische Relevanz haben, wonach Datenübermittlungen ohne Ersuchen obligatorisch mit bestimmten Bedingungen zu verbinden sind. Gleiches gilt für § 92b IRG, der eine Zweckänderung bei der Verarbeitung von personenbezogenen Daten, die im Rahmen der sogenannten Schwedischen Initiative ausgetauscht wurden, nur unter sehr engen Voraussetzungen zulässt. Die Richtlinie (EU) 2016/680 will lediglich ein datenschutzrechtliches Mindestniveau schaffen und lässt gemäß ihrem Artikel 1 Absatz 3 den Fortbestand strengerer nationaler Vorschriften ausdrücklich zu.

Eine inhaltliche und sprachliche Anpassung der existierenden datenschützenden Vorschriften des IRG an den neuen Abschnitt 2 des Siebenten Teils und an den neuen Elften

Teil unterbleibt bewusst. Andernfalls könnte der Eindruck entstehen, die Umsetzung der Richtlinie (EU) 2016/680 führe zu einer Absenkung des bisherigen Datenschutzniveaus im IRG. Die Rechtspraxis muss somit die bisherigen und die neuen Datenschutzregelungen nebeneinander beachten. Dieses Vorgehen ist nicht neu. Schon bisher waren die punktuellen datenschützenden Vorschriften im IRG neben denen der ratifizierten internationalen Übereinkommen zu beachten, siehe etwa Artikel 23 des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union vom 29. Mai 2000 (BGBl. 2005 II S. 661, 662; im Folgenden: EU-RhÜbk). Sollten in der Rechtspraxis gleichwohl künftig Probleme auftreten, kann dies im Rahmen der Novellierung des IRG berücksichtigt werden, die für die bevorstehende Legislaturperiode geplant ist.

Die neuen Vorschriften im IRG ergänzen auch die datenschützenden Vorschriften der StPO und des OWiG; letztere bleiben zusätzlich zu beachten. Es werden keine neuen Befugnisnormen für die zuständigen Behörden geschaffen, sondern die Vorschriften grenzen bestehende Ermächtigungen zur Datenübermittlung ein. Die datenschützenden Regelungen des IRG sind dabei von den deutschen Strafverfolgungsbehörden zu beachten, auch nachdem personenbezogene Daten, die deutsche Behörden im Wege der strafrechtlichen Zusammenarbeit aus dem Ausland erhalten haben, Teil eines im Inland geführten Strafverfahrens geworden sind. Eine sachgerechte Handhabung der datenschützenden Regelungen, insbesondere des rechtshilferechtlichen Zustimmungserfordernisses bei einer (auch rein innerstaatlichen) Zweckänderung bei der Verwendung von Fremddaten, wird in der Rechtspraxis bedeuten, dass die betroffenen personenbezogenen Daten gegebenenfalls zu kennzeichnen sind, vgl. hierzu bereits die Bundestagsdrucksache 18/6285, S. 28.

Dies entspricht dem schon bisher geltenden Verhältnis zwischen dem Rechtshilferecht und dem nationalen Verfahrensrecht. Die datenschützenden Vorgaben aus dem Rechtshilfeverfahren können ein engeres Korsett bilden als etwa die Vorschriften der StPO, und dieses Korsett kann auch im innerstaatlichen Umgang mit den Daten nicht abgelegt werden. Daraus folgt nicht, dass die datenschützenden Regelungen der StPO durch das IRG verdrängt würden, wenn die betroffenen personenbezogenen Daten grenzüberschreitend erlangt wurden. Bei ausgehenden personenbezogenen Daten ist über § 59 Absatz 3 IRG sichergestellt, dass innerstaatliche Vorgaben der Verfahrensordnungen beachtet werden. Die bereichsspezifischen datenschützenden Vorschriften des IRG sind im Rechtshilfeverkehr zusätzlich zu den Vorgaben der StPO zu beachten.

Soweit das IRG keine bereichsspezifischen datenschützenden Vorschriften enthält, bleibt wie bisher gemäß § 77 Absatz 1 IRG ein Rückgriff vor allem auf die Verfahrensvorschriften der StPO und des OWiG möglich. Möglich bleibt zudem ein Rückgriff auf allgemeine datenschützende Vorschriften wie die des BDSG (2018).

### **c) Weitere Anpassungen redaktioneller Natur**

Über die oben genannten Änderungen hinaus sind Folgeänderungen und redaktionelle Anpassungen in Bezug auf Verweise auf das BDSG (2018) sowie an die in der Richtlinie (EU) 2016/680 bzw. dem BDSG (2018) verwendeten Begriffe vorgesehen

- innerhalb der Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters (ZStVBetrV) (Artikel 11) und
- der Eurojust-Anlaufstellen-Verordnung (Artikel 19).

### **d) Verhältnis zu anderen bi- und multilateralen Übereinkommen**

Nach Artikel 60 der Richtlinie (EU) 2016/680 bleiben besondere Bestimmungen zum Schutz personenbezogener Daten unberührt, die die Verarbeitung im Verkehr der Mit-



gliedstaaten untereinander sowie den Zugang der zuständigen nationalen Behörden zu den gemäß den Verträgen errichteten Informationssystemen im Anwendungsbereich der Richtlinie (EU) 2016/680 regeln, wenn diese Bestimmungen in Unionsrechtsakten enthalten sind, die am oder vor dem 6. Mai 2016 im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit in Kraft getreten sind.

Internationale Übereinkünfte, die die Übermittlung personenbezogener Daten an Drittstaaten oder an internationale Organisationen mit sich bringen, und die vor dem 6. Mai 2016 geschlossen wurden und mit dem vor diesem Datum geltenden Unionsrecht vereinbar sind, bleiben gemäß Artikel 61 der Richtlinie (EU) 2016/680 in Kraft, bis sie geändert, ersetzt oder gekündigt werden.

## **2. Gesetzesänderungen im Anwendungsbereich der Datenschutz-Grundverordnung**

Die Datenschutz-Grundverordnung, die ab dem 25. Mai 2018 in allen Mitgliedstaaten unmittelbar gilt, stärkt die gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31) bereits bestehenden Betroffenenrechte. So werden beispielsweise durch die Verordnung das Auskunftsrecht der betroffenen Person (Artikel 15), das Recht auf Berichtigung (Artikel 16) und auf Löschung (Artikel 17), das Recht auf Einschränkung der Verarbeitung personenbezogener Daten (Artikel 18) sowie das Widerspruchsrecht gegen die Verarbeitung personenbezogener Daten (Artikel 21) gestärkt. Artikel 13 und 14 der Datenschutz-Grundverordnung regeln Informationspflichten des Verantwortlichen, wenn die personenbezogenen Daten entweder beim Betroffenen oder bei einem Dritten, also nicht bei der betroffenen Person, erhoben werden. Zugleich enthalten die Regelungen zu den Betroffenenrechten zahlreiche ausdrückliche Ausnahmen (vgl. etwa Artikel 13 Absatz 4, Artikel 14 Absatz 5, Artikel 17 Absatz 3) und formulierungsimmanente Beschränkungen, die sich aus der Verwendung offen normativer Begriffe ergeben. Beispiele für solche Begriffe finden sich etwa in Artikel 16 Satz 1 und 2 („Berichtigung“ und „Unter Berücksichtigung der Zwecke der Verarbeitung“) und in Artikel 21 Absatz 1 Satz 2 der Datenschutz-Grundverordnung („zwingende schutzwürdige Gründe für die Verarbeitung [...]“, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen“).

Darüber hinaus gestattet Artikel 23 Absatz 1 der Datenschutz-Grundverordnung den Mitgliedstaaten, durch nationale Rechtsvorschriften die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5 der Datenschutz-Grundverordnung einzuschränken bzw. bereits bestehende Beschränkungen beizubehalten, soweit eine solche Beschränkung eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zur Sicherung eines der in Artikel 23 Absatz 1 der Datenschutz-Grundverordnung aufgelisteten Rechtsgüter (etwa öffentliche und nationale Sicherheit, Landesverteidigung, Strafverfolgung und -vollstreckung, Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses, Schutz der Unabhängigkeit der Justiz und Schutz von Gerichtsverfahren, Durchsetzung zivilrechtlicher Ansprüche) darstellt und zugleich den Wesensgehalt der Grundrechte und Grundfreiheiten achtet. Eine beschränkende Rechtsvorschrift im Sinne des Artikels 23 Absatz 1 der Datenschutz-Grundverordnung muss die in dessen Absatz 2 genannten Vorgaben erfüllen, also spezifische Vorschriften enthalten zumindest in Bezug auf die Zwecke der Datenverarbeitung oder die Verarbeitungskategorien, die Kategorien personenbezogener Daten, den Umfang der vorgenommenen Beschränkungen, die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung und noch einiges mehr.

Beschränkungen der unmittelbaren Geltung der Datenschutz-Grundverordnung im Sinne des Artikels 23 der Datenschutz-Grundverordnung werden für die Gerichte und Justizbehörden auch im Anwendungsbereich der gerichtlichen Verfahrensordnungen, einschließlich der Grundbuchordnung und der Schiffsregisterordnung, und der gerichtsverfassungs-

rechtlichen Regelungen nur in wenigen Fällen erforderlich. Viele Fallkonstellationen können durch die zuvor genannten tatbestandlichen Ausnahmen und die nach der Datenschutz-Grundverordnung bestehenden Auslegungs- und Handlungsspielräume sowie durch die sich aus den Verfahrensordnungen selbst ergebenden oder die sich aus den subsidiär geltenden datenschutzrechtlichen Vorschriften des neuen BDSG (§ 1 Absatz 2 BDSG (2018)) ergebenden Beschränkungen gelöst werden. Dabei kann davon ausgegangen werden, dass sich das gerichtliche Verfahrensrecht im Grundsatz als abschließend erweist; es geht Hand in Hand mit den Ausnahmevorschriften der Datenschutz-Grundverordnung und des sie ergänzenden Bundesdatenschutzgesetzes. Im justiziellen Bereich kommt es danach für am Gerichtsverfahren nicht beteiligte Personen regelmäßig zu einem Ausschluss der Informationspflichten des Gerichts als verantwortlicher Stelle und, damit korrespondierend, zu einer Beschränkung der Betroffenenrechte. Ganz grundsätzlich ist zu beachten, dass keine Pflicht besteht, „querulatorische“ Anträge zu bearbeiten. Dies ergibt sich aus Artikel 12 Absatz 5 Satz 2 Buchstabe b der Datenschutz-Grundverordnung. Im Übrigen sei hier beispielhaft auf Folgendes hingewiesen:

- Soweit in einem gerichtlichen Verfahren personenbezogene Daten bei einer betroffenen Person erhoben werden, dürfte diese Person typischerweise den Zweck der Datenverarbeitung kennen, so dass insoweit die diesbezügliche Informationspflicht nach Artikel 13 Absatz 4 der Datenschutz-Grundverordnung entfällt. Zudem entfällt die Informationspflicht in den Fällen des § 29 Absatz 2 und § 32 Absatz 1 BDSG (2018). Nach der zuletzt genannten Vorschrift besteht die Informationspflicht unter anderem dann nicht, wenn die Erteilung der Information die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen, was in gerichtlichen Verfahren regelmäßig der Fall ist. Soweit die Informationspflicht besteht und die betroffene Person über die in Artikel 13 Absatz 1 und Absatz 2 der Datenschutz-Grundverordnung genannten Informationen noch nicht verfügt, können diese in allgemeiner Form, beispielsweise auf der Homepage des Gerichts oder als Merkblatt, erteilt werden.
- Soweit in einem gerichtlichen Verfahren personenbezogene Daten nicht bei der betroffenen Person erhoben werden, dürfte regelmäßig eine der in Artikel 14 Absatz 5 der Datenschutz-Grundverordnung genannten Ausnahmen vorliegen, so dass die Informationspflicht entfällt. Nach Absatz 5 Buchstabe b entfällt die Informationspflicht, wenn sich die Erteilung der Informationen als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde. Im Rahmen der bei der Prüfung der Unverhältnismäßigkeit durchzuführenden Abwägung ist insbesondere das Interesse der betroffenen Person an der Mitteilung zu berücksichtigen; dieses dürfte beispielsweise bei einem von einer Partei benannten Zeugen, auf den es im Rahmen des Rechtsstreits nicht ankommt, eher gering sein. In diesen Fällen muss der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person ergreifen, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit. Nach Absatz 5 Buchstabe c entfällt die Informationspflicht darüber hinaus, wenn die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist. Die Erlangung oder Offenlegung von personenbezogenen Daten (etwa durch Beiziehung von Verwaltungsakten oder Verwaltungsvorgängen, § 86 VwGO, § 76 FGO, § 103 SGG, § 56 ArbGG, § 273 ZPO) ist in der jeweiligen Verfahrensordnung, die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht (etwa mit einem auf die Beteiligten beschränkten Akteneinsichtsrecht, der Pflicht zur Wahrung von Dienst- und Beratungsgeheimnissen und in der Sozialgerichtsbarkeit mit dem so genannten verlängerten Sozialdatenschutz, § 78 SGB X), regelmäßig ausdrücklich geregelt (Artikel 14 Absatz 5 Buchstabe c). Soweit die jeweilige Verfahrensordnung ausnahmsweise kei-

ne ausdrückliche Regelung zur Erlangung oder Offenlegung der Daten und keine geeigneten Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht und soweit auch keine andere der in Artikel 14 Absatz 5 der Datenschutz-Grundverordnung genannten Ausnahmen einschlägig ist, kommen subsidiär Ausnahmen nach § 29 Absatz 1 Satz 1 und § 33 Absatz 1 BDSG, jeweils in der ab dem 25. Mai 2018 geltenden Fassung, sowie ggf. nach den Landesdatenschutzgesetzen in Betracht. Ist keine der Ausnahmen gegeben, eröffnet Artikel 14 Absatz 3 der Datenschutz-Grundverordnung in zeitlicher Hinsicht ausreichend Spielraum bei der Erfüllung der Informationspflicht.

- Das Auskunftsrecht gemäß Artikel 15 der Datenschutz-Grundverordnung besteht, soweit nicht die Ausnahmen aus § 27 Absatz 2, § 28 Absatz 2, § 29 Absatz 1 Satz 2 und § 34 Absatz 1 BDSG (2018) eingreifen. Nach der zuletzt genannten Vorschrift besteht ein Auskunftsrecht dann nicht, wenn auch die Informationspflicht aus Artikel 14 der Datenschutz-Grundverordnung gemäß § 33 Absatz 1 Nummer 1, 2 Buchstabe b oder Absatz 3 BDSG (2018) ausgeschlossen ist oder wenn personenbezogene Daten regelmäßig nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen (vgl. § 34 Absatz 1 Nummer 1 und Nummer 2 Buchstabe a BDSG (2018)), und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.
- Soweit in einem gerichtlichen Verfahren die Berichtigung gerichtlicher Verfügungen, Beschlüsse, Protokolle, Urteile, Registereintragungen oder sonstiger gerichtlicher Dokumente geltend gemacht wird, enthalten die Verfahrensordnungen hierzu besondere Regelungen. Die Anwendung des Artikels 16 der Datenschutz-Grundverordnung führt nicht dazu, dass diese Regelungen unterlaufen werden können. Denn es handelt sich bei der „Berichtigung“ im Sinne des Artikels 16 der Datenschutz-Grundverordnung um einen offen normativen Begriff, bei dessen Auslegung im Einzelfall die Zwecke der Verarbeitung zu berücksichtigen sind. Dies ergibt sich auch aus Erwägungsgrund 4 der Datenschutz-Grundverordnung, wonach das Recht auf Schutz der personenbezogenen Daten kein uneingeschränktes Recht ist und im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Rechte, darunter auch das Recht auf einen wirksamen Rechtsbehelf und ein faires Verfahren, abgewogen werden muss. Dies entspricht ebenso der Rechtsprechung des Europäischen Gerichtshofs zu den bisherigen Datenschutzvorschriften der Europäischen Union, wonach die Richtigkeit und Vollständigkeit personenbezogener Daten im Hinblick auf den Zweck zu beurteilen sind, für den die Daten erhoben wurden (Urteil vom 20. Dezember 2017, Rs. C-434/16 – "Nowak"). Folglich begründet beispielsweise nicht jedes objektiv unrichtige personenbezogene Datum einen Berichtigungsanspruch gemäß Artikel 16 der Datenschutz-Grundverordnung. Vielmehr ist zu prüfen, ob das objektiv unrichtige Datum (etwa ein bewusst falsch angegebenes Geburtsdatum eines Zeugen in einem Protokoll) auch unter Berücksichtigung des Zwecks der Datenverarbeitung als „unrichtig“ angesehen werden kann (was im Fall eines Protokolls zu verneinen wäre, da sein Zweck nicht die Wiedergabe objektiv richtiger personenbezogener Daten ist, sondern das Festhalten des Verhandlungsverlaufs). Ist das nicht der Fall, besteht kein Berichtigungsanspruch. Aus den zuvor genannten Gründen kann über die Berichtigungsregelungen des Datenschutzrechts auch keine Änderung der Vorschlagslisten für die Schöffenwahl erreicht werden, insbesondere keine Streichung von der Schöffenliste gemäß § 52 GVG. Denn auch wenn ein Schöffe materiell einen Anspruch auf Streichung haben mag, enthält § 52 GVG die dafür besonderen Regelungen, die durch die Anwendung des Artikels 16 der Datenschutz-Grundverordnung nicht unterlaufen werden können.
- Die Voraussetzungen für die Geltendmachung eines Rechts auf Löschung personenbezogener Daten nach Artikel 17 Absatz 1 der Datenschutz-Grundverordnung dürften im Rahmen gerichtlicher Erkenntnisverfahren regelmäßig nicht vorliegen, da die Da-

tenverarbeitung in Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe und in Ausübung öffentlicher Gewalt sowie im Zusammenhang mit der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erfolgt (Artikel 17 Absatz 3 Buchstabe b und e der Datenschutz-Grundverordnung).

- Die Möglichkeit der Verarbeitung von Daten ist auch für den Fall, dass die betroffene Person die Einschränkung der Verarbeitung verlangt, regelmäßig gewährleistet. Denn auch in diesem Fall ist eine Weiterverarbeitung von personenbezogenen Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen sowie aus Gründen eines wichtigen öffentlichen Interesses eines Mitgliedstaats zulässig (Artikel 18 Absatz 2 der Datenschutz-Grundverordnung).
- Ausnahmen bestehen auch für das Recht auf Datenübertragbarkeit nach Artikel 20 der Datenschutz-Grundverordnung. Denn auch dieses findet insoweit keine Anwendung, als die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (Artikel 20 Absatz 3 Satz 2 der Datenschutz-Grundverordnung).
- Nach Artikel 21 der Datenschutz-Grundverordnung kann der betroffenen Person ein Recht auf Widerspruch gegen die Verarbeitung sie betreffender Daten zustehen. Das setzt zum einen Gründe voraus, die sich aus der besonderen Situation der betroffenen Person ergeben. Zum anderen muss die Verarbeitung personenbezogener Daten auf der Grundlage von Artikel 6 Absatz 1 Buchstabe e oder f der Datenschutz-Grundverordnung erfolgen. Aus Artikel 21 Absatz 1 Satz 2 der Datenschutz-Grundverordnung ergibt sich, dass eine Datenverarbeitung trotz eingelegten Widerspruchs zulässig ist, wenn der Verantwortliche zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient, was in gerichtlichen Verfahren regelmäßig der Fall ist. Zudem ist § 36 BDSG (2018) einschlägig, wonach das Widerspruchsrecht nicht besteht, soweit an der Datenverarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder soweit eine Rechtsvorschrift zur Verarbeitung verpflichtet, was in gerichtlichen Verfahren regelmäßig der Fall ist.

Anpassungen – überwiegend redaktioneller Art – im Hinblick auf die Datenschutz-Grundverordnung und das BDSG (2018) sind erforderlich

- im Bundesverfassungsgerichtsgesetz (BVerfGG) (Artikel 3),
- in der Vorsorgeregister-Verordnung (VRegV) (Artikel 4),
- in der Testamentsregister-Verordnung (ZTRV) (Artikel 5),
- in der Rechtsanwaltsverzeichnis- und -postfachverordnung (RAVPV) (Artikel 6),
- Rechtsdienstleistungsverordnung (RDV) (Artikel 7)
- in der Schuldnerverzeichnisführungsverordnung (Artikel 9),
- in der Schuldnerverzeichnisabdruckverordnung (Artikel 10),
- in der Grundbuchverordnung (Artikel 14)
- in der Verordnung zur Durchführung der Schiffsregisterordnung (Artikel 16),

- in der Handelsregisterverordnung (Artikel 17),
- im Auslandsunterhaltsgesetz (AUG) (Artikel 21) und
- in der Luftfahrzeugpfandrechtsregisterverordnung (Artikel 23).

Von der Möglichkeit zur Beschränkung der aus der Datenschutz-Grundverordnung folgenden Betroffenenrechte nach Artikel 23 dieser Verordnung wird Gebrauch gemacht

- bei den Mitteilungen der Gerichte nach dem Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG) (Artikel 2),
- bei der Verwaltung der Vermögensverzeichnisse und des Schuldnerverzeichnisses nach der ZPO (Artikel 8),
- in der Grundbuchordnung (GBO) (Artikel 13),
- in der Schiffsregisterordnung (SchRegO) (Artikel 15) sowie
- bei der Verwaltung des Vereinsregisters und des Güterrechtsregisters im Bürgerlichen Gesetzbuch (BGB) (Artikel 22).

Von den Öffnungsklauseln in Artikel 6 Absatz 2 und Absatz 3 Satz 1 Buchstabe b in Verbindung mit Artikel 6 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung sowie von der Möglichkeit zur Beschränkung der aus der Datenschutz-Grundverordnung folgenden Betroffenenrechte nach Artikel 23 dieser Verordnung wird bei der Änderung der Datenschutzregelungen

- des Strafvollzugsgesetzes (Artikel 12)

Gebrauch gemacht. Daneben sind auch hier Anpassungen – überwiegend redaktioneller Art – im Hinblick auf die Datenschutz-Grundverordnung und das BDSG (2018) erforderlich.

Im Einzelnen:

#### **a) EGGVG**

Der zweite Abschnitt des EGGVG regelt die verfahrensübergreifenden Mitteilungen der Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften von Amts wegen. § 21 EGGVG enthält in diesem Zusammenhang ein Recht der betroffenen Person auf Auskunft über die übermittelten Daten und deren Empfänger sowie eine Pflicht zu deren Unterrichtung von Amts wegen. Die Datenschutz-Grundverordnung enthält insoweit jedoch eigene Regelungen, so dass § 21 EGGVG im Anwendungsbereich der Datenschutz-Grundverordnung nicht mehr gelten soll. Dabei muss jedoch auch im Anwendungsbereich der Datenschutz-Grundverordnung sichergestellt sein, dass der Zweck der verfahrensübergreifenden Mitteilungen von Amts wegen nicht gefährdet wird. Ebenso muss gewährleistet sein, dass höherrangige Interessen der öffentlichen Sicherheit und Ordnung, der Geheimhaltung oder Rechte Dritter sowie die Gesundheit der betroffenen Person nicht durch die Wahrnehmung der Betroffenenrechte nach der Datenschutz-Grundverordnung gefährdet werden. Aus diesem Grund müssen die inhaltlichen Beschränkungen des § 21 Absatz 3 bis 5 EGGVG auf die Auskunftsrechte und Informationspflichten nach der Datenschutz-Grundverordnung erstreckt und das Recht auf Einschränkung der Verarbeitung nach Artikel 18 der Datenschutz-Grundverordnung sowie das Widerspruchsrecht nach Artikel 21 der Datenschutz-Grundverordnung eingeschränkt werden.

Bei verfahrensübergreifenden Mitteilungen im Sinne des zweiten Abschnitts des EGGVG rechtfertigt der auf die bloße zweckändernde Datenübermittlung an eine öffentliche Stelle des Bundes oder Landes beschränkte Charakter der Verarbeitung eine Einschränkung der Rechte und Pflichten aus der Datenschutz-Grundverordnung. Darüber hinausgehende Betroffenenrechte können gegebenenfalls im Rahmen des Ausgangsverfahrens und des Verfahrens bei dem Empfänger ausgeübt werden, weil die Konsequenzen aus der eigentlichen Mitteilung sich ausschließlich nach deren jeweiligen Verfahrensregelungen richten.

Für den Bereich der Richtlinie (EU) 2016/680 besteht insoweit kein Regelungsbedarf; hier stellen die §§ 12 ff. EGGVG und insbesondere § 21 EGGVG eine bereichsspezifische Sonderregelung des Datenschutzes dar, die nach § 1 Absatz 2 Satz 1 BDSG (2018) den Vorschriften des BDSG (2018) als *lex specialis* vorgehen. Sie genügen als Sonderbestimmungen für die Übermittlung personenbezogener Daten mit Zweckänderung den Anforderungen des Artikels 4 Absatz 2 der Richtlinie (EU) 2016/680. Sie konkretisieren für den Anwendungsbereich der Richtlinie (EU) 2016/680 bzw. des § 45 BDSG (2018) die Rechtsgrundlagen für die Übermittlung personenbezogener Daten und, im Fall des § 21 EGGVG, die Anforderungen der Betroffenenrechte im Sinne der Artikel 12 bis 18 der Richtlinie (EU) 2016/680. Als solche gehen sie den allgemeinen datenschutzrechtlichen Regelungen der Betroffenenrechte nach den §§ 55 bis 59 BDSG (2018) vor.

#### **b) ZPO**

Es werden nähere Regelungen hinsichtlich bestimmter Pflichten und Rechte nach der Datenschutz-Grundverordnung in Bezug auf die von den zentralen Vollstreckungsgerichten verwalteten Vermögensverzeichnisse sowie das Schuldnerverzeichnis in die ZPO eingefügt. Dadurch soll die Funktionalität des Schuldnerverzeichnisses im Hinblick auf seine wesentliche Warn- und Schutzfunktion für den Rechtsverkehr sowie die Verfügbarkeit der Vermögensverzeichnisse gewahrt werden. Außerhalb dieser Regelungen sind in der ZPO aus den zuvor genannten Gründen keine Anpassungen erforderlich.

Soweit keine bereichsspezifischen Vorschriften bestehen, kommt dem BDSG (2018), wie sich aus § 1 Absatz 2 Satz 2 BDSG (2018) ergibt, im Hinblick auf das Datenschutzrecht der Charakter eines Auffanggesetzes zu (siehe oben I.).

#### **c) BGB**

Für das Vereins- und Güterrechtsregister sind einzelne Betroffenenrechte zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses gemäß Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung einzuschränken.

Im Einzelnen sind dies das Auskunftsrecht nach Artikel 15, das Recht auf Berichtigung nach Artikel 16, das Recht auf Löschung nach Artikel 18 sowie das Widerspruchsrecht nach Artikel 21. Die Einschränkungen sind erforderlich, um ein funktionsfähiges und verlässliches Vereinsregister und Güterrechtsregister mit Publizitätswirkung zu erhalten. Die Beschränkungen entsprechen dabei denen, die bereits für das Handels-, Genossenschafts- und Partnerschaftsregister getroffen worden sind durch Artikel 7 des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017 (BGBl. I S. 2541).

#### **d) GBO und SchRegO**

Für die Grundbuchordnung und die Schiffsregisterordnung wird von der Möglichkeit zur Beschränkung der aus der Datenschutz-Grundverordnung folgenden Betroffenenrechte Gebrauch gemacht, namentlich im Hinblick auf das Auskunftsrecht nach Artikel 15, auf das Recht auf Berichtigung nach Artikel 16 und auf das Widerspruchsrecht nach Artikel 21 der Datenschutz-Grundverordnung. Die Beschränkung erfolgt nach Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung in Verbindung mit Erwägungsgrund 73

dieser Verordnung zum Schutz der Funktionalität und Verlässlichkeit des Grundbuchs als wichtiges Ziel des allgemeinen öffentlichen Interesses. Die Beschränkungen entsprechen dabei denen, die bereits für das Handels-, Genossenschafts- und Partnerschaftsregister getroffen worden sind durch Artikel 7 des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017 (BGBl. I S. 2541).

### **e) Strafvollzugsgesetz**

Für die Datenschutzregelungen im Strafvollzugsgesetz (StVollzG), deren Anwendungsbereich nach Inkrafttreten landesrechtlicher Regelungen zum Strafvollzug in allen Ländern grundsätzlich auf den Vollzug der Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft nach § 171 StVollzG beschränkt ist, wird von Artikel 6 Absatz 2 und Absatz 3 Satz 1 Buchstabe b in Verbindung mit Artikel 6 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung Gebrauch gemacht. Diese Vorschriften enthalten für den nationalen Gesetzgeber Öffnungsklauseln für spezifischere Bestimmungen für die Datenverarbeitung, wenn die Verarbeitung in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Bei dem Vollzug von Haft nach § 171 StVollzG ist diese Voraussetzung erfüllt. Daher kann das nationale Recht, im vorliegenden Fall ausgerichtet an den spezifischen Bedürfnissen des Vollzugs der Haft nach § 171 StVollzG, Anpassungen der Vorschriften der Datenschutz-Grundverordnung unter anderem dazu vorsehen, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und –verfahren angewandt werden dürfen. Vor diesem Hintergrund sollen die bisherigen Datenschutzvorschriften des StVollzG weitgehend beibehalten und an den neuen Rechtsrahmen der Datenschutz-Grundverordnung und des BDSG (2018) angepasst werden. Daneben wird, ebenfalls ausgerichtet an den spezifischen Bedürfnissen des Vollzugs der Haft nach § 171 StVollzG, von der Möglichkeit des Artikels 23 der Datenschutz-Grundverordnung Gebrauch gemacht, bestimmte Rechte und Pflichten einzuschränken, die aus der Verordnung mit Bezug auf betroffene Personen gelten.

### **f) Subsidiäre Geltung des BDSG (2018)**

Soweit in spezifischen Rechtsvorschriften des Bundes oder in landesrechtlichen Regelungen keine besonderen Beschränkungen der Pflichten und Rechte nach den Artikeln 12 bis 22, Artikel 34 und Artikel 5 der Datenschutz-Grundverordnung enthalten sind, gelten im Bereich der justiziellen Tätigkeit der Gerichte und Justizbehörden subsidiär die im BDSG (2018) enthaltenen allgemeinen Beschränkungen (§ 1 Absatz 1 Satz 1 in Verbindung insbesondere mit den §§ 32 ff. BDSG (2018)).

## **3. Barrierefreiheit**

Soweit die in dem Entwurf enthaltenen Pflichten der Strafverfolgungsbehörden und der Gerichte Informationspflichten gegenüber betroffenen Personen enthalten, werden die Anforderungen der Barrierefreiheit für Menschen mit Behinderungen berücksichtigt.

Für die Behörden des Bundes und der Länder, soweit sie Bundesrecht ausführen, wurde die barrierefreie Gestaltung in der Kommunikationshilfenverordnung, der Verordnung über barrierefreie Dokumente in der Bundesverwaltung und der Barrierefreien Informationstechnik-Verordnung (BITV) konkretisiert.

Für die Gerichte ergibt sich das Recht auf einen barrierefreien Zugang für blinde und sehbehinderte Menschen aus § 191a GVG in Verbindung mit der Verordnung zur barrierefreien Zugänglichmachung von Dokumenten für blinde und sehbehinderte Personen im gerichtlichen Verfahren (Zugänglichmachungsverordnung - ZMV) vom 26. Februar 2007

(BGBl. I S. 215), die durch Artikel 20 des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3786) geändert worden ist.

### **III. Alternativen**

Keine.

### **IV. Gesetzgebungskompetenz**

Für die Änderungen der StPO, des EGGVG, der VRegV, der ZPO, der ZTRV, der RAVPV, der RDV, der Schuldnerverzeichnisverordnung, der Schuldnerverzeichnisabdruckverordnung, der ZStVBetrV, des StVollzG, des AUG, der GBO, der SchRegO und des BGB folgt die Gesetzgebungskompetenz des Bundes aus dem Kompetenztitel des Artikels 74 Absatz 1 Nummer 1 des Grundgesetzes (GG) (Bürgerliches Recht, Gerichtsverfassung, gerichtliches Verfahren, Rechtsanwaltschaft, Notariat und Rechtsberatung).

Die Gesetzgebungskompetenz für die Änderung des BVerfGG ergibt sich aus Artikel 94 Absatz 2 GG.

Die internationale Zusammenarbeit in strafrechtlichen Angelegenheiten ist Teil der Pflege der auswärtigen Beziehungen nach Artikel 32 Absatz 1 GG. Die Änderungen des IRG und der Eurojust-Anlaufstellen-Verordnung fallen deshalb in den Bereich der ausschließlichen Gesetzgebungskompetenz des Bundes nach Artikel 73 Absatz 1 Nummer 1 GG.

### **V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen**

Der Entwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland abgeschlossen hat, vereinbar. Der Entwurf dient der Umsetzung der Richtlinie (EU) 2016/680, der Anpassung bereichsspezifischen nationalen Rechts an die Datenschutz-Grundverordnung sowie der Durchführung dieser Verordnung.

### **VI. Gesetzesfolgen**

#### **1. Rechts- und Verwaltungsvereinfachung**

Die vorgeschlagenen Änderungen konkretisieren den bereichsspezifischen Datenschutz und erleichtern so den jeweils zuständigen Stellen den angemessenen Umgang mit personenbezogenen Daten.

#### **2. Nachhaltigkeitsaspekte**

Der Entwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie. Denn er ist geeignet, den sozialen Zusammenhalt im Sinne der Managementregel Nummer 2 in Verbindung mit Nummer 10 gem. Ziffer II. 2. des Nachhaltigkeitsmanagementsystems der Deutschen Nachhaltigkeitsstrategie zu stärken, indem auf nationaler Ebene und im Einklang mit den Vorgaben der Europäischen Union der Bereich der innerdeutschen und grenzüberschreitenden Kriminalitätsbekämpfung um klare datenschützende Regelungen ergänzt wird. Dies schafft einheitliche Maßstäbe und mehr Transparenz nicht nur für die beteiligten Behörden, sondern für die von der Verarbeitung personenbezogener Daten betroffenen Bürgerinnen und Bürger. Insgesamt wird der Datenschutz und damit die Rechtsposition betroffener Personen in der Europäischen Union gestärkt.



Die Verbesserung der Zusammenarbeit im Bereich der Strafverfolgung und der Schutz von Grundrechten sind wichtige Bestandteile der Entwicklung eines europäischen Raums der Freiheit, der Sicherheit und des Rechts, der mit dem sogenannten Stockholmer Programm des Europäischen Rates bestätigt und fortgeschrieben wurde. Insoweit dient der Entwurf auch dazu, internationale Verantwortung im Sinne der Managementregel Nummer 2 gemäß Ziffer II. 2. des Nachhaltigkeitsmanagementsystems der Deutschen Nachhaltigkeitsstrategie wahrzunehmen.

### **3. Haushaltsausgaben ohne Erfüllungsaufwand**

Keine

### **4. Erfüllungsaufwand**

#### **a) Bürgerinnen und Bürger**

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

#### **b) Wirtschaft**

Für die Wirtschaft entsteht kein Erfüllungsaufwand. Es werden keine Informationspflichten für die Wirtschaft eingeführt, geändert oder abgeschafft.

Insbesondere für kleinere und mittlere Unternehmen, entstehen keine Kosten. Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

#### **c) Verwaltung**

aa) Im Rahmen der bereichsspezifischen Umsetzung der Richtlinie (EU) 2016/680:

##### **– Änderungen in der StPO**

Für die Justizverwaltungen der Länder kann ein Mehraufwand anfallen, der im Wesentlichen unmittelbar durch die Richtlinie (EU) 2016/680 selbst ausgelöst wird. Dieser Mehraufwand betrifft ganz überwiegend die Strafgerichte und Staatsanwaltschaften, sowie sonstige Strafverfolgungsbehörden des Bundes und der Länder (Polizeibehörden des Bundes und der Länder, Zoll, Finanzbehörden).

Im Zentrum stehen insofern zwei Änderungen, nämlich zum einen der Verzicht auf die Ausschlussklausel und die zeitliche Einschränkung des bisherigen § 491 BDSG in Bezug auf datenschutzrechtliche Auskunftsrechte und zum anderen die Ausweitung der Protokollierungspflichten im Rahmen automatisierter Übermittlungsverfahren in § 488 bzw. § 493 StPO-E. Da hierdurch Aufgaben der Justizverwaltungen betroffen sind, ist dieser Mehraufwand als Erfüllungsaufwand anzusetzen.

Für die Änderungen in Bezug auf Auskunftsrechte im Rahmen des § 491 StPO-E ist davon auszugehen, dass die Kosten dafür nur gering ausfallen werden, da die Erweiterung nur die datenschutzrechtlichen Auskünfte betrifft. Denn neben dem Auskunftsrecht hinsichtlich personenbezogener Daten haben die anderen in der StPO geregelten verfahrensrechtlichen Auskunfts- bzw. Akteneinsichtsrechte eine wesentlich größere Bedeutung. Sie werden von den betroffenen Personen auch zukünftig vorrangig geltend gemacht werden, da sie regelmäßig weiter gehen und umfassendere Informationen bieten als die datenschutzrechtlichen Ansprüche.

Darüber hinaus ist zu beachten, dass die datenschutzrechtliche Auskunft bereits auf der Grundlage des geltenden Rechts, d. h. gemäß § 19 Absatz 4 BDSG zu erteilen ist, sobald die Sperrmöglichkeiten des § 491 Absatz 1 Satz 2 bis 6 StPO nicht (mehr) bestehen (Schmitt in Meyer-Goßner/Schmitt StPO 60. Aufl. § 491 Rdnr. 3). Nach Wegfall dieser Regelung sind daher in der Summe nicht mehr (stattgebende) Bescheide zu erteilen, sondern sie werden nur früher zu erlassen sein. Im Übrigen ist der Antragsteller schon nach geltendem Recht (§ 491 Absatz 1 Satz 6 StPO) in jedem Fall zu bescheiden und auf die Regelungen des § 491 Absatz 1 Satz 2 bis 5 StPO hinzuweisen. Eine Zunahme der Anfragen wird jedoch auch dessen ungeachtet, und zwar im Wesentlichen durch die Neuregelung des Datenschutzrechts und die so auf diesen Bereich gerichtete erhöhte Aufmerksamkeit der Bevölkerung zu erwarten sein. § 491 StPO-E wird nach Wegfall der zeitlichen Beschränkung des § 491 Absatz 1 Satz 2 bis 6 StPO erkennbar bürgerfreundlicher gestaltet sein als bisher. Die dadurch gesteigerten Erwartungen interessierter Kreise werden zu zusätzlichen Anfragen führen, entziehen sich allerdings einer zuverlässigen Prognose.

Die Gesamtzahl der Personen, gegen die von Staatsanwaltschaften der Länder in den Jahren 2013 bis 2015 ermittelt wurde, betrug pro Jahr durchschnittlich 5 490 282,33 (5 723 847 im Jahr 2015, 5 447 255 im Jahr 2014 und 5 299 745 im Jahr 2013). Setzt man für die Prüfung des Auskunftsanspruchs zwanzig Minuten an, so führte dies bei 5 490 282,33 Verfahren zu einem zeitlichen Aufwand von 1 830 094 Stunden (109 805 647 Minuten). Da bereits bislang Auskunftsansprüche aus datenschutzrechtlichen Gründen bestanden und diese Ansprüche nur erweitert werden, wird ein Mehraufwand nur für Fälle anzunehmen sein, in denen von dem Auskunftsrecht auf Grund der oben beschriebenen erhöhten Aufmerksamkeit neu Gebrauch gemacht werden wird. Geht man folglich davon aus, dass diese zusätzlichen Fälle, ca. 1 Prozent aller Verfahren betreffen könnten, so ist von einer Stundenzahl in Höhe von 18 301 Stunden auszugehen. Wenn man von den veranschlagten zwanzig Minuten jeweils fünfzehn Minuten mit einem Stundensatz eines Beamten des mittleren oder gehobenen Dienstes in Höhe von durchschnittlich 36,10 Euro (Mittel aus einem Stundensatz von 40,80 Euro für einen Beamten des gehobenen Dienstes und 31,40 Euro für einen Beamten des mittleren Dienstes, jeweils auf Länderebene, nach der Lohnkostentabelle Verwaltung, Stand 15. November 2017) zugrunde legt, und zusätzlich fünf Minuten für einen Beamten des höheren Dienstes anrechnet, kommt man auf jährlich maximal 772 483 Euro (jeweils fünfzehn Minuten zu einem Stundenlohn von 36,10 Euro und fünf Minuten zu einem Stundenlohn von 60,50 Euro in 1 Prozent der insgesamt 5 490 282,33 Fälle). Dieser Mehraufwand bezieht sich dann auf alle Staatsanwaltschaften aller Bundesländer insgesamt.

Der Generalbundesanwalt teilte mit, im Jahr 2014 insgesamt 135, im Jahr 2015 insgesamt 182 und im Jahr 2016 insgesamt 270 Ermittlungsverfahren neu eingeleitet oder übernommen zu haben. Die durchschnittliche Gesamtzahl wäre auf dieser Basis mit 196 Fällen zu beziffern. Legt man für das Jahr 2017 unter Berücksichtigung des sich bereits abzeichnenden signifikanten Anstiegs eine gegenüber 2016 verdoppelte Anzahl an Ermittlungsverfahren (540) zu Grunde, so kommt man auf eine durchschnittliche Fallzahl von insgesamt 282. Geht man auf Basis der obenstehenden Ausführungen davon aus, dass in 1 Prozent dieser Fälle mit zusätzlichen Auskunftsanträgen zu rechnen ist, so kommt man auf insgesamt drei Fälle. Legt man für diese wenigen Fälle eine erhöhte Bearbeitungszeit von 30 Minuten durch einen Beamten des mittleren oder gehobenen Dienstes mit einem Stundensatz von 37,55 Euro (Mittel aus einem Stundensatz von 43,40 Euro für einen Beamten des gehobenen Dienstes und 31,70 Euro für einen Beamten des mittleren Dienstes, jeweils auf Bundesebene, nach der Lohnkostentabelle Verwaltung, Stand 15. November 2017) und fünfzehn Minuten eines Beamten des höheren Dienstes mit einem Stundensatz von 65,40 Euro zu Grunde, ergibt sich ein Mehraufwand in Höhe von insgesamt 105,39 Euro.

Für die Strafsenate des Bundesgerichtshofes und den Bundesgerichtshof als Ermittlungsrichter ist für den Zeitraum 2014 bis 2016 von einer durchschnittlichen Anzahl erledigter Verfahren im Umfang von 5 212 Verfahren pro Jahr (4541 Verfahren im Jahr 2014, 5290 Verfahren im Jahr 2015 und 5804 Verfahren im Jahr 2016) auszugehen. Hierbei ist allerdings zu berücksichtigen, dass diese Verfahren zuvor bei den Staatsanwaltschaften und Gerichten der Länder bzw. dem Generalbundesanwalt anhängig gewesen sein mussten und sich das Auskunftsbegehren in aller Regel gegen diese zuvor befassten Stellen richten wird. Von zusätzlichem Erfüllungsaufwand in Bezug auf den Bundesgerichtshof ist daher nicht auszugehen.

Für die zusätzlichen Auskunftsrechte in Bezug auf das Zentrale Staatsanwaltschaftliche Verfahrensregister (ZStV) (resultierend aus der mit § 491 StPO-E korrespondierenden Anpassung des § 495 StPO und der ZStVBetrV) ist für das Bundesamt der Justiz ebenfalls ein geringfügiger Aufwand zu erwarten.

Nach Angaben des Bundesamtes der Justiz werden im ZStV jährlich durchschnittlich ungefähr 6 Millionen Mitteilungen gespeichert. Es ist davon auszugehen, dass Auskunftersuchen an die jeweiligen Ermittlungsbehörden für die betroffenen Personen zunächst Priorität haben und Auskünfte in Bezug auf das Zentrale Staatsanwaltschaftliche Verfahrensregister eher nachrangig und eher zu einem späteren Zeitpunkt gestellt werden. Für diese Anfragen dürften die bisherigen Beschränkungen in § 491 StPO auch bisher kaum Relevanz gehabt haben. Für Auskünfte hinsichtlich laufender Verfahren – die den größten Teil der im ZStV gespeicherten Daten betreffen –, werden die jeweiligen zuständigen Staatsanwaltschaften über den Auskunftsanspruch entscheiden müssen. Da darüber hinaus die Zahl von Auskunftsansprüchen in diesem Sinne bislang sehr gering ist, ist nur ein äußerst geringer Mehraufwand zu erwarten, der nicht bezifferbar ist..

Für die Ausweitung der Protokollierungspflichten im Rahmen automatisierter Abrufverfahren nach § 488 StPO-E ist mit einem einmaligen Umstellungsaufwand zu rechnen. Dieser ist im Einzelnen jedoch nicht bezifferbar. Anfallen wird im Übrigen auch ein einmaliger Einarbeitungsaufwand, der gegebenenfalls durch Schulungsangebote von Seiten des Bundes und der Länder verringert werden kann. Insgesamt ist somit zu erwarten, dass ein Mehraufwand mit den bestehenden personellen und sachlichen Ressourcen aufgefangen werden kann. Die Einrichtung neuer Organisationsstrukturen in den Ländern ist daher nicht erforderlich.

Für die erweiterten Protokollierungspflichten im Rahmen des ZStV nach § 493 StPO-E ist für das Bundesamt der Justiz ein einmaliger Umstellungsaufwand in Höhe von 10 000 Euro zu erwarten.

– Änderungen im IRG

Für die Länder kann ein Mehraufwand an Kosten anfallen. Für den Bereich der grenzüberschreitenden strafrechtlichen Zusammenarbeit innerhalb der Europäischen Union gilt der unmittelbare Geschäftsverkehr zwischen den beteiligten justiziellen Stellen der Mitgliedstaaten. Die zuständigen Justizbehörden und Gerichte sind somit ein Hauptadressat der neuen datenschutzrechtlichen Verpflichtungen. Der Mehraufwand wird unmittelbar durch die Richtlinie (EU) 2016/680 selbst ausgelöst, die im Wesentlichen 1:1 im IRG umgesetzt werden soll.

Die Regelungsvorschläge gehen nur an zwei Stellen über eine 1:1-Umsetzung der Richtlinie (EU) 2016/680 hinaus:

Erstens soll auch die bloße Papierakte in den Anwendungsbereich der §§ 77c ff. IRG-E einbezogen werden, während es Artikel 2 Absatz 2 der Richtlinie (EU) 2016/680 zuließe, den Anwendungsbereich auf personenbezogene Daten zu beschränken, die

(teilweise) automatisiert verarbeitet werden oder die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Damit wird hier ein anderer Regelungsansatz gewählt als noch bei der Umsetzung des Rb Datenschutz, wo die Papierakte nicht einbezogen werden sollte, siehe Bundestagsdrucksache 18/6285, § 97a IRG-E mit zugehöriger Begründung. Grund dafür ist, dass eine umfassende Geltung der datenschützenden Vorschriften inzwischen sachgerecht erscheint, zumal in den nächsten Jahren die elektronische Akte in Strafsachen eingeführt wird und sämtliche in elektronischen Akten enthaltenen personenbezogenen Daten der Richtlinie (EU) 2016/680 unterfallen. Damit fallen insbesondere die Prüf-, Informations- und Protokollierungspflichten des § 77e IRG-E auch für personenbezogene Daten an, die in Papierakten vorgehalten werden.

Wie hoch die zusätzlichen Kosten sein werden, die den Ländern bis zur Einführung der elektronischen Akte durch den erweiterten Anwendungsbereich anfallen, lässt sich nicht abschätzen, weil sich insbesondere die Fallzahlen nicht vorhersagen lassen. Umfassende amtliche Rechtshilfestatistiken existieren weder auf Bundes- noch auf Länderebene. Damit lässt sich bereits die Gesamtzahl aller Rechtshilfeporgänge, die Mitgliedstaaten der Europäischen Union betreffen, nicht belastbar ermitteln. Die Einführung entsprechender Statistiken ist von der umzusetzenden Richtlinie (EU) 2016/680 nicht vorgesehen. Es erscheint auch nicht sachgerecht, die Umsetzung der Richtlinie (EU) 2016/680 zum Anlass zu nehmen, amtliche Statistiken einzuführen. Die Aussagekraft, die diese Statistiken mit Blick auf den Datenschutz hätten, stünde in keinem Verhältnis zu dem Aufwand, der auf der Ebene von Bund und Ländern anfiel. Eine Hochrechnung der Fallzahlen anhand anderer existierender Statistiken, insbesondere der Statistik zu dem Rahmenbeschluss 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten, ist ebenfalls nicht möglich. Dieses Vorgehen setzte unter anderem einen allgemeinen Vergleichsmaßstab zwischen dem Fallaufkommen bei Auslieferungen einerseits und bei der Vollstreckungshilfe und der sonstigen Rechtshilfe andererseits voraus, der nicht vorliegt.

Entstehenden Mehrkosten der Länder ist jedenfalls gegenüberzustellen, dass sich die Handhabung der §§ 77c ff. IRG-E dadurch vereinfacht. Zusätzliche Differenzierungen zwischen verschiedenen Datenschutzregimen sind nicht erforderlich. Dies erspart inhaltlichen Prüfaufwand und organisatorische Schritte und damit Kosten, über deren Höhe hier aus den vorstehend skizzierten Gründen aber ebenfalls keine Angaben gemacht werden können.

Zweitens geht das in § 77d Absatz 1 Nummer 3 IRG-E vorgesehene Zustimmungserfordernis vor einer Datenweiterleitung durch deutsche Behörden insoweit über die Vorgaben der Richtlinie (EU) 2016/680 hinaus, als auch die Weiterleitung von personenbezogenen Daten, die aus Drittstaaten oder von internationalen Einrichtungen stammen, erfasst wird. Darüber hinaus soll eine Zustimmung auch dann erforderlich sein, wenn die Weiterleitung der Daten innerhalb der Europäischen Union erfolgt. Der umzusetzende Artikel 35 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680 erfasst dagegen ausschließlich die Weiterleitung von Daten, die von einem anderen Mitgliedstaat oder von einer Einrichtung der Europäischen Union stammen und die an Drittstaaten weitergeleitet werden sollen. Das im IRG damit umfassend angelegte Zustimmungserfordernis entspricht allerdings der schon bisher geübten Rechtspraxis, weil der rechtshilferechtliche Spezialitätsgrundsatz zu wahren ist. Mehrkosten fallen insoweit nicht an. Für die grenzüberschreitende Datenübermittlung im Rahmen der strafrechtlichen Rechtshilfe gibt es im Übrigen schon jetzt internationale Vorgaben, die von den zuständigen Justizbehörden und Gerichten zu beachten sind, siehe etwa Artikel 23 EU-RhÜbk. Die bloße Aktualisierung oder auch die bloße klarstellende Regelung des europäischen Datenschutzniveaus durch die Richtlinie (EU) 2016/680 löst im Grundsatz keinen zusätzlichen Aufwand in sachlicher, personeller oder organisatorischer Hinsicht bei den beteiligten Stellen aus.

Inhaltlich neu bzw. jedenfalls neu gesetzlich kodifiziert sind insbesondere die folgenden Verpflichtungen der deutschen Justizbehörden:

§ 77d Absatz 1 Nummer 3 IRG-E	Verpflichtung zur Einholung einer Zustimmung der zuständigen Behörde vor Datenweiterleitung an andere Staaten oder internationale oder europäische Organisationen
§ 77d Absatz 4 Satz 2 IRG-E	Unterrichtungspflicht, wenn Zustimmung nach § 77d Absatz 1 Nummer 3 IRG-E nicht eingeholt werden kann
§ 77e Absatz 1 IRG-E	Insgesamt acht im Einzelnen geregelte Prüf-, Informations- und Protokollierungspflichten
§ 97c IRG-E	Unterrichtungspflicht im Fall einer Datenschutzverletzung

Die vorstehend aufgelisteten Pflichten führen zu einem gewissen Mehraufwand bei den zuständigen deutschen Justizbehörden. Konkrete Angaben oder belastbare Schätzungen zu den zusätzlichen Kosten, die sich daraus für die Landesjustizbehörden ergeben, können nicht vorgenommen werden, weil sich insbesondere die Fallzahlen nicht vorhersagen lassen, siehe oben.

Anfallen wird für die jeweils befassten Justizbehörden auch ein einmaliger Einarbeitungsaufwand, der gegebenenfalls durch Schulungsangebote von Seiten des Bundes und der Länder verringert werden kann.

Insgesamt ist zu erwarten, dass ein Mehraufwand mit den bestehenden personellen und sachlichen Ressourcen aufgefangen werden kann:

Die Einrichtung neuer Organisationsstrukturen in den Ländern ist nicht erforderlich. Da schon bisher internationale datenschützende Vorschriften einzuhalten waren, stellt sich auch die Frage, ob bestimmte Kennzeichnungs- oder Protokollierungspflichten für die beteiligten Behörden erforderlich sind, damit die datenschützenden Vorgaben tatsächlich Beachtung finden können, nicht erst durch die Neuregelung der Richtlinie (EU) 2016/680. Zudem entspricht die Einholung von Zustimmungen vor einer Zweckänderung bei der Verwendung von Fremddaten mit Blick auf den allgemeinen rechtshilferechtlichen Spezialitätsgrundsatz schon jetzt der Rechtspraxis. Ein Anstieg des Fallaufkommens aus Anlass der Umsetzung der Richtlinie (EU) 2016/680 ist nicht zu erwarten.

Zudem ist etwaigem Mehraufwand gegenüberzustellen, dass die zusammenhängende Regelung der im Rechtshilfeverkehr zu beachtenden allgemeinen datenschützenden Vorschriften der Rechtspraxis die Übersicht und die Handhabbarkeit erleichtert. Dies kann sich dauerhaft entlastend für die zuständigen Justizbehörden auswirken.

Für die Justizbehörden des Bundes kann ebenfalls Mehraufwand anfallen, der sich unmittelbar aus der Richtlinie (EU) 2016/680 ergibt. Fallzahlen gibt es auch hier nicht. Maßgeblich sind insoweit vor allem die Kosten, die beim Bundesamt für Justiz (BfJ) und beim Generalbundesanwalt beim BGH (GBA) anfallen. Das BfJ ist insbesondere dann Normadressat, wenn für den Rechtshilfeverkehr der diplomatische oder der ministerielle Geschäftsweg gilt; dies bedeutet jeweils eine Beteiligung der Bundesebene. Für den Rechtshilfeverkehr innerhalb der Europäischen Union gilt grundsätzlich der sogenannte unmittelbare Geschäftsweg, siehe oben. Hier ist das BfJ nur betroffen, wenn es als zuständige Behörde in die grenzüberschreitende strafrechtliche Zusammenarbeit aktiv eingebunden ist, etwa als zentrale Bewilligungsbehörde des Bundes für eingehende und ausgehende Ersuchen nach den §§ 86 ff. IRG. Aber auch soweit das BfJ etwa von den Länderbehörden unter bestimmten Umständen

über Einzelfälle unterrichtet wird und dann personenbezogene Daten verarbeitet, ist es an die datenschutzrechtlichen Vorgaben gebunden. Der GBA nimmt als Strafverfolgungsbehörde des Bundes an der strafrechtlichen Zusammenarbeit innerhalb der Europäischen Union teil. Sowohl für das BfJ als auch für den GBA gelten die Ausführungen zum Mehraufwand bei den Länderbehörden entsprechend.

Für den Bereich der Zollverwaltung entsteht im Haushaltsjahr 2018 einmaliger Erfüllungsaufwand in Höhe von rund 15 000 Euro. Der einmalige Erfüllungsaufwand teilt sich auf in rund 12 000 Euro Personalkosten und 3 000 Euro Sachkosten für Schulungen von Beschäftigten sowie für die Beschreibung der fachlichen Anforderungen zur Anpassung von IT-Verfahren.

Darüber hinaus wird ein jährlicher Erfüllungsaufwand in Höhe von rund 26 000 Euro (20 000 Euro Personal- und 6 000 Euro Sachkosten) erwartet. Dieser wird bei der Generalzolldirektion im Bereich der FKS und den Datenschutzbeauftragten der Zollverwaltung anfallen.

Mehrbedarf an Sach- und Personalmitteln beim Bund soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden..

– Weitere Anpassungen

Bei den Änderungen innerhalb der ZStVBetrV und der Eurojust-Anlaufstellenverordnung handelt es sich um Anpassungen bzw. Folgeänderungen redaktioneller Natur, die keinen eigenen Erfüllungsaufwand auslösen.

bb) Im Rahmen der bereichsspezifischen Anpassungen an die Datenschutz-Grundverordnung

Die gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31) bereits bestehenden Betroffenenrechte, wie etwa das Auskunftsrecht, das Recht auf Berichtigung und Löschung, das Recht auf Einschränkung der Verarbeitung sowie das Widerspruchsrecht, werden durch die Datenschutz-Grundverordnung gestärkt. Mit dem vorliegenden Gesetzentwurf ist kein zusätzlicher Erfüllungsaufwand für die Verwaltung, verbunden, der über die Folgen der Datenschutz-Grundverordnung hinausgeht.

## **5. Weitere Gesetzesfolgen**

Gleichstellungs- und verbraucherpolitische sowie demografische Auswirkungen sind nicht zu erwarten.

## **VII. Befristung, Evaluierung**

Eine Befristung des Gesetzes ist nicht vorgesehen, weil auch die korrespondierenden EU-Rechtsakte nicht zeitlich befristet sind. Eine Evaluierung auf nationaler Ebene ist ebenfalls nicht vorgesehen; in Bezug auf die Umsetzung der Richtlinie (EU) 2016/680 erfolgt eine Evaluierung nach Artikel 62 Absatz 1 der Richtlinie (EU) 2016/680 durch die Europäische Kommission.

## **B. Besonderer Teil**

### **Zu Artikel 1 (Änderung der Strafprozessordnung - StPO)**

#### **Zu Nummer 1 (Änderung der Inhaltsübersicht)**

##### **Zu Buchstabe a**

Die Anpassung der Inhaltsübersicht ist auf Grund der Neufassung der §§ 477 bis 480 StPO-E erforderlich.

##### **Zu den Buchstaben b bis i**

Es handelt sich um redaktionelle Änderungen, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden sind.

#### **Zu Nummer 2 (Neufassung des § 81f Absatz 2 Satz 3 und 4 StPO)**

##### **Zu Buchstabe a**

Es handelt sich um redaktionelle Änderungen, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

##### **Zu Buchstabe b**

Es handelt sich um eine Folgeänderung auf Grund der Neukonzeption des BDSG und der Einführung der Datenschutz-Grundverordnung. Der bisherige Verweis auf das BDSG wird entsprechend aktualisiert. Der Verweis soll sicherstellen, dass das Datenschutzniveau der Datenschutz-Grundverordnung und des BDSG (2018) auch bei nicht-öffentlichen Stellen technikneutral – d.h. auch bei der nicht automatisierten Verarbeitung der Daten und wenn diese nicht in Dateisystemen gespeichert sind oder werden sollen – gewährleistet ist. Insbesondere unterliegen die betroffenen Stellen damit auch der Aufsicht im Sinne des § 40 BDSG (2018). Wie auch nach der bisherigen Regelung, soll die Aufsichtsbehörde die Einhaltung der datenschutzrechtlichen Vorschriften unabhängig davon überwachen, konkrete Anhaltspunkte für einen Verstoß vorliegen. Einer ausdrücklichen Regelung hierzu bedarf es jedoch nicht, da die Aufsichtsbehörden bereits nach § 40 BDSG (2018) in Verbindung mit den Artikeln 55 und 57 der Datenschutz-Grundverordnung unabhängig vom Vorliegen solcher Anhaltspunkte kontrollieren dürfen.

#### **Zu Nummer 3 (Anpassung des Verweises in § 97 Absatz 5 Satz 2 StPO)**

Es handelt sich um eine redaktionelle Korrektur. Durch das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (BGBl. I 2017, 3618) wurde der frühere Absatz 2 Satz 3 zu Satz 2, so dass der Verweis in Absatz 5 Satz 1 entsprechend anzupassen war.

#### **Zu Nummer 4 (Streichung von § 100e Absatz 6 StPO)**

Die Streichung betrifft die verfahrensübergreifende Verarbeitung personenbezogener Daten, die durch die besonders eingriffsintensive Maßnahmen nach den §§ 100b und 100c StPO erhoben wurden und die nur bei Verdacht bestimmter Straftaten zulässig sind. Diese soll innerhalb der StPO-E zukünftig gebündelt geregelt werden, nämlich in § 161 StPO-E für die Verarbeitung von Daten, die durch polizeiliche Maßnahmen erhoben wurden, und in § 479 StPO-E für die Verarbeitung von Daten, die durch strafverfahrensrechtliche Maßnahmen erhoben wurden. § 100e Absatz 6 ist daher aufzuheben.

Der Regelungsgehalt seiner bisherigen Nummer 1 zur Verwendung der durch eine Maßnahme nach den §§ 100b StPO oder 100c StPO erlangten personenbezogenen Daten in anderen Strafverfahren findet sich nun in § 479 Absatz 2 Satz 1 StPO-E. Der Regelungsgehalt der bisherigen Nummer 2 zur Verwendung der durch eine Maßnahme nach den §§ 100b StPO oder 100c erlangten personenbezogenen Daten zu Zwecken der Gefahrenabwehr findet sich nun in § 479 Absatz 3 Satz 1 Nummer 1, Satz 3 und 4 StPO-E. Die bisher in Nummer 3 geregelte Verwendung von personenbezogenen Daten, die durch polizeiliche Maßnahmen gewonnen wurden, die den in den §§ 100b StPO oder 100c StPO geregelten Maßnahmen entsprechen, in einem Strafverfahren ist nun Gegenstand von § 161 Absatz 3 StPO-E.

#### **Zu Nummer 5 (Änderung von § 100f StPO)**

##### **Zu Buchstabe a**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

##### **Zu Buchstabe b**

Der ergänzte Verweis erklärt die in § 100d Absatz 1 und 2 genannten Vorschriften zum Kernbereichsschutz für anwendbar und greif hiermit die Ausführungen des Bundesverfassungsgerichtes (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 176f.) auf.

#### **Zu Nummer 6 (Änderung von § 100h StPO)**

##### **Zu Buchstabe a**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

##### **Zu Buchstabe b**

[...]Der ergänzte Verweis erklärt die in § 100d Absatz 1 und 2 Vorschriften zum Kernbereichsschutz für anwendbar und greif hiermit die Ausführungen des Bundesverfassungsgerichtes (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 176f.) auf.

#### **Zu Nummer 7 (Änderung von § 100j StPOo)**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

#### **Zu Nummer 8 (Änderung von § 101 Absatz 8 StPO)**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

#### **Zu Nummer 9 (Aufhebung der Absätze 4 und 5)**

##### **Zu Buchstabe a**

Die Aufhebung der Absätze 4 und 5 des bisherigen § 101a StPO betrifft die verfahrensübergreifende Verarbeitung personenbezogener Daten, die durch besonders eingriffssintensive Maßnahmen erhoben wurden, welche nur bei Verdacht bestimmter Straftaten zulässig sind. Diese soll innerhalb der StPO zukünftig gebündelt geregelt werden, nämlich in § 161 StPO-E für die Verarbeitung von Daten, die durch polizeiliche Maßnahmen erhoben wurden, und in § 479 StPO-E für die Verarbeitung von Daten, die durch strafverfahrens-



rechtliche Maßnahmen erhoben wurden. Der Regelungsinhalt des bisherigen Absatzes 4 Satz 1 Nummer 1 zur Verwendung der durch eine Maßnahme nach § 100g Absatz 2, auch in Verbindung mit § 100g Absatz 3 Satz 2 StPO gewonnenen Daten in anderen Strafverfahren findet sich nun in § 479 Absatz 2 Satz 1 StPO-E. Der Regelungsinhalt des bisherigen Absatzes 4 Satz 1 Nummer 2 zur Verwendung entsprechender Daten zu Zwecken der Gefahrenabwehr ist nun Gegenstand des § 479 Absatz 3 Satz 1 Nummer 2 StPO-E. Der bisher in Absatz 4 Satz 2 geregelte Inhalt ist nun Gegenstand des § 478 Absatz 2 StPO-E. Der Inhalt des bisherigen Absatzes 4 Satz 3 und 4 ist nun in § 479 Absatz 2 Satz 3 und 4 StPO-E geregelt. Der Inhalt des bisherigen Absatzes 5 geht nun in § 161 Absatz 3 StPO-E auf.

#### **Zu Buchstabe b**

Es handelt sich um eine Folgeänderung zur Aufhebung der Absätze 4 und 5.

#### **Zu Nummer 10 (Änderung von § 100 b StPO)**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

#### **Zu Nummer 11 Ergänzung von § 110a Absatz 1 StPO)**

Der ergänzte Verweis erklärt die in § 100d Absatz 1 und 2 Vorschriften zum Kernbereichsschutz für anwendbar und greif hiermit die Ausführungen des Bundesverfassungsgerichtes (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 176f.) auf.

#### **Zu Nummer 12 (Änderung von § 119 Absatz 4 Satz 2 StPO)**

Es handelt sich um eine Folgeänderung auf Grund der Neukonzeption des BDSG und der Einführung der Datenschutz-Grundverordnung. Der bisherige Verweis auf das BDSG wird entsprechend aktualisiert.

#### **Zu Nummer 13 (Änderung von § 155b StPO)**

##### **Zu Buchstabe a**

Es handelt sich um redaktionelle Änderungen, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden sind.

##### **Zu Buchstabe b**

Es handelt sich um eine Folgeänderung auf Grund der Neukonzeption des BDSG und der Einführung der Datenschutz-Grundverordnung. Der bisherige Verweis auf das BDSG wird entsprechend angepasst. Auf die Begründung zur Änderung von § 81f wird verwiesen.

#### **Zu Nummer 14 (Aufhebung des § 160 Absatz 4 StPO)**

Der bisherige § 160 Absatz 4 StPO betrifft die Unzulässigkeit einer Maßnahme im Falle eines bundes- oder landesgesetzlichen Verwendungsverbotes. Da sich hieraus eine Einschränkung der in § 161 Absatz 1 StPO-E bestimmten Ermittlungsbefugnisse ergibt, wird § 160 Absatz 4 aufgehoben und dessen bisheriger Wortlaut in § 161 Absatz 1 StPO-E als neuer Satz 3 angefügt.

#### **Zu Nummer 15 (Neufassung des § 161 StPO)**

Die Neufassung des § 161 StPO-E dient der Bündelung verschiedener, bisher an unterschiedlichen Stellen innerhalb der StPO verankerter Erhebungs- und Verwendungsbe-

schränkungen, der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680 und der Anpassung an das BDSG (2018).

Absatz 1 wird um den neuen Satz 3 ergänzt, welcher inhaltlich dem bisherigen § 160 Absatz 4 StPO entspricht. Die Umstellung dient allein systematischen Zwecken, da die Regelung eine Beschränkung der in Absatz 1 geregelten Ermittlungsbefugnisse zum Gegenstand hat. Eine Änderung der bisherigen Rechtslage ist hiermit nicht verbunden.

Absatz 2 Satz 1 dient der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680, wonach die Verarbeitung besonderer Kategorien personenbezogener Daten nur unter besonderen Voraussetzungen zulässig ist. Grundsätzlich sind die Befugnis zur Verarbeitung besonderer Kategorien personenbezogener Daten sowie die hierbei geltenden Anforderungen bereits in § 48 BDSG (2018) vorgesehen. Damit käme § 48 BDSG (2018) auch ohne ausdrücklichen Verweis zur Anwendung. Da die Erhebung besonderer Kategorien personenbezogener Daten im Strafverfahren von hoher praktischer Relevanz sein wird, wird Absatz 2 Satz 1 jedoch zum Zwecke der Klarstellung aufgenommen.

Absatz 2 Satz 2 schließt die im BDSG (2018) vorgesehenen Ausnahmen von der Pflicht zur Löschung personenbezogener Daten für die in der StPO besonders geregelten Löschungspflichten aus. § 58 Absatz 3 BDSG (2018) sieht vor, dass von einer grundsätzlich gebotenen Löschung personenbezogener Daten in bestimmten Fällen abgesehen werden kann; anstelle der Löschung ordnet § 58 Absatz 3 BDSG (2018) insofern die Einschränkung der Verarbeitung der betroffenen Daten an. In der StPO ist jedoch vielfach eine bewusst strikt gefasste Pflicht zur Löschung bestimmter Daten, die als besonders sensibel eingestuft werden, vorgesehen (z. B. § 81h Absatz 3, § 100a Absatz 4, § 100c Absatz 5, § 100g Absatz 4 Satz 2 und § 101 Absatz 8 StPO). Ohne den Ausschluss in Absatz 2 Satz 2 könnten die Ausnahmetatbestände des § 58 Absatz 3 BDSG (2018) über den Verweis in § 75 Absatz 3 BDSG (2018) auch auf diese gesetzlichen Löschungspflichten Anwendung finden. Dies würde aber die bewusst strikte Ausgestaltung der innerhalb der StPO geregelten Löschungspflichten unterlaufen.

Absatz 3 soll an die Stelle des bisherigen Absatz 2 Satz 1 treten und die allgemeinen Voraussetzungen der Verwendung von Daten regeln, die durch besonders eingriffsintensive nicht strafprozessuale Maßnahmen erhoben wurden, welche nach der StPO an das Vorliegen des Verdachts bestimmter Straftaten geknüpft sind. Anders als der bisherige Absatz 2 Satz 1 enthält Absatz 3 insoweit nicht mehr nur die Verwendung „zu Beweis Zwecken“, d.h. die Vorschrift beschränkt nunmehr auch die Verwendung als Spurenansatz oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten. Diese Anpassung greift das durch das Bundesverfassungsgericht präzisierte verfassungsrechtliche Gebot zur Begrenzung der zweckändernden Verwendung von Daten, die durch eingriffsintensive Maßnahmen erhoben wurden, auf (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 315).

Dem Bundesverfassungsgericht zufolge setzt zudem auch die zweckändernde Verwendung mindestens das Vorliegen eines konkreten Ermittlungsansatzes voraus (vgl. BVerfG, a.a.O.). Die Verwendung steht daher unter der Voraussetzung, dass eine Anordnung der jeweiligen Maßnahme „jeweils“, d.h. im Einzelfall, zulässig wäre.

Spezielle Regelungen zur strafprozessualen Verwertbarkeit personenbezogener Daten, die aus polizeilichen Maßnahmen der Wohnraumüberwachung stammen bzw. für Verkehrsdaten, die auf Basis von § 113b des Telekommunikationsgesetzes gespeichert und auf polizeirechtlicher Grundlage erhoben wurden, waren bisher Gegenstand des § 100e Absatz 6 StPO und des § 101a Absatz 5 StPO. Maßgeblicher Unterschied zu der bisherigen Regelung in § 161 Absatz 2 Satz 2 war insoweit, dass durch § 100e Absatz 6 StPO und § 101a Absatz 5 StPO nicht nur die Verwendung „zu Beweis Zwecken“, sondern z.B. auch die Verwendung als Spurenansatz an besondere Bedingungen geknüpft haben.

Dieser Sonderregelung bedarf es angesichts der oben beschriebenen Anpassung nicht mehr. Somit entfällt auch die Notwendigkeit für den bisher in Absatz 2 Satz 2 enthaltenen Verweis.

Absatz 4 entspricht – mit Ausnahme der Streichung der Wörter „zu Beweis Zwecken“ zu deren Begründung auf die Ausführungen zu Absatz 3 verwiesen wird – inhaltlich dem bisherigen Absatz 3.

#### **Zu Nummer 16 (Einfügen eines § 163 Absatz 1 Satz 3 StPO)**

Die nun in § 161 Absatz 1 Satz 3 und Absatz 2 bis 4 StPO-E vorgesehenen Einschränkungen galten auch bisher für die polizeilichen Befugnisse nach § 163 StPO entsprechend. Durch den Verweis in dem neu geschaffenen § 163 Absatz 1 Satz 3 StPO-E soll klargestellt werden, dass dies auch nach der Neuordnung der Fall bleiben wird.

#### **Zu Nummer 17 (Änderung von § 163d Absatz 1 Satz 1 StPO)**

Es handelt sich um redaktionelle Änderungen, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden sind.

#### **Zu Nummer 18 (Änderung von § 406d Absatz 2 Satz 1 StPO)**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

#### **Zu Nummer 19 (Verweis auf § 57 BDSG (2018) in § 475 Absatz 1 Satz 1 StPO)**

Der klarstellende Hinweis auf § 406e StPO erscheint vor dem Hintergrund der unterschiedlichen Anwendungsbereiche und Voraussetzungen des § 406e StPO und des § 475 StPO-E entbehrlich, so dass auf ihn verzichtet werden kann. An seine Stelle tritt ein Hinweis auf § 57 BDSG (2018), der klarstellen soll, dass der datenschutzrechtliche Auskunftsanspruch von den Auskunfts- bzw. Akteneinsichtsmöglichkeiten in § 475 StPO-E zu unterscheiden ist und auch nicht durch § 475 StPO-E verdrängt wird.

Dies soll zukünftig insbesondere auch für den Anwendungsbereich des bisherigen § 491 StPO (vgl. die dortige Begründung) gelten, der nach bisherigem Recht den datenschutzrechtlichen Auskunftsanspruch ausdrücklich ausschließt, soweit in der StPO eigene Auskunftsregelungen vorgesehen sind.

#### **Zu Nummer 20 (Änderung § 476 Absatz 8 StPO)**

Es handelt sich um eine Folgeänderung auf Grund der Neukonzeption des BDSG und der Einführung der Datenschutz-Grundverordnung. Der bisherige Verweis auf das BDSG wird entsprechend angepasst.

#### **Zu Nummer 21 (Neufassung der §§ 477 bis 480 StPO)**

Die §§ 477 ff. StPO-E werden insgesamt systematisch überarbeitet. Der systematische Aufbau des Ersten Abschnitts des Achten Buches soll nun derart gestaltet sein, dass in den §§ 474 bis 477 StPO-E die rechtlichen Voraussetzungen der Datenübermittlung, in § 478 StPO-E die Form der Übermittlung, in § 479 StPO-E Übermittlungsverbote und Verwendungsbeschränkungen sowie in § 480 StPO-E die Verantwortlichkeit für die Beurteilung der Zulässigkeit der Übermittlung sowie das Verfahren hierzu geregelt sind. § 479 StPO-E soll zudem Regelungen zur verfahrensübergreifenden Verarbeitung personenbezogener Daten, die durch besonders eingriffsintensive und daher nur bei Verdacht bestimmter Straftaten zulässige Maßnahmen erhoben worden sind, bündeln. Die Anzahl der

bisher erforderlichen Verweise innerhalb des Ersten Abschnitts des Achten Buches oder auf Regelungen im Achten Abschnitt des Ersten Buches wird hierdurch reduziert.

### **Zu § 477 (Datenübermittlung von Amts wegen)**

Der neu gefasste § 477 StPO-E entspricht dem bisherigen § 479 Absatz 1 und 2 StPO und regelt die Voraussetzungen der Übermittlung von Amts wegen. Die neu gewählte Reihenfolge soll die Übersichtlichkeit der Regelungssystematik verbessern, indem nun in den §§ 474 bis 477 StPO-E jeweils die Voraussetzungen der Übermittlung – auch für die Übermittlung von Amts wegen – und in den §§ 478 bis 480 StPO-E dann für alle Anlässe gebündelt Fragen der Form der Übermittlung, etwaiger Beschränkungen, Zuständigkeits- und Verfahrensfragen geregelt werden. Der insoweit bisher in § 479 Absatz 3, Halbsatz 1 StPO-E enthaltene Verweis wird durch die Neuordnung entbehrlich. Gleiches gilt für die bisher in § 479 Absatz 3 Halbsatz 2 StPO-E enthaltene Regelung zur Verantwortung der übermittelnden Stelle.

### **Zu § 478 (Form der Datenübermittlung)**

Der neu gefasste § 478 StPO-E betrifft die Form der Übermittlung und entspricht inhaltlich dem bisherigen § 477 Absatz 1 StPO.

### **Zu § 479 (Übermittlungsverbote und Verwendungsbeschränkungen)**

Bisher enthalten sowohl § 477 Absatz 2 Satz 2 und 3 als auch § 100e Absatz 6 Nummer 1 und 2 und § 101a Absatz 4 StPO besondere Bestimmungen zur verfahrensübergreifenden Verarbeitung personenbezogener Daten, die durch Maßnahmen nach der StPO erhoben wurden, welche nur bei Verdacht bestimmter Straftaten zulässig sind. Dies führt nach geltender Rechtslage u. a. dazu, dass in Bezug auf Daten, die durch eine Maßnahme nach § 100a StPO gewonnen wurden, die allgemeine Verwertungsbeschränkung in § 477 Absatz 2 Satz 2 StPO Anwendung findet, in Bezug auf Daten, die durch Maßnahmen nach den §§ 100b und 100c StPO oder 100g Absatz 2 StPO erhoben wurden, jedoch jeweils die in den §§ 100e StPO und 101a StPO besonders geregelten Beschränkungen. Zum Zwecke der Bündelung wird deren Regelungsgehalt nun in die neu eingefügten Absätze 3 und 4 aufgenommen. Der Verweis auf § 100i Absatz 2 Satz 2 StPO und § 108 Absatz 2 und 3 StPO bleibt bestehen.

Absatz 2 Satz 1 soll an die Stelle des ehemaligen § 477 Absatz 2 Satz 2 treten; seine Anpassung (Streichung der Wörter „zu Beweis Zwecken“ und Ergänzung des Wortes „jeweils“) greifen das durch das Bundesverfassungsgericht präzisierende verfassungsrechtliche Gebot zur Begrenzung der zweckändernden Verwendung von Daten, die durch eingriffsintensive Maßnahmen erhoben wurden auf (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 315) Es wird auf die Erläuterungen zu § 161 Absatz 3 verwiesen.

Die nunmehr in Absatz 2 Satz 2 Nummer 1 geregelten Voraussetzungen für die Verwendung strafprozessual erhobener Daten zu Zwecken der Gefahrenabwehr soll ebenfalls inhaltlich angepasst werden. Hintergrund sind die durch das Bundesverfassungsgericht formulierten Anforderungen zur zweckändernden Verwendung von Daten, die durch eingriffsintensive Maßnahmen erhoben wurden (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09). Diesen Anforderungen entsprechend soll Absatz 2 Satz 2 Nummer 1 die Voraussetzungen der Verwendung strafprozessual erhobener Daten zu Zwecken der Gefahrenabwehr nunmehr konkretisieren.

Absatz 2 Satz 2 Nummer 2 und 3 entspricht dem bisherigen § 477 Absatz 2 Satz 3 Nummern 2 und 3 StPO.

Absatz 3 regelt nun die Verwertung personenbezogener Daten, die durch Maßnahmen nach den §§ 100b, 100c oder 100g Absatz 2, auch in Verbindung mit § 100g Absatz 3 Satz 2 erlangt wurden, zu Zwecken der Gefahrenabwehr. Absatz 3 bündelt die insoweit bisher in § 100e Absatz 6 und § 101a Absatz 4 enthaltenen Vorgaben. Die Verwendung der durch solche Maßnahmen gewonnenen Daten in anderen Strafverfahren richtet sich nun nach Absatz 2 Satz 1. Hierzu wird auf die Begründung zu § 161 Absatz 3 verwiesen.

Absatz 4 entspricht dem bisherigen Absatz 3, Absatz 5 entspricht dem bisherigen § 477 Absatz 4 bzw. § 479 Absatz 3. Absatz 6 entspricht dem bisherigen Absatz § 477 Absatz 5 StPO.

#### **Zu § 480 (Entscheidung über die Datenübermittlung)**

§ 480 StPO-E entspricht dem derzeitigen § 478 StPO. Hinzu kommt lediglich der neue Absatz 4, der die bisherige Regelung des § 101a Absatz 4 Satz 2 StPO aufgreift, wonach die Übermittlung der betroffenen Daten und der Zweck der Übermittlung aktenkundig zu machen sind. Die bisherige Regelung in § 101a Absatz 4 Satz 2 StPO betraf nur die Übermittlung von Verkehrsdaten, die im Wege des § 100g Absatz 2 StPO erhoben wurden. § 480 Absatz 4 StPO-E vereinheitlicht die Dokumentationspflicht nunmehr für alle verfahrensübergreifenden Übermittlungen nach den §§ 474 bis 477 StPO-E. Diese Dokumentation ist schon auf Grund der verschiedenen zweckbezogenen Verwendungsbeschränkungen sinnvoll und dürfte weitestgehend bereits der Praxis entsprechen, da bei Übermittlungen der genannten Art ohnehin entsprechende Aktenvermerke erfolgen dürften.

Der Inhalt des derzeitigen § 480 StPO wird im Entwurf nicht ausdrücklich übernommen, ohne dass hiermit eine Änderung der Rechtslage verbunden ist. Bei dem bisherigen § 480 handelt es sich um eine rein klarstellende Regelung, der keine weitere Bedeutung zukommt. Auf diese kann verzichtet werden. Besondere gesetzliche Bestimmungen, die die Übermittlung personenbezogener Daten aus Strafverfahren anordnen oder erlauben, bleiben demnach auch nach der Neufassung der §§ 477 bis 480 StPO-E unberührt.

#### **Zu Nummer 22 (Änderung von § 481 Absatz 3 StPO)**

Es handelt sich um eine Folgeänderung zur Neuordnung der §§ 477 bis 480 StPO-E. Der bisherige Verweis wird entsprechend angepasst.

#### **Zu Nummer 23 (Änderung der Überschrift des zweiten Abschnitts des achten Buches der StPO)**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

#### **Zu Nummer 24 (Änderung des § 483 StPO)**

Es handelt sich um redaktionelle Änderungen, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden sind.

#### **Zu Nummer 25 (Änderung des § 484 StPO)**

Es handelt sich um redaktionelle Änderungen, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden sind.

#### **Zu Nummer 26 (Änderung des § 485 StPO)**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

## **Zu Nummer 27 (Änderung des § 486 StPO)**

### **Zu Buchstabe a und Buchstabe b**

Es handelt sich um redaktionelle Änderungen, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden sind.

### **Zu Buchstabe c**

Es handelt sich um eine Folgeänderung auf Grund der Neukonzeption des BDSG und der Einführung der Datenschutz-Grundverordnung. Der bisherige Verweis auf das BDSG wird entsprechend angepasst.

## **Zu Nummer 28 (Änderung des § 487 StPO)**

### **Zu Buchstabe a**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

### **Zu Buchstabe b**

Es handelt sich um eine Folgeänderung zur Neuordnung der §§ 477 bis 480 StPO-E. Der bisherige Verweis wird entsprechend angepasst.

### **Zu Buchstabe c**

Die Regelung soll deutlich machen, dass das allgemeine Auskunftsrecht nunmehr auch neben den sonstigen Regelungen der StPO zu Auskünften aus Akten und zur Akteneinsicht zur Anwendung kommt. Die Ausschlussklausel des bisherigen § 491 Absatz 1 Satz 1 StPO wird aufgehoben (vgl. insoweit die Begründung zu Nummer 9). Die Voraussetzungen, der Gegenstand und etwaige Einschränkungen des Auskunftsrechts richten sich ausschließlich nach § 57 BDSG (2018). Dies gilt auch für die Verfahrensvorschriften, die sich aus dem BDSG (2018) ergeben.

## **Zu Nummer 29 (Änderung von § 488 StPO – Automatisierte Verfahren für Datenübermittlungen)**

### **Zu Buchstabe a**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

### **Zu Buchstabe b**

Es handelt sich um eine Folgeänderung auf Grund der Neukonzeption des BDSG und insbesondere des hiermit verbundenen Wegfalls von § 10 Absatz 2 BDSG.

### **Zu Buchstabe c**

In Umsetzung von Artikel 25 der Richtlinie (EU) 2016/680 sieht § 76 BDSG (2018) eine verpflichtende und nicht auf Stichproben beschränkte Protokollierungspflicht für automatisierte Verarbeitungssysteme vor. Dies gilt auch für die in der StPO vorgesehenen automatisierten Verarbeitungssysteme. Der neue § 488 Absatz 3 StPO-E tritt damit nur noch ergänzend neben § 76 BDSG (2018).

### **Zu Doppelbuchstabe aa**

Durch die Anpassung soll deutlich gemacht werden, dass die durch die Protokollierung vermittelte Überprüfbarkeit umfassend, d. h. nicht mehr nur für Stichproben zu gewährleisten ist.

### **Zu Doppelbuchstabe bb**

§ 76 BDSG (2018) benennt bereits bestimmte Daten, die allgemein bei automatisierten Verarbeitungssystemen zu protokollieren sind. Der neue § 488 Absatz 3 Satz 4 StPO-E soll daher nur noch diejenigen Informationen bezeichnen, die bei automatisierten Anfrage- und Auskunftsverfahren im Sinne des § 488 StPO-E ergänzend protokolliert werden sollen (abgerufene Daten, Kennung der abrufenden Stelle und Aktenzeichen des Empfängers).

§ 488 Absatz 3 Satz 5 StPO-E bestimmt die von § 76 BDSG (2018) abweichende Frist für die Löschung der Protokolldaten. Eine eigene Regelung der Verwendungszwecke der Protokolldaten (wie im bisherigen Absatz 3 Satz 5) ist nicht mehr erforderlich, da diese nunmehr bereits unmittelbar aus § 76 Absatz 3 BDSG (2018) folgen. Inhaltlich ist § 76 Absatz 3 BDSG (2018) weiter gefasst als der bisherige § 488 Absatz 3 Satz 5 StPO, da die dort benannten Verwendungszwecke über die Zulässigkeitskontrolle hinausgehen. Dadurch erfolgt eine Anpassung an Artikel 25 Absatz 3 der Richtlinie (EU) 2016/680.

### **Zu Doppelbuchstabe dd**

§ 488 Absatz 2 und 3 StPO-E stellen sprachlich – im Gegensatz zu § 488 Absatz 1 Satz 1 StPO-E – allein auf das automatisierte Abrufverfahren ab. Nur § 488 Absatz 1 Satz 1 StPO-E nennt daneben ausdrücklich auch das Anfrage- und Auskunftsverfahren. Der neu angefügte § 488 Absatz 4 soll deshalb klarstellen, dass auch das Anfrage- und Auskunftsverfahren als Abrufverfahren im Sinne des Datenschutzrechts zu werten ist und die Vorgaben der Absätze 2 und 3 daher auch hierauf Anwendung finden (vgl. Weßlau in: Systematischer Kommentar zur StPO, 4. Auflage, § 488 StPO, Rn. 1). Die Regelung entspricht insoweit dem für den Bereich des ZStV geltenden § 493 Absatz 4 StPO-E.

### **Zu Nummer 30 (Änderung von § 489 StPO – Berichtigung, Löschung und Einschränkung der Verarbeitung)**

Da die unmittelbar anwendbaren §§ 75 und 57 Absatz 4 und 5 BDSG (2018) bereits allgemeine Regelungen zur Berichtigung, Löschung und Einschränkung der Verarbeitung vorsehen, wurde ein Teil der bisher in § 489 StPO vorgesehenen Regelungen entbehrlich. Dieser ist daher auf die hierüber hinausgehenden, besonderen Regelungsinhalte zu reduzieren.

So ergeben sich die bisher in § 489 Absatz 1 und Absatz 2 Satz 1 StPO vorgesehenen allgemeinen Berichtigungs- und Löschungspflichten nunmehr schon aus § 75 Absatz 1 und 2 BDSG (2018). Eine eigene Regelung innerhalb der StPO ist damit nicht mehr erforderlich.

In § 489 Absatz 1 und 2 StPO-E sind somit nur noch die zuvor in § 489 Absatz 2 Satz 2 und Absatz 3 StPO ausgestalteten besonderen Gründe einer Pflicht zur Löschung ausdrücklich geregelt.

Der neue § 489 Absatz 3 StPO-E tritt an die Stelle des bisherigen § 489 Absatz 4 StPO und legt die nach § 75 Absatz 4 BDSG (2018) einzuhaltenden Fristen zur Überprüfung etwaiger Löschungspflichten fest.

Der neue § 489 Absatz 4 StPO-E tritt an die Stelle des bisherigen § 489 Absatz 5 StPO und lässt weiterhin die Regelung kürzerer Fristen im Wege der Errichtungsanordnung zu.

Der neue § 489 Absatz 5 entspricht dem bisherigen § 489 Absatz 6 StPO.

Der neue § 489 Absatz 6 StPO-E regelt die bisher in § 489 Absatz 7 StPO ausgestaltete Einschränkung der Verarbeitung. Der neu eingefügte Verweis auf § 58 Absatz 3 Satz 1 Nummer 1 und 3 BDSG (2018) ist erforderlich, da der neue § 161 Absatz 2 Satz 2 StPO-E die Anwendung von § 58 Absatz 3 BDSG (2018) grundsätzlich ausschließt. Die Anwendbarkeit von § 58 Absatz 3 Satz 1 Nummer 2 BDSG (2018) kann im Hinblick auf die ohnehin weit formulierten Zwecke und die zusätzliche Verwendungsbefugnis in § 489 Absatz 6 Satz 4 StPO-E weiterhin ausgeschlossen bleiben. Die Verwendungsbeschränkung in § 489 Absatz 6 Satz 3 StPO-E kann durch einen Verweis auf § 58 Absatz 3 Satz 2 BDSG (2018) nicht vollständig ersetzt werden, da sich dieser nur auf die Einschränkung der Verwendung nach § 58 Absatz 3 Satz 1 BDSG (2018) bezieht.

Der bisherige § 489 Absatz 8 StPO entfällt im Hinblick auf §§ 75 Absatz 3 und 58 Absatz 5 BDSG (2018), die der Umsetzung von Artikel 7 Absatz 3 und Artikel 16 Absatz 5 und 6 der Richtlinie (EU) 2016/680 dienen.

### **Zu Nummer 31 (Änderung von § 490 StPO)**

Es handelt sich um redaktionelle Änderungen, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden sind.

### **Zu Nummer 32 (Änderung von § 491 StPO – Geltung des Auskunftsrechts nach BDSG (2018))**

Der bisher in Satz 1 vorgesehene teilweise Ausschluss des allgemeinen Auskunftsrechts nach dem BDSG wird im Zuge der Umsetzung der Richtlinie (EU) 2016/680 nicht aufrechterhalten.

Die bisherige Ausschlussklausel, nach der andere, in der StPO besonders geregelte Auskunftsansprüche den Auskunftsanspruch des BDSG ausschließen, soll daher fallen gelassen werden.

Nach überwiegender Auffassung sind die Regelungen der StPO zu Auskünften aus Akten und zur Akteneinsicht auf Grund dieser Ausschlussklausel als bereichsspezifische und insoweit vorrangige Spezialvorschriften gegenüber dem allgemeinen datenschutzrechtlichen Auskunftsanspruch einzuordnen (Hilger in Löwe-Rosenberg, StPO, § 491, Rn. 2).

Dies wird dem Anliegen der Richtlinie (EU) 2016/680 nicht mehr gerecht. Zwar sieht diese in Artikel 18 und unter Berücksichtigung von Erwägungsgrund 47 vor, dass die Mitgliedstaaten (u. a.) die Ausübung von Auskunftsrechten grundsätzlich auch dem einzelstaatlichen Strafverfahrensrecht unterwerfen können. Zu berücksichtigen ist aber, dass Auskunftsersuchen zur Speicherung personenbezogener Daten in Dateisystemen im Sinne der §§ 483 ff. StPO und die Auskunft aus Akten und die Akteneinsicht meist ganz unterschiedliche Informationen zum Gegenstand haben werden.

Über die in der StPO vorgesehenen Verfahrensregelungen zu Auskünften aus Akten und zur Akteneinsicht sind nämlich nur Informationen zum Inhalt der Verfahrensakte zu erlangen. Informationen über die Verarbeitung von Daten in Dateisystemen außerhalb der Verfahrensakte erhält die betroffene Person auf diesem Wege daher allenfalls, soweit die Datei selbst Gegenstand der Verfahrensakte ist, was allerdings nicht der Fall sein muss. Im Übrigen ist mit den Auskünften aus Akten und der Akteneinsicht gerade keine Auskunft über die Verarbeitung in Dateisystemen nach den §§ 483 ff. StPO verbunden.



Auch die bisher in den Sätzen 3 und 4 vorgesehenen Ausschlussfristen zu Auskunftsersuchen, die sich auf anhängige Verfahren beziehen, sind aufzuheben. Die Regelung steht in einem Spannungsverhältnis mit Artikel 15 der Richtlinie (EU) 2016/680, der vorsieht, dass jede Einschränkung des Auskunftsrechts den Interessen der betroffenen natürlichen Person Rechnung tragen muss. Bei einer starren Begrenzung auf eine bestimmte Verfahrensdauer wäre eine solche Abwägung im Einzelfall gerade versperrt. Eine Einzelfallabwägung der Interessen der betroffenen Person mit den gegen die Auskunft streitenden Belangen ist nun in den allgemeinen Bestimmungen der §§ 57 Absatz 4 und des § 56 Absatz 2 BDSG (2018) enthalten. An die Stelle der Sätze 5 bis 6 treten die allgemeinen Bestimmungen des § 57 Absatz 6 bis 8 BDSG (2018).

#### **Zu Nummer 33 (Änderung von § 492 Absatz 4)**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

#### **Zu Nummer 34 (Änderung von § 493 StPO – Automatisiertes Verfahren für Datenübermittlungen aus dem ZStV)**

Auf die Begründung zur Änderung des § 488 wird verwiesen.

#### **Zu Nummer 35 (Änderung von § 494 StPO – Berichtigung, Löschung und Einschränkung der Verarbeitung im ZStV)**

§ 494 wird im Hinblick auf die Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 redaktionell überarbeitet und inhaltlich auf die Regelungen reduziert, die nicht bereits unmittelbar aus den in §§ 75 und 57 Absatz 4 und 5 BDSG (2018) vorgesehenen allgemeinen Bestimmungen zur Berichtigung, Löschung und Einschränkung der Verarbeitung hervorgehen. Die Anpassung des Verweises in Absatz 3 ist eine Folgeänderung zur Neufassung des § 489 StPO-E. I.E. wird auf die dortige Begründung verwiesen.

#### **Zu Nummer 36 (Änderung von § 495 StPO – Geltung des Auskunftsrechts nach BDSG (2018) in Bezug auf das ZStV)**

§ 494 wird im Hinblick auf die Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 redaktionell überarbeitet und inhaltlich entsprechend der Änderungen zu § 491 angepasst. Auf die dortige Begründung Neufassung des § 489 StPO-E. I.E. ist auf die dortige Begründung wird verwiesen.

#### **Zu Nummer 37 (Änderung von § 496 Absatz 3 StPO)**

Es handelt sich um eine redaktionelle Änderung, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden ist.

#### **Zu Artikel 2 (Änderung des Einführungsgesetzes zum Gerichtsverfassungsgesetz – EGGVG)**

##### **Zu Nummer 1**

Es handelt sich um redaktionelle Änderungen zur Anpassung an die Terminologie der Datenschutz-Grundverordnung.

Soweit die Begriffe „Verwendung“ oder „verwenden“ durch die Begriffe „Verarbeitung“ oder „verarbeiten“ ersetzt wird, ist damit – entgegen der Terminologie der Datenschutz-Grundverordnung – nicht die Erhebung von Daten gemeint. Einer entsprechenden Klar-

stellung im Gesetzestext bedarf es nicht, weil sich der zweite Abschnitt des EGGVG ohnehin nur auf die Übermittlung bereits erhobener Daten bezieht.

In § 18 Absatz 1 Satz 2 EGGVG wird an dem Begriff der „Verwendung“ bewusst festgehalten. Der Begriff der „Verarbeitung“ wäre in diesem Zusammenhang zu weitgehend, weil er der empfangenden Stelle auch das Erfassen und Speichern der zusätzlich übermittelten Daten untersagen würde.

#### **Zu Nummer 5 (Änderung von § 20 EGGVG)**

Es handelt sich um redaktionelle Änderungen zur Anpassung an die Terminologie der Datenschutz-Grundverordnung.

Eine inhaltliche Anpassung des § 20 EGGVG an die Datenschutz-Grundverordnung ist nicht erforderlich. Insbesondere deckt sich dessen Regelungsinhalt nicht mit dem in Artikel 16 der Datenschutz-Grundverordnung verankerten Recht der betroffenen Person auf Berichtigung. § 20 Absatz 1 EGGVG verpflichtet zu einer Aktualisierung des Verfahrensstandes, aber nicht zu einer Berichtigung unrichtiger Daten. § 20 Absatz 2 EGGVG regelt zwar die Berichtigung unrichtiger Daten, allerdings handelt es sich dabei um eine von Amts wegen zu erfüllende Pflicht zur Berichtigung gegenüber den Empfängern dieser Daten. Einen subjektiven Anspruch der betroffenen Person auf Berichtigung der Daten bei der übermittelnden Stelle regelt § 20 Absatz 2 EGGVG hingegen nicht. § 20 Absatz 2 EGGVG entspricht inhaltlich auch nicht Artikel 19 Satz 1 der Datenschutz-Grundverordnung, der im Falle einer Berichtigung von Daten bei der übermittelnden Stelle gemäß Artikel 16 der Datenschutz-Grundverordnung eine Pflicht zur Mitteilung an etwaige Empfänger dieser Daten statuiert. Vielmehr regelt § 20 Absatz 2 EGGVG eine eigenständige und von Artikel 16 der Datenschutz-Grundverordnung unabhängige Pflicht zur Berichtigung. § 20 Absatz 3 EGGVG enthält lediglich eine verwaltungsvereinfachende Regelung, die sich auf die § 20 Absatz 1 und 2 EGGVG bezieht.

#### **Zu Nummer 6 (Änderung von § 21 EGGVG)**

##### **Zu Buchstabe a**

Es handelt sich um redaktionelle Änderungen zur Anpassung an die Terminologie der Datenschutz-Grundverordnung.

##### **Zu Buchstabe b**

Durch die vorgeschlagene Änderung wird der Kreis der von der Informationspflicht nach § 21 Absatz 2 Satz 1 EGGVG Begünstigten auf den Personenkreis der unmittelbar vom Ausgangsverfahren betroffenen Personen erweitert und bezieht nun auch den Beschuldigten in Strafsachen sowie die Partei und den Beteiligten in Zivilsachen ein. Die bisher bestehende Beschränkung der Informationspflicht auf betroffene Personen, die nicht zugleich Beschuldigte, Partei oder Beteiligte einer Straf- bzw. Zivilsache sind, soll entfallen. Es ist zum Schutz des gerichtlichen oder behördlichen Verfahrens nicht erforderlich, die Partei, den Beteiligten oder den Beschuldigten von der Informationspflicht des § 21 EGGVG auszunehmen. Denn schon nach geltendem Recht erhält die Partei bzw. der Beschuldigte in der Praxis regelmäßig Kenntnis von der erteilten Mitteilung von Amts wegen, entweder auf Grund prozessualer Grundsätze nach den Anforderungen des rechtlichen Gehörs oder über den Weg der Akteneinsicht. Sofern eine Information an den Beschuldigten oder die Partei nach geltendem Recht unterbleibt, weil sie den Verfahrenszweck oder sonstige überwiegende Belange gefährden würde, kann auch nach der vorgeschlagenen Änderung gemäß § 21 Absatz 4 EGGVG von einer Unterrichtung der betroffenen Person abgesehen werden. Im Übrigen enthält auch Artikel 13 der Richtlinie (EU) 2016/680 keine Beschränkung auf Personen außerhalb des Ausgangsverfahrens.

### **Zu Buchstabe c**

Es handelt sich um redaktionelle Änderungen zur Anpassung an die Terminologie der Datenschutz-Grundverordnung.

### **Zu Buchstabe d**

Im Anwendungsbereich der Datenschutz-Grundverordnung sollen die Absätze 1 bis 5 keine Geltung beanspruchen, weil die Artikel 12 bis 15 der Datenschutzgrundverordnung insoweit vorrangige Regelungen für den Auskunftsanspruch der betroffenen Personen sowie die Informationspflicht der übermittelnden Stelle enthalten.

### **Zu Nummer 7 (Einfügung eines neuen § 21a EGGVG)**

Mit dem neuen § 21a EGGVG wird von der Möglichkeit Gebrauch gemacht, bestimmte Rechte und Pflichten der Datenschutz-Grundverordnung im Wege von Gesetzgebungsmaßnahmen zu beschränken, sofern dies der Sicherstellung eines der in Artikel 23 Absatz 1 Buchstabe a bis j der Datenschutz-Grundverordnung genannten Schutzzwecke dient. Bei den vorgesehenen Beschränkungen geht es vor allem um den Schutz von Gerichtsverfahren (Artikel 23 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung), im Übrigen aber auch – je nach Art der verfahrensübergreifenden Mitteilung – um die weiteren Schutzgüter nach Artikel 23 Absatz 1 Buchstabe a bis j.

Gemäß dem neuen § 21 Absatz 6 EGGVG gilt § 21 EGGVG im Anwendungsbereich der Datenschutz-Grundverordnung nicht. Etwaige Auskunftsrechte der betroffenen Person sowie Informationspflichten der übermittelnden Stelle richten sich nach den Artikeln 12 bis 15 sowie 19 Satz 2 der Datenschutz-Grundverordnung. Dabei muss jedoch sichergestellt sein, dass zumindest bereichsspezifischen Beschränkungen des § 21 Absatz 3 und 4 EGGVG weiterhin Beachtung finden. Andernfalls könnte die Erteilung einer Auskunft oder die Unterrichtung der betroffenen Person dazu führen, dass die ordnungsgemäße Aufgabenerfüllung der übermittelnden oder empfangenden Stelle nicht mehr gewährleistet ist. Außerdem könnten sonstige öffentliche Interessen oder Rechte Dritter gefährdet werden. Ohne den Schutz des § 21 Absatz 4 Satz 1 Nummer 2 EGGVG müsste zum Beispiel eine Information auf Grund der in den Artikeln 13 und 14 der Datenschutz-Grundverordnung geregelten Informationspflichten oder des in Artikel 15 der Datenschutz-Grundverordnung geregelten Auskunftsrechts unter Umständen auch dann gewährt werden, wenn sie die öffentliche Sicherheit gefährden würde. Der Schutz des § 21 Absatz 3 und 4 EGGVG darf im Anwendungsbereich der Datenschutz-Grundverordnung schließlich auch nicht dadurch unterlaufen werden, dass die tatsächlichen und rechtlichen Gründe für die Ablehnung einer Auskunft mitgeteilt werden. Deshalb ist auch § 21 Absatz 5 EGGVG im Anwendungsbereich der Datenschutz-Grundverordnung entsprechend anzuwenden.

Ebenso wäre im Anwendungsbereich der Datenschutz-Grundverordnung der Zweck der verfahrensübergreifenden Mitteilungen gefährdet, wenn eine betroffene Person die Weitergabe ihrer Daten aufgrund des Rechts auf Einschränkung der Verarbeitung gemäß Artikel 18 der Datenschutz-Grundverordnung oder aufgrund des Widerspruchsrechts gemäß Artikel 21 der Datenschutz-Grundverordnung verhindern oder verzögern könnte. Zur Gewährleistung der Aufgabenwahrnehmung der übermittelnden sowie der empfangenden Stelle ist es daher erforderlich, diese Rechte der Datenschutz-Grundverordnung bei verfahrensübergreifenden Mitteilungen auszuschließen. Dem Betroffenen steht es jedoch frei, die Rechte aus den Artikeln 18 und 21 der Datenschutz-Grundverordnung gegebenenfalls in dem Ausgangsverfahren oder in dem Verfahren bei der Empfängerbehörde geltend zu machen. In der Regel wird er, soweit er Beteiligter in einem Verfahren ist und keine überwiegenden Gründe dem entgegenstehen, von der Datenverarbeitung in dem Ausgangsverfahren bereits Kenntnis erlangt haben. Hat er mit der Geltendmachung seiner Rechte im Ausgangsverfahren Erfolg, wird damit auch die Mitteilung als solche verhindert. Erhebt er jedoch erfolglos im Ausgangsverfahren Widerspruch oder begehrt ohne

Erfolg die Einschränkung der Verarbeitung, sollen diese Rechte nicht im Hinblick auf die „logische Sekunde“ der Übermittlung seiner Daten wieder aufleben. Es erscheint verfahrensökonomisch und sachgerecht, die betroffene Person in diesem Fall auf die Geltendmachung der Rechte aus den Artikeln 18 und 21 der Datenschutz-Grundverordnung in dem Verfahren vor der Empfängerbehörde zu verweisen. Anderenfalls würde der bloße Informationsaustausch und damit die Aufgabenerfüllung der beteiligten Behörden in einem Verfahrensschritt blockiert, in dem weder die Speicherung der Daten erfolgt, noch verfahrensrechtliche Entscheidungen gegen die betroffene Person getroffen werden.

Die Sätze 1 und 2 gelten entsprechend für die Bestimmungen des Artikels 5 der Datenschutz-Grundverordnung, soweit diese den in den Sätzen 1 und 2 genannten Rechten und Pflichten nach der Datenschutz-Grundverordnung entsprechen.

Im Übrigen bleiben die Betroffenenrechte nach der Datenschutz-Grundverordnung sowie – für den Bereich der Richtlinie (EU) 2016/680 – nach den §§ 55 bis 61 BDSG (2018) unberührt.

### **Zu Nummer 8 (Änderung von § 22 EGGVG)**

Es handelt sich um redaktionelle Änderungen zur Anpassung an die Terminologie der Datenschutz-Grundverordnung. Soweit in Absatz 3 Satz 3 der Begriff der „Verwendung“ durch den Begriff der „Verarbeitung“ ersetzt, wird auf die Begründung zu den Nummern 1 bis 4 verwiesen.

### **Zu Artikel 3 (Änderung des Bundesverfassungsgerichtsgesetzes – BVerfGG)**

#### **Zu Nummer 1 (Änderung von § 35a BVerfGG)**

Bislang regelte § 35a BVerfGG die Geltung der Vorschriften „des Bundesdatenschutzgesetzes“. Für die Zulässigkeit der Verarbeitung von personenbezogenen Daten gelten ab dem 25. Mai 2018 die Vorschriften der Datenschutz-Grundverordnung unmittelbar in der gesamten Europäischen Union (Artikel 288 Absatz 2 AEUV). Daneben gelten weiterhin die ergänzenden nationalen allgemeinen Datenschutzvorschriften, in Deutschland also das BDSG. Dem trägt die Erweiterung der Bezugnahme auf „die allgemeinen datenschutzrechtlichen Vorschriften“ Rechnung. Wie bislang stellt § 35a des Bundesverfassungsgesetzes in der Entwurfsfassung (BVerfGG-E) damit klar, dass hinsichtlich der Verarbeitung personenbezogener Daten durch das Bundesverfassungsgericht die Regelungen des allgemeinen Datenschutzrechts gelten, soweit die nachfolgenden Regelungen nichts Abweichendes bestimmen.

#### **Zu Nummer 2 (Änderung von § 35b BVerfGG)**

§ 35b BVerfGG-E betrifft die Gewährung von Auskünften oder Akteneinsicht an Außenstehende und damit eine Übermittlung der in den Akten befindlichen Informationen für verfahrensfremde Zwecke (Bundestagsdrucksache 13/7673, S. 10).

In Absatz 1 Nummer 1 werden die Verweisungen auf das BDSG angepasst. Weil die bislang in Bezug genommenen Regelungen der Voraussetzung einer Zweckänderung in § 14 Absatz 2 Nummer 4, 6 bis 8 BDSG sich künftig – in zum Teil erweiterter Form – in § 23 Absatz 1 Nummer 2 und Nummer 4 bis 6 BDSG (2018) befinden, wird die Verweisung entsprechend umgestellt. Die bisherige Verweisung auf § 14 Absatz 2 Nummer 9 BDSG betrifft die Übermittlung zu wissenschaftlichen Zwecken. Da § 14 Absatz 2 Nummer 9 BDSG nicht in den künftigen § 23 Absatz 1 BDSG (2018) aufgenommen wurde, der bisherige Rechtszustand im BVerfGG aber gleichwohl beibehalten werden soll, wird anstelle der Verweisung die bislang in Bezug genommene Regelung des bisherigen § 14 Absatz 2 Nummer 9 BDSG in den Absatz 1 Nummer 1 übernommen.

Absatz 1 Nummer 2, der die Auskunftserteilung an Privatpersonen und andere nichtöffentliche Stellen regelt, lehnte sich in seiner bisherigen eigenständigen Formulierung der Voraussetzungen an die §§ 15 und 16 des bisherigen BDSG an. Stattdessen wird nun auf die entsprechende Regelung in § 25 Absatz 2 Nummer 2 des BDSG (2018) verwiesen. § 16 Absatz 3 des bisherigen BDSG ist jedoch im künftigen BDSG (2018) so nicht mehr enthalten. Soweit § 35 b Absatz 1 Nummer 2 Satz 2 bisher die Anwendung von § 16 Absatz 3 des bisherigen BDSG ausschließt, wird die sich bislang aus der Anordnung der Nichtgeltung des bisherigen § 16 Absatz 3 BDSG ergebende Regelung künftig eigenständig getroffen. Schon die bisherige Regelung war damit begründet worden, dass dem ohnehin bis an die Grenzen belasteten Bundesverfassungsgericht die mit der Unterrichtung des Betroffenen verbundene zusätzliche Arbeitsbelastung erspart werden muss. An der hohen Belastung des Bundesverfassungsgerichts hat sich nichts geändert. Es erscheint deshalb im Interesse der Funktionsfähigkeit des Bundesverfassungsgerichts erforderlich, im Ergebnis an der bisherigen Rechtslage festzuhalten.

### **Zu Nummer 3 (Änderung von § 35c BVerfGG)**

Die Ersetzung des Wortes „nutzen“ durch „verarbeiten“ dient der Anpassung an die datenschutzrechtliche Begrifflichkeit. Eine sachliche Änderung der Rechtslage erfolgt nicht.

### **Zu Artikel 4 (Änderung der Vorsorgeregister-Verordnung – VRegV)**

Wegen Wegfalls des bisherigen § 10 BDSG ist § 6 Absatz 1 Satz 1 der VRegV entsprechend anzupassen und der Verweis auf § 10 BDSG zu streichen. Weder die Datenschutz-Grundverordnung noch das DSAnpUG-EU enthalten Regelungen für die Einrichtung automatisierter Abrufverfahren. Grundsätzlich gelten deshalb die allgemeinen Vorschriften der Datenschutz-Grundverordnung für Abrufverfahren, insbesondere die Artikel 24 bis 26, 32 und 35. Die Aufnahme oder der Erhalt von Regelungen zum automatisierten Abrufverfahren für den öffentlichen Bereich kann zudem auf Artikel 6 Absatz 3 der Datenschutz-Grundverordnung gestützt werden. Die Führung des Zentralen Vorsorgeregisters durch die Bundesnotarkammer ist nach der Datenschutz-Grundverordnung dem öffentlichen Bereich zuzuordnen, da diese Aufgabe im öffentlichen Interesse liegt.

Um die Fortgeltung der schriftlichen Festlegungen mit den Landesjustizverwaltungen auf Grund der bislang geltenden Regelung in § 6 Absatz 1 Satz 1 VRegV zu erhalten, wird lediglich die Verweisung auf § 10 Absatz 2 BDSG durch eine allgemeine Bezugnahme auf die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit ersetzt. So soll auch weiterhin der Schutz der personenbezogenen Daten der Betroffenen sowie der Datensicherheit gewährleistet werden.

### **Zu Artikel 5 (Änderung der Testamentsregister-Verordnung – ZTRV)**

#### **Zu Nummer 1 (Änderung von § 8 Absatz 4 ZTRV)**

Es handelt sich um eine Änderung infolge der Neufassung des BDSG durch das DSAnpUG-EU. Die datenschutzrechtlichen Vorgaben für das Auskunftsrecht des Erblassers aus dem Zentralen Testamentsregister ergeben sich nunmehr unmittelbar aus dem Auskunftsrecht der betroffenen Person nach Artikel 15 der Datenschutz-Grundverordnung.

#### **Zu Nummer 2 (Änderung von § 12 ZTRV)**

##### **Zu Buchstabe a**

Der bisherige § 12 Absatz 1 der ZTRV wird aufgehoben, da die Regelungen der Datenschutz-Grundverordnung unmittelbar gelten. Ein Verweis auf die Datenschutz-Grundverordnung hätte rein deklaratorischen Charakter. Da die Registerbehörde auch künftig bei der Wahrnehmung ihrer Tätigkeiten grundsätzlich die Bestimmungen der Da-

tenschutz-Grundverordnung und des BDSG (2018) zu beachten hat, tritt keine Absenkung des derzeitigen Datenschutzniveaus ein.

#### **Zu Buchstabe b**

Buchstabe b) ist eine Folgeänderung zu Buchstabe a).

#### **Zu Buchstabe c**

Die Änderung ist sowohl eine Folgeänderung zum DSAnpUG-EU als auch Folge der Streichung des bisherigen Absatzes 1. Auch in § 12 Absatz 3 ZTRV bedarf es keines deklaratorischen Verweises auf die Datenschutz-Grundverordnung, da diese unmittelbar gilt. Ein allgemeiner Verweis auf Datenschutz und -sicherheit ist ausreichend.

#### **Zu Artikel 6 (Änderung der Rechtsanwaltsverzeichnis- und -postfachverordnung)**

Es handelt sich um eine Anpassung der Begrifflichkeiten an die Definition in Artikel 4 Nummer 7 der Datenschutz-Grundverordnung.

#### **Zu Artikel 7 (Änderung der Rechtsdienstleistungsverordnung – RDV)**

Die in § 9 Absatz 2 Satz 2 der RDV bisher enthaltene Verweisung auf § 10 Absatz 2 und 4 BDSG wird mit der am 25. Mai 2018 in Kraft getretenen Neufassung des BDSG durch das DSAnpUG-EU inhaltlich gegenstandslos, da § 10 BDSG (2018) dann einen völlig anderen Gegenstand regelt. Das BDSG (2018) enthält auch an keiner anderen Stelle eine dem § 10 Absatz 2 und 4 BDSG entsprechende Regelung zu automatisierten Abrufverfahren mehr. Soweit die Gegenstände der bisherigen Verweisungen daher für den Anwendungsbereich der RDV noch regelungsbedürftig sind, muss dies zukünftig unmittelbar in der RDV erfolgen. Im Ergebnis erscheint dies jedoch nur in Bezug auf die bisherige Verweisung auf § 10 Absatz 4 Satz 1 BDSG der Fall, weshalb deren Gegenstand zukünftig in § 9 Absatz 2 Satz 2 der Rechtsdienstleistungsverordnung in der Entwurfsfassung (RDV-E) selbst geregelt werden soll. Im Übrigen können die Verweisungen entfallen.

Denn zum einen werden die Inhalte der bisherigen Verweisung auf § 10 Absatz 2 BDSG zukünftig im Wesentlichen unmittelbar in der Datenschutz-Grundverordnung selbst geregelt, so dass es keiner Spezialregelung im nationalen Recht mehr bedarf. Dabei wird der Gegenstand des bisherigen § 10 Absatz 2 Satz 2 Nummer 1 BDSG dann durch Artikel 30 Absatz 1 Buchstabe b Datenschutz-Grundverordnung abgebildet. Der Inhalt von § 10 Absatz 2 Satz 2 Nummer 2 BDSG findet sich in vergleichbarer Form in Artikel 30 Absatz 1 Buchstabe d Datenschutz-Grundverordnung, derjenige des § 10 Absatz 2 Satz 2 Nummer 3 BDSG in Artikel 30 Absatz 1 Buchstabe c Datenschutz-Grundverordnung und derjenige des § 10 Absatz 2 Satz 2 Nummer 4 in Verbindung mit § 9 BDSG in Artikel 30 Absatz 1 Buchstabe g in Verbindung mit Artikel 32 Absatz 1 Datenschutz-Grundverordnung.

Zum anderen erscheint die bisher durch die Verweisung auf § 10 Absatz 4 Satz 2 bis 4 BDSG vorgeschriebene stichprobenartige Kontrolle der Abrufe auch durch die speichernde Stelle nicht mehr erforderlich. Denn zunächst werden diese Daten nach § 9 Absatz 2 Satz 1 RDV ohnehin nur einem sehr begrenzten Kreis von Behörden und keinen außenstehenden Dritten zugänglich gemacht. Diese Behörden haben zudem nach dem neuen § 9 Absatz 2 Satz 2 RDV-E die Verantwortung für die Zulässigkeit des Abrufs und diese daher durch geeignete Maßnahmen zu kontrollieren. Eine darüber hinausgehende weitere Kontrolle auch durch die speichernde Stelle erscheint dabei auch deshalb nicht erforderlich, weil es sich nicht um besonders sensible Daten handelt. Denn diese betreffen lediglich die frühere berufliche Tätigkeit der Personen und waren zudem bereits für die Öffentlichkeit einsehbar, bevor sie noch für einen begrenzten Zeitraum in das besondere Dateisystem nach § 18 Absatz 1 Satz 2 des Rechtsdienstleistungsgesetzes überführt wurden.

## **Zu Artikel 8 (Änderung der Zivilprozessordnung – ZPO)**

### **Zu Nummer 1 (Änderung der Inhaltsangabe zu § 882h ZPO)**

Die Änderung der Inhaltsübersicht spiegelt die Einfügung des neuen § 882i ZPO wider.

### **Zu Nummer 2 (Änderung von § 755 Absatz 3 ZPO)**

Die Änderung erfolgt zum Zwecke der Anpassung an die Terminologie der Datenschutz-Grundverordnung. Der Gerichtsvollzieher darf die Daten zur Durchführung des Zwangsvollstreckungsverfahrens eines weiteren Gläubigers unter den bereits bislang bestimmten Voraussetzungen verarbeiten, mithin sich ihrer auch in dem Verfahren eines weiteren Gläubigers bedienen. Darüber hinausgehende Befugnisse – etwa zur Speicherung der Daten durch den Gerichtsvollzieher – werden damit nicht eingeführt.

### **Zu Nummer 3 (Änderung von § 802d Absatz 1 Satz 3)**

Mit der Änderung soll eine Anpassung an die Terminologie der Datenschutz-Grundverordnung herbeigeführt werden. Eine Erweiterung der Befugnisse des Gläubigers ist damit nicht verbunden.

### **Zu Nummer 4 (Änderung von § 802k ZPO)**

#### **Zu Buchstabe a**

Die Änderung des § 802k Absatz 3 Satz 3 der ZPO ist eine Folge der Einführung der Datenschutz-Grundverordnung, die unmittelbar anwendbare Regelungen des materiellen Datenschutzrechts enthält und somit Pflichten für die Abdruckempfänger begründet. Für den Umfang der Pflichten der Betroffenen ist es unerheblich, ob diese unmittelbar auf europäischen Rechtsakten oder Vorschriften des Bundes- oder Landesrechts beruhen. Daher soll der Verweis auf die jeweiligen datenschutzrechtlichen Bestimmungen des Bundes und der Länder im Sinne einer einheitlichen Terminologie durch einen allgemeinen Verweis auf die anwendbaren datenschutzrechtlichen Vorschriften ersetzt werden. Dabei ist auch zu berücksichtigen, dass der Verweis auf die zu beachtenden datenschutzrechtlichen Vorschriften sich nicht nur auf die Datenschutz-Grundverordnung bezieht, sondern auch auf mögliche datenschutzrechtliche Vorschriften des Bundes und der Länder zur Auftragsverarbeitung in diesem Bereich (vgl. Artikel 28 Absatz 3 DS-GVO).

#### **Zu Buchstabe b**

Der neu eingefügte § 802k Absatz 5 ZPO trifft ergänzende Regelungen betreffend die Geltendmachung des Rechts der betroffenen Person auf Auskunft über die Verarbeitung ihrer personenbezogener Daten gemäß Artikel 15 Absatz 1 der Datenschutz-Grundverordnung und ihres Widerspruchsrechts gegen die Verarbeitung ihrer personenbezogenen Daten gemäß Artikel 21 der Datenschutz-Grundverordnung.

Nach § 802f Absatz 6 ZPO hat der Gerichtsvollzieher das von ihm auf Grund der Vermögensauskunft des Schuldners als elektronisches Dokument errichtete Vermögensverzeichnis bei dem für das jeweilige Land zuständigen zentralen Vollstreckungsgericht zu hinterlegen. Das Vermögensverzeichnis enthält die in § 802c Absatz 1 und 2 ZPO aufgeführten Angaben und somit umfassende Daten zu persönlichen Umständen und pfändbarem Vermögen des Schuldners. Es stellt eine maßgebliche Grundlage für die Entscheidung des Gläubigers darüber dar, welche weiteren Schritte bei der Vollstreckung sinnvoll sind. Es ist nach § 802d Absatz 1 Satz 2 ZPO in den Fällen, in denen zu einem späteren Zeitpunkt ein weiterer Gläubiger den Antrag auf Abgabe der Vermögensauskunft stellt, durch den zuständigen Gerichtsvollzieher bei dem zentralen Vollstreckungsgericht abzurufen; ein Ausdruck davon ist an den weiteren Gläubiger zu leiten. Das erstellte Vermö-

gensverzeichnis ist somit sowohl im ursprünglichen als auch in späteren Vollstreckungsverfahren ein zentraler Faktor.

Diese wichtigen im öffentlichen Interesse an einem effizienten Vollstreckungsverfahren liegenden Funktionen und der Schutz von laufenden Vollstreckungsverfahren machen es erforderlich, den Umfang des Auskunftsrecht nach Artikel 15 Absatz 1 der Datenschutz-Grundverordnung in Bezug auf personenbezogene Daten in den hinterlegten Vermögensverzeichnissen nach Artikel 23 der Datenschutz-Grundverordnung zu beschränken. Die im § 802k Absatz 5 einzufügende Regelung stützt sich dabei auf die Buchstaben e und j des Artikels 23 Absatz 1 der Datenschutz-Grundverordnung.

Nach Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung können die Pflichten und Rechte dann beschränkt werden, wenn dies für den Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses eine notwendige und verhältnismäßige Maßnahme ist. Die Funktionalität der Vermögensverzeichnisse verlangt die vorgenommenen Beschränkungen.

Nach Artikel 23 Absatz 1 Buchstabe j der Datenschutz-Grundverordnung können Einschränkungen zudem zur Durchsetzung zivilrechtlicher Ansprüche erfolgen. Hierzu gehört auch die Durchsetzung von Ansprüchen, die unter Inanspruchnahme von hoheitlicher Hilfe im gesetzlich ausgestalteten Verfahren der Zwangsvollstreckung erfolgt. Die zentrale Verwaltung der Vermögensverzeichnisse bei den zentralen Vollstreckungsgerichten und ihre Abrufbarkeit durch Gerichtsvollzieher auf Antrag eines weiteren Gläubigers ist ein wesentlicher Aspekt des geltenden Vollstreckungsverfahrens nach der ZPO. Da die Einsichtnahme durch berechtigte Stellen der Durchführung von deren Vollstreckungsverfahren, insbesondere dem Schutz auch künftiger Vollstreckungsverfahren dient, ist insoweit eine beschränkende Regelung erforderlich.

Diese Regelung achtet den Wesensgehalt der Grundrechte und Grundfreiheiten und stellt eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme im Sinne des Artikels 23 Absatz 1 der Datenschutz-Grundverordnung dar. Bei einer Abwägung zwischen der betroffenen grundrechtlichen Position des Einzelnen hinsichtlich des Schutzes seiner personenbezogenen Daten und dem Interesse der Allgemeinheit an einem effizienten Vollstreckungsverfahren, überwiegt das Interesse der Allgemeinheit; zu diesem gehört insbesondere die Möglichkeit für weitere Gläubiger, über einen beauftragten Gerichtsvollzieher Einsicht in ein hinterlegtes Vermögensverzeichnis zu erhalten und sich so vor weiteren Vollstreckungsmaßnahmen ein umfassendes und zutreffendes Bild über die der Zwangsvollstreckung unterliegenden Vermögensgegenstände des Schuldners zu machen, ohne wiederum die Effektivität dieser Vollstreckungsmaßnahmen zu gefährden. Ferner ist zu berücksichtigen, dass die Erhebung der Daten durch den das Vermögensverzeichnis erstellenden Gerichtsvollzieher ausschließlich beim Schuldner selbst erfolgt und dabei bereits der Grundsatz der Datensparsamkeit beachtet wird. In die Vermögensverzeichnisse werden Daten nur in dem in § 802c Absatz 1 und 2 ZPO genau beschriebenen Umfang aufgenommen. Besondere Kategorien personenbezogener Daten sind somit von der Beschränkung nicht betroffen.

§ 802k Absatz 5 Satz 1 ZPO trifft eine Regelung für die Fälle, in denen eine betroffene Person ihr Auskunftsrecht nach Artikel 15 Absatz 1 der Datenschutz-Grundverordnung in Bezug auf die zentral verwalteten Vermögensverzeichnisse geltend macht; dies gilt für die nach Artikel 15 Absatz 1 Buchstabe c der Datenschutz-Grundverordnung vorgesehene Mitteilung der Empfänger oder Kategorien von Empfängern, gegenüber denen personenbezogene Daten offengelegt worden sind oder noch werden. Insoweit sind lediglich die Kategorien von Empfängern zu bezeichnen, denen Vermögensverzeichnisse übermittelt werden dürfen; dieser eng begrenzte Kreis ist in § 802k Absatz 2 ZPO näher bestimmt und umfasst vornehmlich Gerichtsvollzieher; daneben auch andere nach Bundes- oder Landesrecht zur Abnahme einer Vermögensauskunft befugte Behörden sowie Gerichte und Strafverfolgungsbehörden. Es ist nicht erforderlich, dass die einzelnen berechtigten



Personen oder Stellen, die die betroffenen Vermögensverzeichnisse im Einzelfall abgerufen haben, mitgeteilt werden. Hierdurch wird namentlich in Fällen des § 802d ZPO, in denen ein Gerichtsvollzieher auf Antrag eines weiteren Gläubigers ein hinterlegtes Vermögensverzeichnis abrufen, das Vollstreckungsverfahren geschützt; wenn der Schuldner über sein Auskunftsrecht nach Artikel 15 der Datenschutz-Grundverordnung vor der verfahrensrechtlich bestimmten Information (§ 802d Absatz 1 Satz 4 ZPO) Kenntnis vom Abruf des Vermögensverzeichnisses erlangen würde, könnte möglicherweise eine Gefährdung von Vollstreckungsmaßnahmen dieses Gläubigers, eintreten. Dies gilt auch für den Schutz von Einsichtnahmen anderer Stellen in das Vermögensverzeichnis, insbesondere dort, wo diese Stellen ohne vorherige Kenntnis des Schuldners Ermittlungsmaßnahmen durchführen dürfen.

§ 802k Absatz 5 Satz 2 ZPO regelt die Fälle der Ausübung des Widerspruchsrechts gemäß Artikel 21 der Datenschutz-Grundverordnung, das zu einer Einschränkung der Verarbeitung führen könnte. Das allgemeine öffentliche Interesse erfordert zur Sicherstellung der Informationsmöglichkeiten für weitere Gläubiger den Ausschluss des Widerspruchsrechts. Kern der Funktion des abgegebenen Vermögensverzeichnisses ist es, auch für weitere Vollstreckungsverfahren zur Verfügung zu stehen. Die Zuleitung des Abdrucks eines abgegebenen Vermögensverzeichnisses an einen weiteren Gläubiger ersetzt nach § 802d Absatz 1 Satz 2 ZPO die erneute Abgabe der Vermögensauskunft; hierdurch wird vor allem im Interesse des Schuldners dieser grundsätzlich für einen Zeitraum von zwei Jahren der Pflicht enthoben, für jeden weiteren Gläubiger neue Vermögensauskünfte abzugeben. Für diese Funktion der abgegebenen Vermögensverzeichnisse ist erforderlich, dass diese auch für weitere Vollstreckungsverfahren während des Speicherzeitraums für Einsicht und Abruf zur Verfügung stehen. Wenn schon bei Ausübung des Widerspruchsrechts der betroffenen Person das abgegebene Vermögensverzeichnis zunächst über einen längeren Zeitraum nicht verarbeitet werden könnte und daher nicht einsehbar wäre, wäre diese wesentliche Funktionalität gefährdet und würde weiteren Gläubigern die Möglichkeit vorenthalten, sich ein Bild über die Vermögenslage des Schuldners zu machen.

Weitere Regelungen zu Betroffenenrechten nach der Datenschutz-Grundverordnung erfolgen im Hinblick auf die von den zentralen Vollstreckungsgerichten verwalteten Vermögensverzeichnisse nicht. Diese Rechte sind jedoch teilweise schon auf Grund der Regelungen der Datenschutz-Grundverordnung selbst hinsichtlich der in den verwalteten Vermögensverzeichnissen enthaltenen personenbezogenen Daten nicht anwendbar.

#### **Zu Nummer 5 (Änderung von § 802l ZPO)**

Die Änderung des § 802l Absatz 2 Satz 1 ZPO ist eine Folge des durch die Datenschutz-Grundverordnung eingeführten europarechtlich einheitlichen Begriffs der datenschutzrechtlichen Einschränkung der Verarbeitung von Daten, der dem bisherigen Begriff der Sperrung entspricht.

#### **Zu Nummer 6 (Änderung von § 850k Absatz 8 ZPO)**

Die Änderung des § 850k Absatz 8 Satz 5 ZPO ist eine Folge des durch die Datenschutz-Grundverordnung eingeführten europarechtlich einheitlichen Begriffs der datenschutzrechtlichen Verarbeitung, der die bisherigen Begriffe der Erhebung, Verarbeitung und Nutzung umfasst.

#### **Zu Nummer 7 (Änderung von § 882f Absatz 1 Satz 2 ZPO)**

Die Änderung erfolgt zur Anpassung an die Terminologie der Datenschutz-Grundverordnung. Eine Befugnisenerweiterung ist damit nicht verbunden.

### **Zu Nummer 8 (Änderung von § 882g Absatz 7 ZPO)**

Die Änderung des § 882g Absatz 7 Satz 1 ZPO passt die Norm ohne Änderung in der Sache an das BDSG (2018) an. Regelungen über die Aufsichtsbehörden der Länder für die Datenverarbeitungen durch nichtöffentliche Stellen finden sich nun in § 40 BDSG (2018). Durch die Norm soll weiterhin sichergestellt sein, dass nichtöffentliche Empfänger von Abdrucken aus dem Schuldnerverzeichnis und die nichtöffentliche Stellen, die von Abdruckempfängern Auskünfte erhalten, auch bei der Verarbeitung und Nutzung dieser personenbezogenen Daten in oder aus Akten der Aufsicht durch die Datenschutzaufsichtsbehörden unterliegen. Weitergehende Änderungen – insbesondere mit Blick auf den weiterhin verwandten Aktenbegriff, dem bereits derzeit keine besondere praktische Bedeutung zukommt - sind nicht veranlasst.

### **Zu Nummer 9 (Änderung von § 882h Absatz 3 ZPO)**

Die Änderung des § 882h Absatz 3 ZPO ist eine Folge des durch die Datenschutz-Grundverordnung eingeführten europarechtlich einheitlichen Begriffs der datenschutzrechtlichen Verarbeitung. Zur Klarstellung wird die Norm dieser Terminologie angepasst.

### **Zu Nummer 10 (Einfügung von § 882 i ZPO)**

Mit der Einfügung von § 882i ZPO wird hinsichtlich des Schuldnerverzeichnisses von der Möglichkeit nach Artikel 23 der Datenschutz-Grundverordnung Gebrauch gemacht, wonach die Pflichten und Rechte gemäß den Artikeln 12 bis 22 im Wege von Gesetzgebungsmaßnahmen beschränkt werden können, sofern dies der Sicherstellung eines der in Artikel 23 Absatz 1 Buchstabe a bis j der Datenschutz-Grundverordnung genannten Schutzzwecke dient. Die im einzufügenden § 882i ZPO enthaltenen Regelungen stützen sich dabei sowohl auf Artikel 23 Absatz 1 Buchstabe e als auch auf Artikel 23 Absatz 1 Buchstabe j der Datenschutz-Grundverordnung.

Nach Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung können die Pflichten und Rechte dann beschränkt werden, wenn dies für den Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses eine notwendige und verhältnismäßige Maßnahme ist. Die Funktionalität des Schuldnerverzeichnisses verlangt die vorgenommenen Beschränkungen.

Das Schuldnerverzeichnis ist durch das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung umgestaltet und den Bedürfnissen des modernen Rechtsverkehrs und Wirtschaftslebens angepasst worden. Es erfüllt eine Warn- und Informationsfunktion zugunsten des Rechtsverkehrs in Bezug auf kreditunwürdige Schuldner (vgl. Bundestagsdrucksache 16/10069, S. 55). Vor dem Hintergrund der Freizügigkeit innerhalb der Europäischen Union ist zum Schutz des Rechtsverkehrs eine zumindest bundesweite Recherchemöglichkeit über die Kreditwürdigkeit von Schuldnern erforderlich. Das Schuldnerverzeichnis, wie es durch die §§ 882b ff. ZPO ausgestaltet worden ist, ist somit in seiner jetzigen Funktionalität und Transparenz eine für die Sicherheit und Leichtigkeit des Rechtsverkehrs unerlässliche Einrichtung.

Auch Erwägungsgrund 73 der Datenschutz-Grundverordnung nennt im Zusammenhang mit möglichen Beschränkungen ausdrücklich das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses.

Nach Artikel 23 Absatz 1 Buchstabe j der Datenschutz-Grundverordnung können Einschränkungen im Übrigen zur Durchsetzung zivilrechtlicher Ansprüche erfolgen. Hierzu gehört auch die Durchsetzung von Ansprüchen, die unter Inanspruchnahme von hoheitlicher Hilfe im gesetzlich näher ausgestalteten Verfahren der Zwangsvollstreckung erfolgt. Die Anordnung der Eintragung eines kreditunwürdigen Schuldners in das Schuldnerverzeichnis unter den in § 882c Absatz 1 ZPO genannten Voraussetzungen ist Teil des Voll-

streckungsverfahrens (§ 882c Absatz 1 Satz 2 ZPO). Die Führung des Schuldnerverzeichnisses stellt ein amtliches Folgeverfahren zu einem Vollstreckungsverfahren dar, das nicht zuletzt im Interesse von weiteren Gläubigern die Durchsetzung von deren Ansprüchen erleichtert.

Die vorgesehenen Beschränkungen achten den Wesensgehalt der Grundrechte und Grundfreiheiten und stellen eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme im Sinne des Artikels 23 Absatz 1 der Datenschutz-Grundverordnung dar. Bei einer Abwägung zwischen der betroffenen grundrechtlichen Position des Einzelnen auf Schutz seiner personenbezogenen Daten und dem Interesse der Allgemeinheit an einem sicheren und erleichterten Rechtsverkehr durch den Schutz vor kreditunwürdigen Schuldnern überwiegt letzteres. Dabei ist zu berücksichtigen, dass bereits bei der Erhebung der Daten der Grundsatz der Datensparsamkeit beachtet wird. Personenbezogene Daten für das Schuldnerverzeichnis werden nur in dem in § 882b Absatz 2 und 3 ZPO genau beschriebenen Umfang erhoben, insbesondere zur sicheren Identifizierung der eingetragenen Person. Die erhobenen personenbezogenen Daten sind auf die Angabe des Namens, des Geburtsdatums und -ortes und der Wohnsitze des Schuldners beschränkt. Besondere Kategorien personenbezogener Daten sind somit von der Beschränkung nicht betroffen.

Einige weitere Ansprüche aus der Datenschutz-Grundverordnung bestehen bezüglich des Schuldnerverzeichnisses bereits auf Grund der in der Datenschutz-Grundverordnung selbst vorgesehenen Ausnahmen nicht:

Eine Informationspflicht der mit dem Schuldnerverzeichnis befassten Stellen nach Artikel 14 Absatz 1 bis 4 der Datenschutz-Grundverordnung ist bereits gemäß Artikel 14 Absatz 5 Buchstabe c ausgeschlossen, da die Erlangung und Offenlegung durch Rechtsvorschriften ausdrücklich geregelt ist, die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen.

Eine Ausnahme von Artikel 17 der Datenschutz-Grundverordnung (Recht auf Löschung) ist nicht erforderlich, weil im Schuldnerverzeichnis personenbezogene Daten zur Wahrnehmung einer Aufgabe im öffentlichen Interesse verarbeitet werden und sich daher der Verantwortliche auf die Ausnahmeregelung gemäß Artikel 17 Absatz 3 Buchstabe b der Datenschutz-Grundverordnung berufen kann.

Eine Ausnahme vom Anspruch auf Beschränkung der Verarbeitung gemäß Artikel 18 Absatz 1 der Datenschutz-Grundverordnung ist nicht erforderlich, weil die Verarbeitung personenbezogener Daten im Schuldnerverzeichnis ein wichtiges öffentliches Interesse darstellt (vgl. auch Erwägungsgrund 73 der Datenschutz-Grundverordnung) und das Recht auf Einschränkung der Verarbeitung insoweit gemäß Artikel 18 Absatz 2 der Datenschutz-Grundverordnung ausgeschlossen ist.

Eine Mitteilungspflicht der mit dem Schuldnerverzeichnis befassten Stellen aus Artikel 19 der Datenschutz-Grundverordnung ist bereits nach dessen Wortlaut ausgeschlossen, da dies mit einem unverhältnismäßigen Aufwand verbunden wäre. Die Unverhältnismäßigkeit beruht zum einen auf der Anzahl an verarbeiteten personenbezogenen Daten vor dem Hintergrund von etwa acht Millionen Eintragungen im Schuldnerverzeichnis. Darüber hinaus müssten zusätzlich personenbezogene Daten der Abrufenden und Abdruckempfänger über den Umfang hinaus, der in den Vorschriften zur Führung des Schuldnerverzeichnisses und dem Bezug von Abdrucken daraus vorgesehen ist, erfasst und gespeichert werden, um der Mitteilungspflicht nachzukommen. Dies wäre mit einem unverhältnismäßigen Eingriff in das Persönlichkeitsrecht der Empfänger und einem unverhältnismäßigen Verwaltungsaufwand verbunden.

Artikel 20 der Datenschutz-Grundverordnung (Recht der betroffenen Person auf Datenübertragbarkeit) findet auf die öffentlichen Register, zu denen auch das Schuldnerver-

zeichnis gehört, keine Anwendung, da die Verarbeitung gemäß Artikel 20 Absatz 3 Satz 2 der Datenschutz-Grundverordnung für die Wahrnehmung einer öffentlichen Aufgabe erforderlich ist.

### **Zu Absatz 1**

Die Erfüllung des Auskunftsrechts der betroffenen Person nach Artikel 15 Absatz 1 der Datenschutz-Grundverordnung wäre für die mit der Führung des Schuldnerverzeichnisses befassten zentralen Vollstreckungsgerichte mit einem unverhältnismäßigen Aufwand verbunden und meist auch nicht möglich. Denn das Schuldnerverzeichnis wird nach § 882h Absatz 1 Satz 1 ZPO dezentral geführt, nämlich für jedes Land durch das nach Landesrecht bestimmte zentrale Vollstreckungsgericht. Das Schuldnerverzeichnis stellt somit letztlich eine Zusammenfassung von Landesverzeichnissen dar, wobei jedes zentrale Vollstreckungsgericht nur für sein Verzeichnis mit den in dem jeweiligen Land eingeleiteten Daten verantwortlich ist. Demzufolge kann es zu durch andere zentrale Vollstreckungsgerichte eingetragene Personen keine Auskunft geben. Lediglich für die Einsichtnahme in die Eintragungen wird eine länderübergreifende Anfrage im Internet angeboten (§ 882h Absatz 1 Satz 2 ZPO). Diese Einsichtnahme im Internet, die die gleichzeitige und parallele Durchsuchung der von allen zentralen Vollstreckungsgerichten geführten Eintragungen erlaubt, stellt für die betroffene Person somit die einzige Möglichkeit dar, mit Sicherheit auf alle zu ihr im Schuldnerverzeichnis vorhandenen Informationen zuzugreifen.

§ 882f Satz 1 Nummer 6 ZPO und § 5 Nummer 6 der Schuldnerverzeichnisführungsverordnung (SchuFV) stellen sicher, dass jede betroffene Person zum Zweck der Auskunft über sie selbst betreffende Eintragungen ohne weitere materielle Voraussetzungen in das Schuldnerverzeichnis Einsicht nehmen darf.

Die in Artikel 15 Absatz 1 der Datenschutz-Grundverordnung genannten Informationen können den betroffenen Personen in allgemeiner Form, z. B. durch eine allgemeine Aufstellung auf dem gemeinsamen Vollstreckungsportal der Länder gegeben werden. Der betroffenen Person ist die Tatsache ihrer Eintragung in das Schuldnerverzeichnis im Übrigen bereits aufgrund des Umstandes bekannt, dass die Eintragungsanordnung ihr von Amts wegen zugestellt wurde (§ 882c Absatz 2 Satz 2 ZPO).

In Satz 2 wird – im Hinblick auf die Vielzahl der Abrufe aus dem Vollstreckungsportal – ausdrücklich klargestellt, dass eine Information über die einzelnen konkreten Empfänger der Daten nur insoweit erfolgen muss, als Daten zu diesen Empfängern nach den Vorschriften für Zwecke der Datenschutzkontrolle zu speichern sind. In § 6 Absatz 4 SchuFV und der Schuldnerverzeichnisabdruckverordnung (SchuVAbdrV) ist festgelegt, dass das über jeden Datenabruf erstellte Protokoll im Regelfall nach sechs Monaten gelöscht wird. Für personenbezogene Daten der Bezieher von Abdrucken zum laufenden Bezug aus dem Schuldnerverzeichnis bestimmt § 4 Absatz 3 der SchuVAbdrV eine maximale Speicherdauer von sechs Jahren. Diese Regelungen sind ihrerseits das Ergebnis einer Abwägung der datenschutzrechtlichen Interessen von in das Schuldnerverzeichnis eingetragenen Personen mit den Interessen von Personen, die berechtigterweise in das Schuldnerverzeichnis Einsicht nehmen oder Abdrucke erhalten – die Registrierungsdaten der Einsicht nehmenden Personen und der Abdruckempfänger stellen ebenfalls personenbezogene Daten dar. Dieser auf diese Weise bereits bestehende Interessenausgleich bleibt somit gewahrt.

### **Zu Absatz 2**

Das Recht der betroffenen Person auf Berichtigung nach Artikel 16 der Datenschutz-Grundverordnung wird dadurch beschränkt, dass die betroffene Person stattdessen auf das bestehende verfahrensrechtliche Änderungsverfahren nach § 882e Absatz 4 ZPO verwiesen wird. Aufgrund des streng formalisierten Charakters, den sowohl die Zwangsvollstreckung wie auch das ihr nachgelagerte Amtsverfahren der Führung des Schuldner-

verzeichnisses haben, muss sichergestellt sein, dass veröffentlichte Eintragungen im Schuldnerverzeichnis nur unter den formellen Voraussetzungen und in dem Verfahren, die § 882e Absatz 4 ZPO im Einzelnen vorgibt, geändert werden können. Dabei können nach § 882e Absatz 4 ZPO von Amts wegen oder auf Anregung auch der betroffenen Person solche Eintragungen geändert werden, deren Inhalt von Beginn an fehlerhaft war. In das Schuldnerverzeichnis sind die Schuldnerdaten einzutragen, die im Zeitpunkt der Eintragungsanordnung zutreffen. Spätere Änderungen in den personenbezogenen Daten der einzutragenden Person führen nicht zu einer Änderung des Eintrags im Schuldnerverzeichnis; eine fortlaufende Aktualisierung der Daten der eingetragenen Personen ist nicht vorgesehen. § 882i Absatz 2 ZPO-E bestimmt, dass eine solche laufende Aktualisierung auch nicht im Rahmen des datenschutzrechtlichen Rechts auf Berichtigung nach Artikel 16 der Datenschutz-Grundverordnung zu bewirken ist.

Die Rechte des von der Verarbeitung personenbezogener Daten Betroffenen werden neben der Löschungspflicht nach der Regelzeit von drei Jahren nach Eintragungsanordnung (§ 882e Absatz 1 ZPO) auch dadurch gewahrt, dass in Fällen des Nachweises der Befriedigung des Gläubigers und der Aufhebung der Eintragungsanordnung der Schuldner vorzeitig zu löschen ist (§ 882e Absatz 2 Nummer 1 und 3 ZPO). Fehlt der Eintragungsgrund von Anfang an oder fällt er später weg, erfolgt die Löschung durch das zentrale Vollstreckungsgericht von Amts wegen (§ 882e Absatz 3 Nummer 2 ZPO).

Im Übrigen sind Streitigkeiten über die Berechtigung der Eintragung oder den Wegfall des Eintragungsgrundes (etwa die Erfüllung der Forderung) grundsätzlich im Wege der bestehenden vollstreckungsrechtlichen Rechtsbehelfe – wie dem Widerspruch gegen die Eintragung oder der Vollstreckungsabwehrklage – auszutragen. Eine Klärung dieser Streitigkeiten im Rahmen eines Antrags auf Berichtigung gestützt auf Artikel 16 der Datenschutz-Grundverordnung wäre mit den Grundsätzen der Führung des Schuldnerverzeichnisses als Justizverwaltungsverfahren unvereinbar.

### **Zu Absatz 3**

Für im Schuldnerverzeichnis erfolgte Eintragungen gilt der Grundsatz der Erhaltung der Eintragung. Diese wird unter anderem dadurch geschützt, dass Eintragungen im Schuldnerverzeichnis nach Ablauf der Widerspruchsfrist gemäß § 882d Absatz 1 Satz 1 ZPO von Amts wegen erfolgen und auch der Widerspruch gegen die Eintragungsanordnung – vorbehaltlich einer abweichenden einstweiligen Anordnung des Vollstreckungsgerichts – die Eintragung nicht hemmt; nach Ablauf der Widerspruchsfrist sind Eintragungen nicht mit einer sofortigen Beschwerde anfechtbar. Der Grundsatz der Erhaltung der Eintragung macht es erforderlich, dass auch das Widerspruchsrecht gemäß Artikel 21 der Datenschutz-Grundverordnung, das zu einer Einschränkung der Verarbeitung führen könnte, bezüglich der im Schuldnerverzeichnis und in den Anordnungen der Eintragung in das Schuldnerverzeichnis enthaltenen personenbezogenen Daten ausgeschlossen ist. Das zwingende öffentliche Interesse an diesem Ausschluss ergibt sich aus der wesentlichen Funktion, die das Schuldnerverzeichnis für die Sicherheit des Rechtsverkehrs durch Information und Warnung vor kreditunwürdigen Schuldnern hat. Diese Funktion setzt indes die ständige Verfügbarkeit der jeweiligen Eintragungen und die Möglichkeit zur Einsicht für die Berechtigten voraus. Es würde dem Zweck der dem Schuldnerverzeichnis obliegenden Warn- und Informationsfunktion für den Rechtsverkehr widersprechen, wenn sogleich bei Ausübung des Widerspruchsrechts durch die betroffene Person die Eintragung eines Schuldners über einen längeren Zeitraum nicht mehr verarbeitet werden könnte und daher für die zur Einsichtnahme in das Schuldnerverzeichnis Berechtigten nicht einsehbar wäre.

### **Zu Nummer 11 (Änderung von § 947 Absatz 2 Satz 2 ZPO)**

Die Änderung des § 947 Absatz 2 Satz 2 ZPO ist eine Folge des durch die Datenschutz-Grundverordnung eingeführten europarechtlich einheitlichen Begriffs der datenschutz-

rechtlichen Einschränkung der Verarbeitung von Daten, der dem bisherigen Begriff der Sperrung entspricht.

### **Zu Artikel 9 (Änderung der Schuldnerverzeichnisführungsverordnung – SchuFV)**

#### **Zu Nummer 1 (Änderung von § 6 Absatz 4 Satz 2 SchuFV)**

Die Änderung des § 6 Absatz 4 Satz 2 der Schuldnerverzeichnisführungsverordnung (SchuFV) ersetzt in Anpassung den im BDSG (2018) nicht mehr verwendeten Begriff der Datenschutzkontrolle durch den der Datenschutzaufsicht.

#### **Zu Nummer 2 (Änderung von § 9 Absatz 1 Satz 1 SchuFV)**

Mit der Änderung soll eine Anpassung an die Terminologie der Datenschutz-Grundverordnung herbeigeführt werden. Eine Erweiterung der Befugnisse ist damit nicht verbunden.

#### **Zu Nummer 3 (Änderung von § 10 Absatz 4 Satz 4 SchuFV)**

Mit der Änderung der Absätze 1 und 2 SchuFV soll eine Anpassung an die Terminologie der Datenschutz-Grundverordnung herbeigeführt werden. Ebenso ist die Änderung des § 10 Absatz 4 Satz 4 SchuFV eine Folge des durch die Datenschutz-Grundverordnung eingeführten europarechtlich einheitlichen Begriffs der datenschutzrechtlichen Einschränkung der Verarbeitung von Daten, der dem bisherigen Begriff der Sperrung entspricht.

### **Zu Artikel 10 (Änderung der Schuldnerverzeichnisabdruckverordnung – SchuVAbdrV)**

#### **Zu Nummer 1 (Änderung von § 1 Absatz 3 SchuVAbdrV)**

Die Änderung des § 1 Absatz 3 SchuVAbdrV passt die bisher verwendete Terminologie an die europarechtlich einheitlichen Regelungen der Datenschutz-Grundverordnung an. Vor dem Hintergrund der dort gewählten Terminologie werden ohne inhaltliche Änderung sämtliche bisher im Einzelnen aufgeführten Verarbeitungsweisen einheitlich mit dem Begriff der Verarbeitung bezeichnet.

#### **Zu Buchstabe b (Änderung von § 4 Absatz 2 Satz 2 SchuVAbdrV)**

Die Streichung in Absatz 1 erfolgt zur Anpassung an die Terminologie der Datenschutz-Grundverordnung, da die Erhebung von Daten nunmehr eine Teilmenge des umfassenden Verarbeitungsbegriffs ist. Die Änderung des Absatz 2 Satz 2 ist eine Folge des durch die Datenschutz-Grundverordnung eingeführten europarechtlich einheitlichen Begriffs der datenschutzrechtlichen Verarbeitung, der die bisherigen Begriffe der Erhebung, Verarbeitung und Nutzung umfasst.

#### **Zu Nummer 3 (Änderung von § 6 Absatz 2 SchuVAbdrV)**

Die Änderung des § 6 Absatz 2 SchuVAbdrV ist eine Folge der Einführung der Datenschutz-Grundverordnung, die unmittelbar anwendbare Regelungen des materiellen Datenschutzrechts enthält und somit Pflichten für die Abdruckempfänger begründet. Für den Umfang der Pflichten der Betroffenen ist es unerheblich, ob diese unmittelbar auf europäischen Rechtsakten oder Vorschriften des Bundes- oder Landesrechts beruhen. Daher soll der Verweis auf die Datenschutzgesetze des Bundes und der Länder durch einen allgemeinen Verweis auf die anwendbaren datenschutzrechtlichen Vorschriften ersetzt werden.

#### **Zu Nummer 4 (Änderung von § 16 Absatz 2 Satz 2 SchuVAbdrV)**

Die Änderung des § 16 Absatz 2 Satz 2 Nummer 2 SchuVAbdrV ist eine Folge des durch die Datenschutz-Grundverordnung eingeführten europarechtlich einheitlichen Begriffs der datenschutzrechtlichen Verarbeitung, der die bisherigen Begriffe der Erhebung, Verarbeitung und Nutzung umfasst.

#### **Zu Nummer 5 (Änderung von § 17 Satz 1 SchuVAbdrV)**

Die Änderung zieht die sich aus der unmittelbaren Geltung der Datenschutz-Grundverordnung ergebenden Konsequenzen. Durch den Hinweis auf die Artikel 24, 25 und 32 DS-GVO wird die Pflicht zur Gewährleistung der technischen und organisatorischen Mittel unterstrichen.

#### **Zu Nummer 6 (Änderung von § 18 Absatz 1 Satz 1 SchuVAbdrV)**

Die Änderung des § 18 Absatz 1 Satz 1 SchuVAbdrV passt die bisher verwendete Terminologie an die europarechtlich einheitlichen Regelungen der Datenschutz-Grundverordnung an. Vor dem Hintergrund der dort gewählten Terminologie werden ohne inhaltliche Änderung die bisher im Einzelnen aufgeführten Verarbeitungsweisen einheitlich mit dem Begriff der Verarbeitung bezeichnet.

#### **Zu Artikel 11 (Änderung der Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters – ZStVBetrV)**

##### **Zu Nummer 1 (Änderung von § 5 ZStVBetrV)**

Es handelt sich um redaktionelle Anpassungen, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden sind.

##### **Zu Nummer 2 (Änderung von § 9 ZStVBetrV)**

Es handelt sich um redaktionelle Anpassungen, die im Zuge der Neuordnung des BDSG im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 notwendig geworden sind, und um eine inhaltliche Anpassung anlässlich der Aufhebung des bisher in § 495 Absatz 1 Satz 1 Halbsatz 2 StPO enthaltenen Verweises bzw. die Aufhebung der Regelungen des § 491 Absatz 1 Satz 2 bis 6 StPO. Auf die dortige Begründung wird verwiesen.

#### **Zu Artikel 12 (Änderung des Strafvollzugsgesetzes – StVollzG)**

##### **Zu Nummer 1 (Änderung der Inhaltsübersicht)**

##### **Zu Buchstabe a und Buchstabe b**

Die Änderungen in der Angabe zum Fünften Abschnitt und in der Angabe zum Fünften Titel des Fünften Abschnitts sollen den grundsätzlich auf den Vollzug der Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft nach § 171 StVollzG beschränkten Anwendungsbereich der Datenschutzregelungen verdeutlichen. Nachdem in allen Ländern landesrechtliche Regelungen zum Strafvollzug in Kraft getreten sind, finden die Datenschutzregelungen des Strafvollzugsgesetzes des Bundes grundsätzlich nur noch auf den Vollzug dieser sogenannten Zivilhaft nach § 171 StVollzG Anwendung.

##### **Zu den Buchstaben c bis g**

Die Überschriften sollen an die Terminologie der Datenschutz-Grundverordnung angepasst werden. Die neue Angabe zu § 181 StVollzG-E soll den Inhalt der Vorschrift konkreter bezeichnen.

## **Zu Buchstabe h**

Die Angabe ist anzupassen, da § 187 StVollzG aufgehoben werden soll.

## **Zu Nummer 2 (Änderung von § 86 StVollzG)**

Es handelt sich zum einen um redaktionelle Folgeänderungen zur Neufassung von § 180 Absatz 2 StVollzG-E. Der bisherige Verweis wird entsprechend angepasst und der Regelungsgehalt des derzeitigen § 180 Absatz 2 Nummer 4 StVollzG in die Vorschrift integriert. Zum anderen wird die Terminologie der Vorschrift an den durch die Datenschutz-Grundverordnung eingeführten europarechtlich einheitlichen Begriff der datenschutzrechtlichen Verarbeitung angepasst, der die bisherigen Begriffe der Erhebung, Verarbeitung und Nutzung umfasst.

## **Zu Nummer 3 (Änderung von § 130 StVollzG)**

Da alle Länder landesrechtliche Regelungen für den Vollzug der Sicherungsverwahrung geschaffen haben, findet das Datenschutzregime des Strafvollzugsgesetzes des Bundes hier keine Anwendung mehr. Der entsprechende Verweis kann daher gestrichen werden.

## **Zu Nummer 4 (Änderung der Überschrift des Fünften Abschnitts)**

Die Überschrift des Fünften Abschnitts soll an den grundsätzlich auf den Vollzug der Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft nach § 171 StVollzG beschränkten Anwendungsbereich der Datenschutzregelungen angepasst werden.

## **Zu Nummer 5 (Änderung von § 167 StVollzG)**

Es handelt sich um eine redaktionelle Folgeänderung. Diese ist erforderlich, da einige Länder die Fortgeltung der §§ 167 bis 170 StVollzG angeordnet haben. Da die §§ 179 bis 186 StVollzG-E keine Anwendung mehr auf den Vollzug der Freiheitsstrafe finden, sind die Vorschriften aus der Aufzählung der entsprechend anwendbaren Vorschriften über den Vollzug der Freiheitsstrafe auszunehmen und ist ihre Anwendbarkeit gesondert anzuordnen.

## **Zu Nummer 6 (Änderung von § 171 StVollzG)**

In § 179 Absatz 1 StVollzG-E und in § 180 Absatz 1 StVollzG-E soll ausdrücklich geregelt werden, dass die Erhebung und Verarbeitung personenbezogener Daten nach den dortigen Regelungen zulässig ist, soweit dies für den Vollzug der Haft nach § 171 StVollzG erforderlich ist. Da sich die Anwendbarkeit der Datenschutzregelungen daher aus diesen Normen direkt ergibt, kann die Anordnung ihrer entsprechenden Anwendbarkeit in § 171 StVollzG-E gestrichen werden.

## **Zu Nummer 7 (Änderung der Überschrift des Fünften Titels)**

Die Überschrift des Fünften Titels des Fünften Abschnitts soll an den grundsätzlich auf den Vollzug der Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft nach § 171 StVollzG beschränkten Anwendungsbereich der Datenschutzregelungen angepasst werden.

## **Zu Nummer 8 (Änderung von § 179 StVollzG)**

## **Zu Buchstabe a**

Nachdem in allen Ländern landesrechtliche Regelungen zum Strafvollzug in Kraft getreten sind, finden die Datenschutzregelungen des Strafvollzugsgesetzes des Bundes grund-



sätzlich nur noch auf den Vollzug der Ordnungs-, Sicherungs-, Zwangs- und Erzwingungshaft nach § 171 StVollzG Anwendung. Der Wortlaut des § 179 Absatz 1 StVollzG-E wird daher entsprechend angepasst.

### **Zu Buchstabe b**

Die Erhebung personenbezogener Daten ohne Mitwirkung der betroffenen Person oder bei anderen Personen oder Stellen richtete sich bisher durch die Verweisung in § 179 Absatz 2 StVollzG nach § 4 Absatz 2 und 3 und § 13 Absatz 1a BDSG a. F. Diese Vorschriften werden im BDSG (2018) nicht mehr enthalten sein. Ihre Vorgaben werden daher durch die Neufassung des § 179 Absatz 2 StVollzG-E und durch den neu eingefügten § 179 Absatz 2a StVollzG-E in das Strafvollzugsgesetz übernommen. Der bisherige Regelungsgehalt bleibt damit erhalten.

Soweit § 179 Absatz 2 StVollzG durch die Verweisung auf das BDSG a. F. bisher auch Vorgaben für die Hinweis- und Aufklärungspflichten enthalten hat, wird auf die Ausführungen zu § 179 Absatz 4 StPO-E (vgl. Nummer 8 Buchstabe d) verwiesen.

### **Zu Buchstabe c**

Es handelt sich um redaktionelle Änderungen aufgrund des auf den Vollzug der Haft nach § 171 StVollzG beschränkten Anwendungsbereichs der Vorschrift und um eine redaktionelle Änderung zur Anpassung der Vorschrift an die Terminologie der Datenschutz-Grundverordnung.

### **Zu Buchstabe d**

Die Informationspflichten bei der Erhebung persönlicher Daten richten sich zukünftig nach den Artikeln 13 und 14 der Datenschutz-Grundverordnung.

Artikel 23 der Datenschutz-Grundverordnung ermöglicht es, diese Rechte und Pflichten aus den Artikeln 13 und 14 der Verordnung im Wege von Gesetzgebungsmaßnahmen zu beschränken, sofern dies der Sicherstellung eines der in Artikel 23 Absatz 1 Buchstabe a bis j der Datenschutz-Grundverordnung genannten Schutzzwecke dient. Von dieser Möglichkeit soll mit § 179 Absatz 4 StVollzG-E Gebrauch gemacht werden.

Die in § 179 Absatz 4 StVollzG-E vorgenommenen Beschränkungen dienen dem Schutz von Gerichtsverfahren (Artikel 23 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung) und der Durchsetzung zivilrechtlicher Ansprüche (Artikel 23 Absatz 1 Buchstabe j der Datenschutz-Grundverordnung). Ordnungs-, Sicherungs-, Zwangs- oder Erzwingungshaft kann sowohl der Sicherung eines gerichtlichen Verfahrens, beispielsweise der Erzwingung einer Zeugenaussage, als auch der Durchsetzung zivilrechtlicher Ansprüche, beispielsweise der Sicherung einer gefährdeten Zwangsvollstreckung in das Vermögen des Schuldners, dienen.

Vor diesem Hintergrund ermöglicht § 179 Absatz 4 Nummer 1 StVollzG-E wie nach bisher geltender Rechtslage, bei der Erhebung personenbezogener Daten ohne Kenntnis der betroffenen Person von den Rechten und Pflichten nach Artikel 13 und 14 der Datenschutz-Grundverordnung abzuweichen, wenn ansonsten der Vollzug der Haft nach § 171 StVollzG gefährdet würde. Werden die personenbezogenen Daten bei anderen Personen oder Stellen erhoben, sind zunächst die Ausnahmeregelungen des Artikels 14 Absatz 5 der Datenschutz-Grundverordnung einschlägig. Diese beinhalten unter anderem die – auch nach bisheriger Rechtslage bestehende – Möglichkeit, von der Information der betroffenen Person abzusehen, wenn die Erteilung dieser Information einen unverhältnismäßigen Aufwand erfordern würde. Bei der Abwägung, ob es sich um einen unverhältnismäßigen Aufwand handeln würde, ist wie nach bisheriger Rechtslage zu berücksichtigen, ob der Aufwand der Unterrichtung außer Verhältnis zum Schutzzweck steht und kei-

ne Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Person beeinträchtigt werden. Darüber hinaus ermöglicht § 179 Absatz 4 Nummer 2 StVollzG-E wie nach bisheriger Rechtslage, von der Information der betroffenen Person abzusehen, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden berechtigten Interesses eines Dritten, geheim gehalten werden müssen.

Über diese abschließenden Sonderregelungen zu den Beschränkungen der Rechte und Pflichten nach Artikel 13 und 14 der Datenschutz-Grundverordnung hinaus gelten mit Blick auf die aus der Datenschutz-Grundverordnung folgenden Rechte der betroffenen Personen die einschlägigen Vorschriften des BDSG (2018). Beispielsweise ist bei der Prüfung eines Widerspruchsrechts der betroffenen Person nach Artikel 21 der Datenschutz-Grundverordnung § 36 BDSG (2018) zu beachten. Bei der Entscheidung über eine Mitteilungspflicht nach Artikel 34 der Datenschutz-Grundverordnung ist § 29 Absatz 1 BDSG (2018) zu berücksichtigen.

### **Zu Nummer 9 (Änderung von § 180 StVollzG)**

#### **Zu Buchstabe a**

Es handelt sich um eine redaktionelle Änderung zur Anpassung der Überschrift an den durch die Datenschutz-Grundverordnung eingeführten europarechtlich einheitlichen Begriff der datenschutzrechtlichen Verarbeitung.

#### **Zu Buchstabe b**

Es handelt sich um eine redaktionelle Änderung zur Anpassung der Terminologie der Vorschrift an die Datenschutz-Grundverordnung und um eine Änderung zur Anpassung der Vorschrift an ihren auf den Vollzug der Haft nach § 171 StVollzG beschränkten Anwendungsbereich.

#### **Zu Buchstabe c**

§ 180 Absatz 2 StVollzG enthielt bisher eine Aufzählung der Zwecke, zu denen eine Weiterverarbeitung personenbezogener Daten zulässig war. Diese Aufzählung soll zugunsten einer Verweisung auf § 23 BDSG (2018) in § 180 Absatz 2 StVollzG-E aufgehoben werden. § 23 Absatz 1 BDSG (2018) regelt die Voraussetzungen, unter denen die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung zulässig ist. Diese Voraussetzungen entsprechen weitgehend den bisher in § 180 Absatz 2 StVollzG enthaltenen Vorgaben.

Mit Blick auf die Weiterverarbeitung personenbezogener Daten ist zu berücksichtigen, dass Artikel 13 Absatz 3 und Artikel 14 Absatz 4 der Datenschutz-Grundverordnung die Pflicht statuieren, den Betroffenen von der Absicht zu unterrichten, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die Daten erhoben wurden. Diese mit der Datenschutz-Grundverordnung erstmals eingeführte (Folge)Informationspflicht des Verantwortlichen bei beabsichtigter Zweckänderung fand bisher in den Datenschutzregelungen des Strafvollzugsgesetzes und im BDSG a. F. keine Entsprechung. Der Verpflichtung kann jedoch im Rahmen des Vollzugs von Haft nach § 171 StVollzG in der Form Rechnung getragen werden, dass die Information etwa im Rahmen der Belehrung bei Haftantritt bzw. bei der Erhebung der Daten in genereller Form erteilt wird. Eine Weiterverarbeitung personenbezogener Daten ist nach § 180 Absatz 2 StVollzG-E nur unter den engen Voraussetzungen des § 23 des Bundesdatenschutzgesetzes statthaft. Die Voraussetzungen für eine mögliche Weiterverarbeitung stehen daher bereits bei Erhebung der Daten fest, so dass eine Information der betroffenen Person bereits bei Haftantritt bzw. bei Erhebung der personenbezogenen Daten möglich ist.

#### **Zu Buchstabe d**

§ 180 Absatz 3 StVollzG ermöglichte bisher die Verarbeitung personenbezogener Daten für die Zwecke des gerichtlichen Rechtsschutzes nach den §§ 109 bis 121 StVollzG sowie für die in § 14 Absatz 3 BDSG a. F. genannten Zwecke. Diese Vorschrift kann aufgehoben werden. Die Verarbeitung der personenbezogenen Daten einer betroffenen Person für die Zwecke des Rechtsschutzes nach den §§ 109 bis 121 ist von § 23 Absatz 1 Nummer 1 BDSG (2018) umfasst, nach dem die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung zulässig ist, wenn offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde. § 14 Absatz 3 BDSG a. F. wurde in § 23 Absatz 1 Nummer 6 BDSG (2018) aufgenommen, auf den § 180 Absatz 2 StVollzG-E verweist.

#### **Zu Buchstabe e**

Die Vorschrift benennt über die in § 180 Absatz 1 StVollzG-E und § 23 des Bundesdatenschutzgesetzes genannten Voraussetzungen hinaus weitere Fälle, in denen die zuständigen öffentlichen Stellen personenbezogene Daten übermitteln können. Aus dieser Aufzählung können Nummer 1 und Nummer 2 gestrichen werden, da ihnen beim Vollzug von Haft nach § 171 StVollzG kein Anwendungsbereich zukommt. Nummer 5 kann gestrichen werden, da die Regelung bereits von § 23 Absatz 1 Nummer 1 BDSG (2018) erfasst ist.

Auch die Übermittlung personenbezogener Daten nach den Vorgaben dieses Absatzes löst die (Folge)Informationspflicht nach Artikel 13 Absatz 3 und Artikel 14 Absatz 4 Datenschutz-Grundverordnung aus (vgl. hierzu die Ausführungen zu § 180 Absatz 2 StVollzG-E unter Nummer 9 Buchstabe c). Auch diese Information kann der betroffenen Person aber in genereller Form erteilt werden, etwa im Rahmen der Belehrung bei Haftantritt bzw. bei der Erhebung der personenbezogenen Daten.

#### **Zu Buchstabe f**

Die Sätze 2 bis 4 der Vorschrift betreffen die Erteilung von Auskünften an den Verletzten einer Straftat. Aufgrund des auf den Vollzug der Haft nach § 171 StVollzG beschränkten Anwendungsbereichs der Vorschrift können diese Sätze aufgehoben werden.

#### **Zu Buchstabe g**

Es handelt sich um Folgeänderungen aufgrund des auf den Vollzug der Haft nach § 171 StVollzG beschränkten Anwendungsbereichs der Vorschrift.

#### **Zu Buchstabe h**

Es handelt sich um eine redaktionelle Folgeänderung und um redaktionelle Änderungen zur Anpassung der Vorschrift an die Terminologie der Datenschutz-Grundverordnung.

#### **Zu Buchstabe i**

Es handelt sich um eine Folgeänderung aufgrund der Neufassung des § 180 Absatz 2 StVollzG-E, um eine Folgeänderung aufgrund des auf den Vollzug der Haft nach § 171 StVollzG beschränkten Anwendungsbereichs der Vorschrift und um eine redaktionelle Änderung zur Anpassung der Vorschrift an die Terminologie der Datenschutz-Grundverordnung.

### **Zu Buchstabe j**

Es handelt sich zum einen um eine redaktionelle Folgeänderung. Der Regelungsgehalt des bisherigen § 180 Absatz 2 Nummer 1 bis 3 StVollzG, auf den bisher in § 180 Absatz 9 StVollzG verwiesen wurde, findet sich jetzt in § 23 Absatz 1 Nummer 3 und 5 BDSG (2018). Zum anderen wird die Terminologie der Vorschrift an die Datenschutz-Grundverordnung angepasst.

### **Zu Buchstabe k**

Aus der Verweisung auf die zu beachtenden Regelungen der §§ 182 und 184 StVollzG ist § 184 Absatz 4 StVollzG auszunehmen, da diese Vorschrift aufgehoben werden soll (vgl. hierzu Nummer 13 Buchstabe e). Durch die bisherige Bezugnahme auf § 184 Absatz 4 StVollzG wurde zum Ausdruck gebracht, dass unrichtige personenbezogene Daten nicht übermittelt werden dürfen. Eine inhaltliche Änderung folgt aus der Streichung dieser Bezugnahme nicht. Denn die Übermittlung unrichtiger personenbezogener Daten ist grundsätzlich unzulässig und kann für die Wahrnehmung der Aufgaben der Vollzugsbehörde nicht erforderlich sein (vgl. § 180 Absatz 1 StVollzG). Darüber hinaus ergibt sich die Unzulässigkeit der Übermittlung unrichtiger personenbezogener Daten auch aus dem Grundsatz der Datenrichtigkeit des Artikels 5 Absatz 1 Buchstabe d der Datenschutz-Grundverordnung.

### **Zu Buchstabe l**

Es handelt sich um eine redaktionelle Folgeänderung.

### **Zu Buchstabe m**

Artikel 19 Satz 2 der Datenschutz-Grundverordnung enthält die Pflicht, die betroffene Person im Falle einer Berichtigung, Löschung oder Einschränkung der Verarbeitung übermittelter Daten zu unterrichten, wenn die betroffene Person dies verlangt. Auch von dieser Unterrichtungspflicht kann unter den Voraussetzungen des Artikels 23 der Datenschutz-Grundverordnung abgewichen werden (vgl. hierzu die Ausführungen zu § 179 Absatz 4 StVollzG-E unter Nummer 8 Buchstabe d). Von dieser Möglichkeit soll hier nur für den Fall Gebrauch gemacht werden, dass die Unterrichtung der betroffenen Person den Zweck der Übermittlung gefährden würde.

### **Zu Nummer 10 (Änderung von § 181 StVollzG)**

Die vorgenommene Neufassung der Vorschrift entspricht dem Regelungsmuster des § 25 BDSG (2018).

### **Zu Nummer 11 (Änderung von § 182 StVollzG)**

#### **Zu Buchstabe a**

Es handelt sich um eine redaktionelle Änderung zur Anpassung der Überschrift an die Terminologie der Datenschutz-Grundverordnung.

#### **Zu Buchstabe b**

Es handelt sich um eine redaktionelle Folgeänderung.

#### **Zu Buchstabe c**

Es handelt sich um redaktionelle Änderungen zur Anpassung der Vorschrift an die Terminologie der Datenschutz-Grundverordnung.

## **Zu Nummer 12 (Änderung von § 183 StVollzG)**

### **Zu Buchstabe a**

Es handelt sich um eine redaktionelle Änderung zur Anpassung der Überschrift an die Terminologie der Datenschutz-Grundverordnung, in der statt des Begriffs „Dateien“ der Begriff „Dateisysteme“ verwendet wird.

### **Zu Buchstabe b**

Für technische und organisatorische Maßnahmen gelten die Artikel 24, 25 und 32 der Datenschutz-Grundverordnung abschließend. § 9 BDSG a. F. nebst Anlage sind daher im neuen Bundesdatenschutzgesetz nicht mehr enthalten. Daher soll durch die vorliegende Änderung rein deklaratorisch auf die einschlägigen Vorgaben der Datenschutz-Grundverordnung hingewiesen werden. Daneben soll die Vorschrift an die Terminologie der Datenschutz-Grundverordnung angepasst werden.

## **Zu Nummer 13 (Änderung von § 184 StVollzG)**

### **Zu Buchstabe a**

Es handelt sich um eine redaktionelle Änderung zur Anpassung der Überschrift an die Terminologie der Datenschutz-Grundverordnung, in der statt des Begriffs „Sperrung“ der Begriff „Einschränkung der Verarbeitung“ verwendet wird.

### **Zu Buchstabe b**

Es handelt sich um eine redaktionelle Änderungen zur Anpassung der Vorschrift an die Terminologie der Datenschutz-Grundverordnung.

### **Zu Buchstabe c**

Es handelt sich um redaktionelle Änderungen zur Anpassung der Vorschrift an die Terminologie der Datenschutz-Grundverordnung und um Folgeänderungen aufgrund des auf den Vollzug der Haft nach § 171 StVollzG beschränkten Anwendungsbereichs der Vorschrift.

### **Zu Buchstabe d**

Es handelt sich um eine redaktionelle Änderung zur Anpassung der Vorschrift an die Terminologie der Datenschutz-Grundverordnung.

### **Zu Buchstabe e**

§ 184 Absatz 4 StVollzG regelte bisher, dass dem Empfänger die Übermittlung unrichtiger Daten mitzuteilen war, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich war. Eine entsprechende Verpflichtung enthält auch Artikel 19 Satz 1 der Datenschutz-Grundverordnung. Die vorliegende Regelung soll daher aufgehoben werden.

§ 184 Absatz 5 StVollzG erklärte bisher für die Berichtigung, Löschung und Sperrung personenbezogener Daten § 20 Absatz 1 bis 4 und 6 bis 8 BDSG a. F. für anwendbar. Da die Fragen der Berichtigung, Löschung und Sperrung personenbezogener Daten in der Datenschutz-Grundverordnung in Artikel 16 bis 18 geregelt sind, enthält das neue Bundesdatenschutzgesetz keine entsprechenden Regelungen mehr. Vielmehr sind die Vorgaben der Datenschutz-Grundverordnung unmittelbar anwendbar; daneben greifen die ergänzenden Regelungen in § 35 BDSG (2018). § 184 Absatz 5 StVollzG soll daher aufgehoben werden.

## **Zu Nummer 14 (Änderung von § 185 StVollzG)**

### **Zu Buchstabe a**

Es handelt sich um eine redaktionelle Änderung zur Anpassung der Überschrift an die Terminologie der Datenschutz-Grundverordnung.

### **Zu Buchstabe b und Buchstabe c**

Das bisher in § 19 BDSG a. F. geregelte Auskunftsrecht der betroffenen Person richtet sich zukünftig nach Artikel 15 der Datenschutz-Grundverordnung. § 34 BDSG (2018) enthält daneben zum einen Einschränkungen dieses Auskunftsrechts der betroffenen Person und regelt zum anderen Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Person. Die Ausnahmemöglichkeiten nach Absatz 1 dieser Vorschrift sollen daher in § 185 Satz 1 StVollzG-E ausdrücklich in Bezug genommen werden. Satz 2 und Satz 3 enthalten redaktionelle Folgeänderungen.

## **Zu Nummer 15 (Änderung von § 187 StVollzG)**

§ 187 StVollzG enthielt bisher Verweisungen auf das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze. Diese Verweisungen soll mit Blick auf die unmittelbare Geltung der Datenschutz-Grundverordnung aufgehoben werden. Daneben gelten die Vorschriften des Bundesdatenschutzgesetzes, soweit die Datenschutzregelungen des Strafvollzugsgesetzes einen Sachverhalt nicht oder nicht abschließend regeln (vgl. § 2 Absatz 1 BDSG (2018)).

## **Zu Artikel 13 (Änderung der Grundbuchordnung – GBO)**

### **Zu Nummer 1 (Einfügung von § 12d)**

Mit dem in die GBO neu eingefügten § 12d der Grundbuchverordnung in der Entwurfsfassung (GBO-E) wird von der Möglichkeit nach Artikel 23 der Datenschutz-Grundverordnung Gebrauch gemacht, wonach die Pflichten und Rechte gemäß den Artikeln 12 bis 22 der Datenschutz-Grundverordnung im Wege von Gesetzgebungsmaßnahmen beschränkt werden können, sofern dies der Sicherstellung eines der in Artikel 23 Absatz 1 Buchstabe a bis j der Datenschutz-Grundverordnung genannten Schutzzwecke dient. Die im neu eingefügten § 12d GBO-E enthaltenen Regelungen stützen sich dabei auf Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung. Danach können die Pflichten und Rechte dann beschränkt werden, wenn dies für den Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses eine notwendige und verhältnismäßige Maßnahme ist.

Die effektive Gestaltung der Grundbuchführung sowie die Funktionalität und Verlässlichkeit des Grundbuchs verlangen die vorgenommenen Beschränkungen. Als öffentliches Register bildet es für die Grundstücke und grundstücksgleichen Rechte die daran bestehenden Eigentumsverhältnisse und die damit verbundenen Belastungen ab und stellt ihre Rangverhältnisse untereinander fest. Sein Hauptzweck besteht darin, auf zuverlässiger Grundlage die Entstehung und Gestaltung der Rechtsverhältnisse an Immobilien zu dokumentieren und damit eine rechtssichere Grundlage für den Rechtsverkehr zu schaffen. Einer Eintragung in das Grundbuch kommt eine wesentliche Bedeutung zu. Sie ist Publizitätsakt, der das vorgenommene Rechtsgeschäft vollendet und die Basis der gesetzlichen Vermutung der Richtigkeit des Grundbuchinhaltes nach § 891 BGB schafft. Ferner bildet die Eintragung die Grundlage des Schutzes durch den öffentlichen Glauben des Grundbuchs bei Verfügungen über eingetragene Rechte und bei Leistungen an den Eingetragenen. In seiner gegenwärtigen Form ist das Grundbuch folglich eine für die Sicherheit und Leichtigkeit des Rechtsverkehrs unerlässliche Einrichtung. Erwägungsgrund 73 Datenschutz-Grundverordnung nennt im Zusammenhang mit möglichen Beschränkungen von

Rechten der von der Datenverarbeitung betroffenen Personen zudem ausdrücklich das Führen öffentlicher Register als allgemeines öffentliches Interesse im Sinne des Artikels 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung.

Die vorgesehenen Beschränkungen achten den Wesensgehalt der Grundrechte und Grundfreiheiten und stellen eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme im Sinne des Artikels 23 Absatz 1 der Datenschutz-Grundverordnung dar. Bei einer Abwägung zwischen dem betroffenen grundrechtlichen Interesse des Einzelnen auf Schutz seiner personenbezogenen Daten und dem Interesse des Rechts- und Wirtschaftsverkehrs an der Funktionsfähigkeit und Verlässlichkeit des Grundbuchs überwiegt Letzteres. Ein funktionsfähiges und verlässliches Grundbuch mit Publizitätswirkung ist für die Sicherheit und Leichtigkeit des Rechtsverkehrs unerlässlich. Dabei ist zu berücksichtigen, dass bereits hohe Anforderungen an die Eintragungen in das Grundbuch selbst gestellt werden. In der Regel bedarf es hierfür einer notariellen Beurkundung oder Beglaubigung der erforderlichen Erklärungen. Darüber hinaus ist dem betroffenen Grundstückseigentümer sowie Inhaber dinglicher Rechte an dem Grundstück regelmäßig bekannt, dass seine persönlichen Daten im Grundbuch gespeichert und grundsätzlich abrufbar sind. Die erhobenen und in das Grundbuch selbst eingetragenen personenbezogenen Daten sind zudem grundsätzlich auf die Angabe des Namens und des Geburtsdatums beschränkt. Gegebenenfalls können auch der akademische Grad, der frühere Familienname und der Wohnort eingetragen sein (vgl. § 15 Absatz 1 Buchstabe a der Grundbuchverordnung – GBV).

Einige weitere Ansprüche aus der Datenschutz-Grundverordnung bestehen bezüglich des Grundbuchs bereits aufgrund der in der Datenschutz-Grundverordnung selbst vorgesehenen Ausnahmen nicht:

Eine Informationspflicht der die Grundbücher führenden Amtsgerichte (Grundbuchämter) nach Artikel 14 Absatz 1 bis 4 der Datenschutz-Grundverordnung ist bereits gemäß Artikel 14 Absatz 5 Buchstabe c der Datenschutz-Grundverordnung ausgeschlossen, da die Erlangung oder Offenlegung von Informationen durch Rechtsvorschriften, die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist. Einer Informationspflicht kommen die Grundbuchämter allerdings nach dem geltenden Recht bereits nach. Gemäß § 55 muss jede Eintragung dem den Antrag einreichenden Notar, dem Antragsteller und dem eingetragenen Eigentümer sowie allen aus dem Grundbuch ersichtlichen Personen, zu deren Gunsten die Eintragung erfolgt ist oder deren Recht durch sie betroffen wird, bekanntgemacht werden.

Eine Ausnahmeregelung zu dem in Artikel 17 der Datenschutz-Grundverordnung enthaltenen Recht auf Löschung personenbezogener Daten ist nicht erforderlich, weil die Speicherung und Verarbeitung personenbezogener Daten im Grundbuch zur Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich ist und daher Artikel 17 Absatz 3 Buchstabe b der Datenschutz-Grundverordnung greift. Die Löschung der Daten im Sinne einer Streichung oder Unkenntlichmachung würde der Funktionsfähigkeit des Grundbuches und seiner Aufgabe, die rechtlichen Verhältnisse am Grundstück zu jeder beliebigen Zeit korrekt abzubilden, zuwider laufen. Eine Löschung im Sinne des Grundbuchrechts muss daher die zu löschende Eintragung weiterhin erkennen lassen.

Eine Ausnahme vom Recht auf Einschränkung der Verarbeitung gemäß Artikel 18 Absatz 1 der Datenschutz-Grundverordnung ist nicht erforderlich, weil die Verarbeitung personenbezogener Daten bei der Führung des Grundbuches ein wichtiges öffentliches Interesse darstellt (vgl. auch Erwägungsgrund 73 Datenschutz-Grundverordnung) und das Recht auf Einschränkung der Verarbeitung insoweit gemäß Artikel 18 Absatz 2 der Datenschutz-Grundverordnung ausgeschlossen ist.

Eine Mitteilungspflicht der für die Führung des Grundbuchs verantwortlichen Stelle aus Artikel 19 der Datenschutz-Grundverordnung ist bereits nach dessen Wortlaut ausge-

geschlossen, da dies mit einem unverhältnismäßigen Aufwand verbunden wäre. Die Unverhältnismäßigkeit beruht zum einen auf der hohen Anzahl an verarbeiteten personenbezogenen Daten im Grundbuch. Darüber hinaus müssten regelmäßig zusätzlich personenbezogene Daten der Abrufenden und Abdruckempfänger über den Umfang hinaus, der in den Vorschriften zur Durchführung der GBO insoweit vorgesehen ist, erfasst und gespeichert werden, um der Mitteilungspflicht nachzukommen. Dies wäre mit einem unverhältnismäßigen Eingriff in das Persönlichkeitsrecht der Empfänger und einem unverhältnismäßigen Verwaltungsaufwand verbunden.

Artikel 20 der Datenschutz-Grundverordnung (Recht auf Datenübertragbarkeit) findet auf die öffentlichen Register, zu denen auch das Grundbuch gehört, keine Anwendung, da die Verarbeitung gemäß Artikel 20 Absatz 3 Satz 2 der Datenschutz-Grundverordnung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt.

### **Zu Absatz 1**

Das Recht der betroffenen Person auf Auskunft nach Artikel 15 Datenschutz-Grundverordnung wird dadurch beschränkt, dass die betroffene Person stattdessen auf die bestehenden Auskunftsansprüche nach § 12 und den dazu erlassenen Vorschriften der GBV sowie die in § 55 vorgeschriebene Bekanntmachung verwiesen wird.

Nach § 12 Absatz 1 GBO ist die Einsicht des Grundbuchs jedem gestattet, der ein berechtigtes Interesse darlegt. Ausreichend ist insoweit, dass der Antragsteller ein verständiges, durch die Sachlage gerechtfertigtes Interesse rechtlicher, wirtschaftlicher oder rein tatsächlicher Art verfolgt. Das trifft insbesondere auf jeden zu, dem ein Recht am Grundstück oder an einem solchen Grundstücksrecht zusteht oder der als Inhaber eines solchen Rechts im Grundbuch eingetragen ist. Das Erfordernis des Vorliegens eines berechtigten Interesses dient dazu, missbräuchliche Einsichtnahmen, durch die die schutzwürdigen Interessen der Eingetragenen verletzt werden könnten, zu verhindern. Im Hinblick auf das Grundrecht der informationellen Selbstbestimmung des Artikel 2 Absatz 1 GG ist eine solche Voraussetzung zur Gewährung des Einsichtsrechts auch geboten. Das Grundbuch und die Grundakten enthalten zahlreiche Informationen aus dem persönlichen und wirtschaftlichen Bereich des Eigentümers; an der weitmöglichen Geheimhaltung dieser Fakten gegenüber unbeteiligten Dritten hat der Grundstückseigentümer oder Inhaber eines anderen Rechts am Grundstück ein schützenswertes Interesse. Der Einsicht unterliegen auch die Urkunden, auf die im Grundbuch Bezug genommen werden kann, sowie die noch nicht erledigten Eintragungsanträge oder Eintragungsersuchen zum betreffenden Grundbuchblatt. Der Umfang des Einsichtsrechts bestimmt auch das Recht, Abschriften selbst zu fertigen oder sich solche Abschriften erteilen zu lassen. Ausfluss des Einsichtsrechts ist das weitere Recht des Betroffenen, eine Abschrift des Grundbuchs zu verlangen. Das Recht auf Grundbucheinsicht erstreckt sich darüber hinaus auf das Eigentümerverzeichnis und die weiteren, nach § 12a Absatz 1 GBO mit Genehmigung der Landesjustizverwaltung geführten Verzeichnisse.

Durch das Gesetz zur Einführung des Datenbankgrundbuchs vom 1. Oktober 2013 (BGBl. I S. 3719), das zuletzt durch Artikel 19 des Gesetzes vom 21. November 2016 (BGBl. I S. 2591) geändert worden ist, wurde zudem eine Protokollierungspflicht nach § 12 Absatz 4 in Verbindung mit § 46a GBV (bzw. § 85a GBV bei isolierter Grundbucheinsicht durch den Notar) eingefügt. Diese umfasst die Protokollierung von allen Einsichten in Grundbücher und Grundakten sowie die Protokollierung der Erteilung von Abschriften aus Grundbüchern und Grundakten. Dem Eigentümer des betroffenen Grundstücks oder dem Inhaber eines grundstücksgleichen Rechts ist grundsätzlich auf Verlangen Auskunft aus diesem Protokoll zu geben.

Die Einsicht in das Grundbuch kann unter bestimmten Voraussetzungen auch im automatisierten Grundbuchabrufverfahren ermöglicht werden (§ 133 GBO). Auch die Grundbuch-



abrufe sind zu protokollieren. Und auch in diesem Verfahren steht dem Eigentümer des jeweils betroffenen Grundstücks oder dem Inhaber des grundstücksgleichen Rechts ein Auskunftsrecht nach § 133 Absatz 5 Satz 2 GBO darüber zu, durch wen der Grundbuchabruf erfolgt ist.

Soweit die bestehenden Regelungen hinter dem Auskunftsrecht nach Artikel 15 der Datenschutz-Grundverordnung zurückbleiben, bedarf es dieser Beschränkung nach Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung. Das Interesse des Rechts- und Wirtschaftsverkehrs an der Funktions- und Handlungsfähigkeit der Grundbuchämter überwiegt das Interesse der von einer Datenverarbeitung betroffenen Person. Ein weitergehender Anspruch als nach den grundbuchrechtlichen Regelungen bereits vorgesehen, wäre für die Grundbuchämter mit einem unverhältnismäßigen Aufwand verbunden. Dies gilt zum einen mit Blick auf die Vielzahl an enthaltenen Daten. Der Aufwand stünde zudem außer Verhältnis zu dem Nutzen der Mitteilungspflicht. Jedermann kann sich unkompliziert über den aktuellen Inhalt des Grundbuchs informieren und niemand kann sich darauf verlassen, dass sich der Grundbuchinhalt nicht ändert.

### **Zu Absatz 2**

Das Recht der betroffenen Person auf Berichtigung nach Artikel 16 der Datenschutz-Grundverordnung soll nach Absatz 2 dadurch beschränkt werden, dass die betroffene Person stattdessen auf die bestehenden Grundbuchberichtigungsansprüche verwiesen wird. Die Berichtigung des Grundbuchs ist nur im grundbuchrechtlichen Verfahren durch das jeweilige Grundbuchamt möglich, wenn die Voraussetzungen des § 22 GBO für eine Berichtigung oder die Löschung nach den §§ 894 ff. BGB und den §§ 23 bis 25 GBO und 27 GBO vorliegen. Die materiell-rechtliche Publizitätswirkung schließt ein gänzliches Löschen im Sinne des Unkenntlichmachens von Daten oder eine Berichtigung, die implizit zu einer Tilgung oder Streichung der zu berichtenden Eintragung führt, aus. Eine Berichtigung oder eine Löschung, die sich außerhalb des hierfür in der GBO vorgesehenen Verfahrens und in anderer als der hier vorgesehenen Weise vollzieht, wäre mit gravierenden Einschränkungen der Publizität des Grundbuches verbunden; die gesetzlich angeordnete Richtigkeitsgewähr (§ 891 BGB) würde eingeschränkt.

Ein Recht auf Löschung nach Artikel 17 Absatz 1 der Datenschutz-Grundverordnung besteht nicht, da bereits der Ausschlussstatbestand nach Artikel 17 Absatz 3 Buchstabe b der Datenschutz-Grundverordnung vorliegt. Das Grundbuch kann seinen Zweck nur erfüllen, wenn dauerhaft aus dem Grundbuch ersichtlich ist, über welchen Zeitraum welche Eintragungen im Grundbuch enthalten waren, auf die der Rechtsverkehr vertrauen konnte, unabhängig davon, ob sie richtig oder unrichtig waren.

Die Berichtigung von bloßen Schreibfehlern oder anderen offensichtlichen Unrichtigkeiten ist im Grundbuchrecht zudem auch von Amts wegen möglich. Das insoweit einschlägige Verfahren ist gesetzlich nicht geregelt, aber allgemein anerkannt. Neben Korrekturen des Bestandsverzeichnisses sind auf diese Weise vor allem Bezeichnungsänderungen des Berechtigten sowie die Präzisierung unklarer Grundbucheintragungen möglich.

### **Zu Absatz 3**

Für erfolgte Eintragungen im Grundbuch gilt der Grundsatz der Erhaltung der Eintragung. Grundbucheintragungen werden unter anderem dadurch geschützt, dass nach § 71 Absatz 2 Satz 1 GBO die Beschwerde gegen eine Eintragung unzulässig ist. Die Rechtsordnung enthält spezifische Möglichkeiten, gegen eine bestimmte Eintragung im Grundbuch vorzugehen. Hierzu zählen die Ansprüche auf Löschung oder Berichtigung von Eintragungen. Materielle Unrichtigkeiten können nur unter engen Voraussetzungen auf Grundlage von § 22 GBO im Grundbuchverfahren durch Nachweis der Unrichtigkeit gegenüber dem Grundbuchamt oder durch Vorlage einer Berichtigungsbewilligung desjenigen Betei-

ligten, der einen Rechtsverlust erleidet, beseitigt werden. Daneben haben die Beteiligten die Wahl, eine Klage nach § 894 BGB zu erheben. In diesem Zusammenhang kann ein Widerspruch gegen die Richtigkeit des Grundbuchs eingetragen werden. Dieser Widerspruch stellt eine vorläufige Eintragung als Protest gegen die Richtigkeit des Grundbuchs bezüglich eines bestimmten Rechts zur Sicherung eines Berichtigungsanspruchs dar. Es handelt sich also um ein gänzlich vom Widerspruch nach Artikel 21 der Datenschutz-Grundverordnung verschiedenes Rechtsinstrument. Der Grundsatz der Erhaltung der Eintragung macht es ebenso erforderlich, dass ein Widerspruch gemäß Artikel 21 der Datenschutz-Grundverordnung, der zu einer Einschränkung der Verarbeitung führt, ausgeschlossen ist. Es würde die Funktionsfähigkeit des Grundbuchs massiv beeinträchtigen, wenn zugelassen würde, dass ein Betroffener im Wege des Widerspruchs nach Artikel 21 der Datenschutz-Grundverordnung die Grundbucheintragung verhindern könnte. Durch bloßes Einlegen eines Widerspruchs nach der Datenschutz-Grundverordnung könnte der Betroffene wegen des konstitutiven Charakters der Grundbucheintragungen zudem die Entstehung und Änderung von Rechten verhindern und so auf die rechtliche Situation des Grundstücks Einfluss nehmen. Ein solcher Widerspruch wird deshalb durch § 12d Absatz 3 GBO-E auf der Grundlage des Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung ausgeschlossen.

### **Zu Nummer 2 (Änderung von § 126 Absatz 1 GBO)**

#### **Zu Buchstabe a**

Die Änderung ist eine Folge der europarechtlichen Vereinheitlichung von Begriffen durch die Datenschutz-Grundverordnung. Zur Klarstellung wird die Norm dieser Terminologie angepasst.

#### **Zu Buchstabe b**

In ihrer bisherigen Fassung enthielt § 126 Absatz 1 Satz 2 Nummer 3 die Anordnung, dass bei der Führung des maschinellen Grundbuchs diejenigen Standards einzuhalten sind, die in der Anlage zu dieser Vorschrift aufgeführt sind. Rechtstechnisch wurde die Anlage zu § 9 BDSG a. F. in die Anlage zu § 126 GBO übernommen. Es geht um geeignete Vorkehrungen gegen einen unbefugten Zugriff, insbesondere gegen eine unbefugte Einsicht und Veränderung der Daten des Grundbuchs. Für technische und organisatorische Maßnahmen gelten nunmehr die Artikel 24, 25 und 32 der Datenschutz-Grundverordnung unmittelbar. Aufgrund der abschließenden Geltung haben die Mitgliedstaaten keine Konkretisierungsbefugnisse. Die Ausführungen des BDSG zu technischen und organisatorischen Maßnahmen (§ 9 BDSG a. F. nebst Anlage) sind daher im BDSG (2018) entfallen. Aufgrund der unmittelbar geltenden Datenschutz-Grundverordnung ist es unionsrechtlich unzulässig, die Anlage zu § 9 BDSG a. F. in das Fachrecht zu übernehmen. Daher wird auch die Anlage zur Grundbuchordnung, auf die in der bisherigen Fassung von Nummer 3 Bezug genommen wird, mit dem vorliegenden Gesetz aufgehoben. Aus Gründen der Anwenderfreundlichkeit und Einheitlichkeit wird daher deklaratorisch auf die Artikel 24, 25 und 32 der Datenschutz-Grundverordnung verwiesen.

### **Zu Nummer 3 (Änderung von § 131 Absatz 1)**

Die Änderung ist eine Folge der europarechtlichen Vereinheitlichung von Begriffen durch die Datenschutz-Grundverordnung. Zur Klarstellung wird die Norm dieser Terminologie angepasst.

## **Zu Nummer 4 (Änderung von § 133 GBO)**

### **Zu Buchstabe a**

Der aufzuhebende Satz 1 hat seine ursprüngliche Funktion mit der Änderung von § 38 BDSG a. F. durch Gesetz vom 18. Mai 2001 (BGBl. I S. 904) verloren. Bis zu dieser Änderung sah die Vorschrift eine Kontrolle durch die Aufsichtsbehörde nur vor, wenn dieser hinreichende Anhaltspunkte dafür vorlagen, dass datenschutzrechtliche Vorschriften durch nicht-öffentliche Stellen verletzt wurden. Davon abweichend sah der nunmehr aufzuhebende Satz 1 Kontrollen auch ohne das Vorliegen solcher Anhaltspunkte vor.

### **Zu Buchstabe b und c**

Die Streichung von Absatz 6 ist wegen der unmittelbaren Geltung der Datenschutz-Grundverordnung geboten. Der Regelungsinhalt von Absatz 6 wird durch Artikel 5 Absatz 1 Buchstabe b der Datenschutz-Grundverordnung über die Zweckbindung der personenbezogenen Daten abgedeckt. In Folge der Streichung wird der bisherige Absatz 7 neuer Absatz 6.

## **Zu Nummer 5 (§ 134a Absatz 1 Satz 1 GBO)**

Mit der Aufhebung des BDSG a. F. kann auch der rein klarstellende Verweis auf diese Vorschrift und auf die Datenschutzgesetze der Länder aufgehoben werden.

## **Zu Nummer 6 (Aufhebung der Anlage)**

Es handelt sich um eine redaktionelle Folgeänderung zur Änderung von § 126 Absatz 1 Satz 2 Nummer 3. Die hier benannte Anlage ist aufzuheben.

## **Zu Artikel 14 (Änderung der Grundbuchverfügung)**

Es handelt sich um eine Folgeänderung zur Aufhebung von § 133 Absatz 6 GBO.

## **Zu Artikel 15 (Änderung der Schiffsregisterordnung – SchRegO)**

### **Zu Nummer 1 (Einführung von § 97 SchRegO)**

Mit dem in die SchRegO neu eingefügten § 97 der Schiffsregisterordnung in der Entwurfsfassung (SchRegO-E) wird von der Möglichkeit nach Artikel 23 der Datenschutz-Grundverordnung Gebrauch gemacht, wonach die Pflichten und Rechte gemäß den Artikeln 12 bis 22 der Datenschutz-Grundverordnung im Wege von Gesetzgebungsmaßnahmen beschränkt werden können, sofern dies der Sicherstellung eines der in Artikel 23 Absatz 1 Buchstabe a bis j der Datenschutz-Grundverordnung genannten Schutzzwecke dient. Die im neu eingefügten § 97 SchRegO-E enthaltenen Regelungen stützen sich dabei auf Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung. Danach können die Pflichten und Rechte dann beschränkt werden, wenn dies für den Schutz wichtiger Ziele des allgemeinen öffentlichen Interesses eine notwendige und verhältnismäßige Maßnahme ist.

Im Übrigen kann Bezug genommen werden auf die Begründung zu § 12d GBO-E. An das Schiffsregister sind im Hinblick auf die Anforderungen an die Funktionalität und Verlässlichkeit vergleichbare Anforderungen gestellt, wie an das Grundbuch. Das Schiffsregister hat die Aufgabe, die Rechtsverhältnisse an Schiffen und Schiffsbauwerken für jedermann ersichtlich und möglichst erschöpfend zu dokumentieren. Einer Eintragung in das Schiffsregister kommt eine wesentliche Bedeutung zu. Sie ist Publizitätsakt, der das vorgenommene Rechtsgeschäft vollendet und die Basis der gesetzlichen Vermutung der Richtigkeit des Registerinhaltes nach § 16 des Gesetzes über Rechte an eingetragenen Schiffen und

Schiffsbauwerken schafft. Ferner bildet die Eintragung die Grundlage des Schutzes durch den öffentlichen Glauben des Registers bei Verfügungen über eingetragene Rechte und bei Leistungen an den Eingetragenen. Die Führung des Schiffsregisters weist viele Parallelen zur Grundbuchführung auf.

Auch die Ausführungen in der Begründung zu § 12d GBO-E zu den weiteren Rechten aus der Datenschutz-Grundverordnung, die aufgrund der in der Datenschutz-Grundverordnung selbst vorgesehenen Ausnahmen nicht bestehen, sind übertragbar. Dies betrifft die Informationspflicht der das Schiffsregister führenden Amtsgerichte (Registergerichte) nach Artikel 14 Absatz 1 bis 4 der Datenschutz-Grundverordnung, das in Artikel 17 der der Datenschutz-Grundverordnung enthaltene Recht auf Löschung personenbezogener Daten, das Recht auf Einschränkung der Verarbeitung gemäß Artikel 18 Absatz 1 der Datenschutz-Grundverordnung, eine Mitteilungspflicht der für die Führung des Schiffsregisters verantwortlichen Stelle aus Artikel 19 der Datenschutz-Grundverordnung sowie eine Regelung zu Artikel 20 der Datenschutz-Grundverordnung (Recht auf Datenübertragbarkeit). Diese Bestimmungen der Verordnung finden entweder bereits keine Anwendung oder Ausnahmeregelungen dazu sind aus Gründen, die sich aus der Verordnung selbst ergeben, nicht erforderlich.

### **Zu Absatz 1**

Das Recht der betroffenen Person auf Auskunft nach Artikel 15 der Datenschutz-Grundverordnung wird dadurch beschränkt, dass die betroffene Person stattdessen auf die bestehenden Auskunftsansprüche nach den §§ 8 und 65 SchRegO und den dazu erlassenen Vorschriften der Schiffsregister-Durchführungsverordnung sowie die in § 57 SchRegO vorgeschriebene Bekanntmachung verwiesen wird.

Das Schiffsregister ist nach § 8 Absatz 1 SchRegO öffentlich und die Einsicht darin jedem gestattet. Nach § 65 Absatz 2 SchRegO ist die Einsicht in das Schiffsbauregister jedem gestattet, der ein berechtigtes Interesse darlegt. Die Einsicht in die Registerakten ist wiederum nur gestattet, soweit ein berechtigtes Interesse glaubhaft gemacht wird (§ 8 Absatz 2 SchRegO). Der Umfang des Einsichtsrechts bestimmt auch das Recht, Abschriften erteilen zu lassen.

Soweit die bestehenden Regelungen hinter dem Auskunftsrecht nach Artikel 15 der Datenschutz-Grundverordnung zurückbleiben, bedarf es der Beschränkung nach Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung. Das Interesse des Rechts- und Wirtschaftsverkehrs an der Funktions- und Handlungsfähigkeit der Registergerichte überwiegt das Interesse der von einer Datenverarbeitung betroffenen Person. Ein weitergehender Anspruch als nach den registerrechtlichen Regelungen bereits vorgesehen, wäre für die Gerichte mit einem unverhältnismäßigen Aufwand verbunden. Der Aufwand stünde zudem außer Verhältnis zu dem Nutzen der Mitteilungspflicht. Jedermann kann sich unkompliziert über den aktuellen Inhalt des Schiffsregisters informieren.

### **Zu Absatz 2**

Das Recht der betroffenen Person auf Berichtigung nach Artikel 16 der Datenschutz-Grundverordnung soll nach Absatz 2 dadurch beschränkt werden, dass die betroffene Person stattdessen auf die bestehenden Berichtigungsansprüche verwiesen wird. Die Berichtigung des Schiffsregisters ist nur im Registerverfahren durch das Registergericht möglich, wenn die Voraussetzungen der §§ 24, 31 und 35 SchRegO vorliegen. Die materiell-rechtliche Publizitätswirkung schließt ein gänzlichliches Löschen im Sinne des Unkenntlichmachens von Daten oder eine Berichtigung, die implizit zu einer Tilgung oder Streichung der zu berichtenden Eintragung führt, aus. Eine Berichtigung oder eine Löschung, die sich außerhalb des hierfür in der SchRegO vorgesehenen Verfahrens und in anderer

als der hier vorgesehenen Weise vollzieht, wäre mit gravierenden Einschränkungen der Publizität des Schiffsregisters verbunden.

Ein Recht auf Löschung nach Artikel 17 Absatz 1 der Datenschutz-Grundverordnung besteht nicht, da bereits der Ausschlussstatbestand nach Artikel 17 Absatz 3 Buchstabe b der Datenschutz-Grundverordnung vorliegt. Das Schiffsregister kann seinen Zweck nur erfüllen, wenn dauerhaft aus dem Register ersichtlich ist, über welchen Zeitraum welche Eintragungen enthalten waren, auf die der Rechtsverkehr vertrauen konnte, unabhängig davon, ob sie richtig oder unrichtig waren.

### **Zu Absatz 3**

Für erfolgte Eintragungen im Schiffsregister gilt der Grundsatz der Erhaltung der Eintragung. Nach § 75 SchRegO ist die Beschwerde gegen eine Eintragung im Register möglich. Allerdings kann mit der Beschwerde nur verlangt werden, dass das Registergericht angewiesen wird, einen Widerspruch gegen die Richtigkeit der Eintragung einzutragen oder die betreffende Eintragung zu löschen. Neben dem Antragsrecht, das auf die Eintragung, die Berichtigung oder die Löschung einer Eintragung gerichtet ist, soll es keine anderen Möglichkeiten der Einflussnahme eines Betroffenen auf den Registerinhalt geben. Insbesondere soll das Widerspruchsrecht nach Artikel 21 der Datenschutz-Grundverordnung ausgeschlossen sein. Es würde die Funktionsfähigkeit des Schiffsregisters massiv beeinträchtigen, wenn zugelassen würde, dass ein Betroffener im Wege des Widerspruchs nach Artikel 21 der Datenschutz-Grundverordnung die Registereintragung verhindern könnte. Durch bloßes Einlegen eines Widerspruchs könnte der Betroffene wegen des konstitutiven Charakters der Registereintragungen zudem die Entstehung und Änderung von Rechten verhindern und so auf die Rechtsverhältnisse am Schiff Einfluss nehmen. Ein solcher Widerspruch wird deshalb durch § 97 Absatz 3 SchRegO-E auf der Grundlage des Artikels 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung ausgeschlossen.

### **Zu Nummer 2**

Es handelt sich um eine Folgeänderung. Wegen der Einfügung des neuen § 97 SchRegO-E wird der bisherige § 97 SchRegO zu § 98 SchRegO.

### **Zu Artikel 16 (Änderung der Verordnung zur Durchführung der Schiffsregisterordnung)**

#### **Zu Nummer 1 (Änderung von § 58)**

Es handelt sich um eine Folgeänderung zur Änderung von § 126 Absatz 1 Satz 2 Nummer 3 GBO. Die dort bislang benannte Anlage wird mit dem vorliegenden Gesetz aufgehoben. An ihrer Stelle wird deklaratorisch auf diejenigen Bestimmungen der Datenschutz-Grundverordnung hingewiesen, die die notwendigen technisch-organisatorischen Maßnahmen regeln.

#### **Zu Nummer 2 (Änderung von § 68 Satz 3)**

Es handelt sich um eine Folgeänderung zur Aufhebung von § 133 Absatz 6 GBO.

### **Zu Artikel 17 (Änderung der Handelsregisterverordnung)**

Es handelt sich um eine Folgeänderung zur Änderung von § 126 Absatz 1 Satz 2 Nummer 3 GBO. Die dort bislang benannte Anlage wird mit dem vorliegenden Gesetz aufgehoben. An ihrer Stelle wird deklaratorisch auf diejenigen Bestimmungen der Datenschutz-Grundverordnung hingewiesen, die die notwendigen technisch-organisatorischen Maßnahmen regeln, soweit es um personenbezogene Daten geht.

## **Zu Artikel 18 (Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen – IRG)**

### **Zu Nummer 1 (Änderung der Inhaltsübersicht)**

Die Inhaltsübersicht ist auf Grund der Einfügung neuer Vorschriften in das IRG zu ergänzen.

### **Zu Nummer 2 (Einfügung einer Abschnittsüberschrift)**

Es handelt sich um eine redaktionelle Anpassung. Die neuen Regelungen zur Umsetzung der Richtlinie (EU) 2016/680 sollen in einem eigenen Gliederungsabschnitt zusammengefasst werden, um die Übersichtlichkeit zu erhöhen. Insoweit wird der Siebte Teil des IRG in zwei Abschnitte unterteilt. Der Abschnitt, der die bisherigen Vorschriften des Siebten Teils enthält, erhält die Überschrift „Abschnitt 1 – Allgemeine Regelungen“.

### **Zu Nummer 3 (Einfügung von Abschnitt 2)**

Mit Abschnitt 2 wird die Richtlinie (EU) 2016/680 für den Rechtshilfeverkehr mit Drittstaaten und internationalen Organisationen umgesetzt, soweit dies erforderlich ist. Kapitel V der Richtlinie (EU) 2016/680 trifft mit den dortigen Artikeln 35 bis 40 Regelungen für die Übermittlung personenbezogener Daten an Drittstaaten oder internationale Organisationen. Damit bindet die Richtlinie (EU) 2016/680 die zuständigen deutschen Stellen auch im Rechtshilfeverkehr außerhalb der Europäischen Union. Sofern Mitgliedstaaten der Europäischen Union nicht an der Richtlinie (EU) 2016/680 teilnehmen (laut den Erwägungsgründen 99 und 100 kann dies Dänemark, Irland und das Vereinigte Königreich betreffen), sind diese wie Drittstaaten zu behandeln.

Die Regelungen in Abschnitt 2 differenzieren nicht nach „eingehenden“ und „ausgehenden“ Ersuchen, sondern lediglich nach eingehenden und ausgehenden personenbezogenen Daten. Die datenschützenden Vorschriften sind damit grundsätzlich sowohl auf die Erledigung eingehender Rechtshilfeersuchen als auch auf ausgehende Ersuchen anwendbar. Sowohl bei eingehenden Ersuchen als auch bei ausgehenden Ersuchen kommt es regelmäßig zu einer Datenübermittlung durch die nationalen Strafverfolgungsbehörden oder Gerichte der beteiligten Staaten oder Institutionen. Beispielsweise zielen Ersuchen, die die Bundesrepublik Deutschland aus einem anderen Staat erhält, vor allem darauf ab, dass die deutschen Behörden in Erledigung des Ersuchens Daten an das Ausland übermitteln. Bereits das Ersuchen selbst enthält aber regelmäßig ebenfalls personenbezogene Daten, die dann von den deutschen Stellen verwendet werden könnten. Umgekehrt übermitteln deutsche Stellen in einem Ersuchen an einen anderen Staat regelmäßig personenbezogene Daten und erhalten in Erledigung des Ersuchens gegebenenfalls weitere dieser Daten. Für das Recht einer betroffenen Person auf einen angemessenen Datenschutz ist es ohne Bedeutung, ob die Daten bei eingehenden oder ausgehenden Ersuchen erlangt oder verwendet wurden. Dementsprechend behandelt der Gesetzentwurf die Verwendung von Daten im Rahmen von eingehenden und ausgehenden Ersuchen im Grundsatz gleich.

Zum Verhältnis der Regelungen im Abschnitt 2 zu den bereits bestehenden datenschützenden Vorschriften des IRG sowie zu den datenschützenden Vorschriften insbesondere der StPO und des OWiG wird auf die Anmerkungen unter Ziffer II. Nummer 1 Buchstabe b) im Allgemeinen Teil der Begründung verwiesen.

### **Zur Überschrift**

Die Überschrift ist allgemein gehalten und spricht lediglich vom „Schutz personenbezogener Daten im Rechtshilfeverkehr“. Der Begriff „personenbezogene Daten“ ist ein eingeführter Rechtsbegriff des allgemeinen Datenschutzes und muss im IRG nicht be-

reichsspezifisch definiert werden. Erfasst wird damit der gesamte Rechtshilfeverkehr in strafrechtlichen Angelegenheiten im Sinne von § 1 Absatz 1 IRG. Dies sind gemäß § 1 Absatz 2 IRG auch Verfahren wegen einer Tat, die nach deutschem Recht als Ordnungswidrigkeit mit Geldbuße oder die nach ausländischem Recht mit einer vergleichbaren Sanktion bedroht ist, sofern über deren Festsetzung ein auch für Strafsachen zuständiges Gericht entscheiden kann. Erfasst wird zudem der Aus- und Durchlieferungsverkehr ebenso wie die Vollstreckungshilfe und die sonstige Rechtshilfe.

Soweit der Elfte Teil des IRG-E keine Sonderregelungen enthält, gelten die datenschützenden Vorschriften des Abschnitts 2 auch im Rechtshilfeverkehr innerhalb der Europäischen Union und mit den Schengen-assozierten Staaten.

### **Zu § 77c (Anwendungsbereich)**

Die Regelung legt den Anwendungsbereich für die datenschutzrechtlichen Vorschriften im Abschnitt 2 fest. Erfasst werden sämtliche personenbezogene Daten, die im Rechtshilfeverkehr übermittelt oder empfangen werden. Zu dem Begriff des Rechtshilfeverkehrs wird auf die Anmerkungen zur Überschrift verwiesen. Vom Anwendungsbereich erfasst werden auch solche personenbezogene Daten, die in einer papiergeführten Akte in Form einer bloßen Blattsammlung ohne die Möglichkeit des Zugangs nach bestimmten Kriterien enthalten sind. Dies geht über eine 1:1 Umsetzung der Richtlinie (EU) 2016/680 hinaus, nach deren Artikel 2 Absatz 2 der Anwendungsbereich auf personenbezogene Daten beschränkt ist, die (teilweise) automatisiert verarbeitet werden oder die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, siehe bereits unter Ziffer IV. 4. c) aa) 2. Spiegelstrich im Allgemeinen Teil der Begründung. Im IRG sollen die neuen datenschützenden Vorschriften umfassend gelten. Die Richtlinie (EU) 2016/680 lässt dies zu, weil sie lediglich ein datenschützendes Mindestniveau regelt. Ein einheitliches Datenschutzsystem erhöht nicht nur den Grundrechtsschutz der Personen, deren Daten betroffen sind, es ist auch für die Rechtspraxis leichter zu handhaben. Hinzu kommt, dass in den nächsten Jahren die elektronische Akte in Strafsachen eingeführt wird, auch im Bereich der strafrechtlichen Rechtshilfe. Die in elektronischen Akten enthaltenen personenbezogenen Daten unterfallen der Richtlinie (EU) 2016/680. Für eine Differenzierung zwischen verschiedenen datenschützenden Systemen besteht deshalb zunehmend weniger Anlass.

### **Zu § 77d (Übermittlung personenbezogener Daten)**

Die Vorschrift regelt die grundsätzlichen Voraussetzungen und sonstigen Vorgaben für die Übermittlung von personenbezogenen Daten an sämtliche ausländische, zwischen- und überstaatliche Stellen.

Ausdrücklich erwähnt wird nur die Übermittlung von personenbezogenen Daten. Anders als noch der Rb Datenschutz differenziert die Richtlinie (EU) 2016/680 nicht mehr zwischen der Übermittlung und der Bereitstellung von Daten. In der Definition gemäß Artikel 3 Nummer 2 der Richtlinie (EU) 2016/680 werden zwar noch beide Begriffe nebeneinander genannt. In Kapitel V der Richtlinie (EU) 2016/680, das maßgeblich im IRG umzusetzen ist, wird aber nur noch die Übermittlung von personenbezogenen Daten erwähnt. Soweit in Artikel 7 Absatz 2 der Richtlinie (EU) 2016/680 ausnahmsweise doch gesondert von der Bereitstellung von Daten gesprochen wird, scheint dies auf einem bloßen redaktionellen Versehen zu beruhen. Die Vorschrift wurde aus dem Rb Datenschutz übernommen und eine sprachliche Anpassung ist offenbar versehentlich unterblieben. Insoweit ist nicht anzunehmen, dass hier bewusste Unterscheidungen getroffen werden sollten zwischen den Anforderungen, die für eine Datenübermittlung gelten und solchen, die für das Bereitstellen von Daten eingreifen. Dementsprechend soll in den §§ 77d ff. IRG-E einheitlich nur die Datenübermittlung Erwähnung finden. Das Bereitstellen von personenbezoge-

nen Daten wird von dieser Formulierung gemäß der Definition von Artikel 3 Nummer 2 der Richtlinie (EU) 2016/680 ebenfalls erfasst.

### **Zu Absatz 1**

Absatz 1 setzt Artikel 35 Absatz 1 der Richtlinie (EU) 2016/680 um und berücksichtigt zudem die Vorgaben der verfassungsgerichtlichen Rechtsprechung zur Datenweiterleitung an das Ausland auf der Grundlage des BKAG (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 323 ff.).

Die Vorschrift versteht sich nicht als Befugnisnorm. Die Befugnis zur Datennutzung und auch die Reichweite der Befugnis muss sich aus den einschlägigen rechtshilferechtlichen Vorschriften ergeben, beispielsweise aus § 59 Absatz 1 und 3 oder § 92c IRG. Die Formulierung „soweit dies gesetzlich vorgesehen ist“ stellt dies klar.

Statt der in der Richtlinie (EU) 2016/680 verwendeten Formulierung „internationale Organisation“ wird hier von „zwischen- oder überstaatlichen Einrichtungen“ gesprochen, was sich an den Sprachgebrauch des § 67a IRG anlehnt. Die internationalen Strafgerichtshöfe sind hiervon mit umfasst.

Die Formulierung „vorbehaltlich der weiteren Vorschriften der §§ 97a und 97b“ im Chapeau von Absatz 1 weist den Rechtsanwender darauf hin, dass für die strafrechtliche Zusammenarbeit innerhalb der Europäischen Union zum Teil besondere Vorschriften gelten, die zusätzlich zu beachten sind und die die allgemeinen Regelungen zum Teil abändern, zum Teil ergänzen.

### **Zu Nummer 1**

Nummer 1 entspricht Artikel 35 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/680. Der Rb Datenschutz enthielt in seinem Artikel 13 eine vergleichbare Regelung (nur) für den Fall, dass Daten, die aus einem anderen Mitgliedstaat stammen, an Drittstaaten übermittelt werden, siehe hierzu auch die Bundestagsdrucksache 18/6285, S. 13. Die Richtlinie (EU) 2016/680 beansprucht insoweit umfassendere Geltung, als die Mitgliedstaaten auch bei der Übermittlung eigener Daten konkreten Anforderungen unterliegen. Die Ordnungswidrigkeiten werden in die aufgezählten Zwecke ausdrücklich mit einbezogen, auch wenn Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680, auf den in Artikel 35 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/680 Bezug genommen wird, lediglich von „Straftaten“ spricht. Auf die Anmerkungen zur Überschrift von Abschnitt 2 IRG-E wird verwiesen. Dies entspricht dem Ansatz, den die Bundesregierung auch bei der Umsetzung des Rb Datenschutz vorgesehen hatte, siehe Bundestagsdrucksache 18/6285, S. 46.

Ausdrücklich einbezogen werden personenbezogene Daten, die den „Strafvollzug“ betreffen. Die Richtlinie (EU) 2016/680 selbst erwähnt zwar ausschließlich die Strafvollstreckung, nicht den Vollzug; dennoch fällt der Strafvollzug nach Auffassung des deutschen Gesetzgebers in ihren Anwendungsbereich. Strafvollstreckung und Strafvollzug sind zudem auch im Rechtshilfeverkehr, insbesondere der Vollstreckungshilfe, nicht voneinander zu trennen. Im Rahmen einer Vollstreckungsübernahme von freiheitsentziehenden Maßnahmen kann gerade auch der Austausch von personenbezogenen Daten, die den Strafvollzug betreffen, wesentlich sein. Dies gilt etwa für Vollstreckungsübernahmen gegenüber internationalen Strafgerichtshöfen, die jeweils „Herr der Strafvollstreckung“ bleiben. Hat ein Internationaler Gerichtshof beispielsweise mit Blick auf den gesundheitlichen Zustand einer inhaftierten Person über die Fortsetzung der Vollstreckung zu entscheiden, ist er auf Informationen aus dem deutschen Strafvollzug angewiesen. Die ausdrückliche Erwähnung des Strafvollzugs im IRG stellt deshalb klar, dass auch zu diesem Zweck die Übermittlung von personenbezogenen Daten in Betracht kommt.



## **Zu Nummer 2**

Mit Nummer 2 wird Artikel 35 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/680 umgesetzt, der ebenfalls einen vergleichbaren Vorläufer in Artikel 13 des Rb Datenschutz findet. Die Vorschrift will Datenstreuungen vermeiden. Die deutschen Behörden müssen also die Zuständigkeit der empfangenden Stelle überprüfen, bevor sie personenbezogene Daten an das Ausland oder an internationale Einrichtungen, z. B. den Europarat oder die Vereinten Nationen, übermitteln. Dies wird mit Blick auf die internationalen Einrichtungen von praktischer Bedeutung sein, wenn diese nicht über eigene Strafverfolgungsbefugnisse verfügen. Eine Ausnahme von Nummer 2 findet sich in Absatz 3.

## **Zu Nummer 3**

Nummer 3 sieht für die Übermittlung von personenbezogenen Daten ein Zustimmungserfordernis des Ursprungsstaates oder der internationalen oder europäischen Einrichtung vor, aus dem beziehungsweise die Daten ursprünglich stammen. Es muss sich um echte „Fremddaten“ handeln. Stammen die aus dem Ausland erhaltenen personenbezogenen Daten ursprünglich aus der Bundesrepublik Deutschland selbst, greift das Zustimmungserfordernis nicht, vgl. bereits Bundestagsdrucksache 18/6285, S. 45.

Die Regelung setzt Artikel 35 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680 um, der allerdings lediglich die Datenübermittlung an Drittstaaten erfasst, nicht auch die Übermittlung an Mitgliedstaaten oder an Einrichtungen der Europäischen Union. Darüber hinaus sieht Artikel 35 Absatz 1 der Richtlinie (EU) 2016/680 ein Zustimmungserfordernis nur dann vor, wenn der Staat, aus dem die personenbezogenen Daten ursprünglich stammen, ein Mitgliedstaat der Europäischen Union ist. Daten aus Drittstaaten sowie Daten von internationalen oder europäischen Einrichtungen fallen nicht in den Anwendungsbereich der europarechtlichen Vorgabe. Die Regelung in Nummer 3 geht damit in doppelter Weise über die Richtlinie (EU) 2016/680 hinaus. Grund dafür ist, dass ein Zustimmungserfordernis nicht nur mit Blick auf den Datenschutz von Bedeutung sein kann, sondern vor allem auch der Sicherung allgemeiner rechtshilferechtlicher Grundsätze dient, etwa der Beachtung der sogenannten Spezialitätsbindung. Die allgemeinen rechtshilferechtlichen Grundsätze bleiben von der Richtlinie (EU) 2016/680 unberührt, was sich dem Rechtsanwender allerdings nicht ohne weiteres erschließt. Die ausdrückliche Regelung des Zustimmungserfordernisses erleichtert deshalb der Rechtspraxis die Handhabung sowohl der datenschutzrechtlichen als auch der allgemeinen rechtshilferechtlichen Vorschriften. Insoweit ist es auch sachgerecht, das Zustimmungserfordernis weiterhin für den gesamten Bereich der strafrechtlichen Rechtshilfe beziehungsweise der Zusammenarbeit in Strafsachen zur Anwendung zu bringen. Die deutsche Rechtspraxis verfährt regelmäßig bereits heute entsprechend, so dass im IRG kein Erfordernis für eine Differenzierung von Datenübermittlungen zwischen Drittstaaten, internationalen Einrichtungen oder Mitgliedstaaten und Einrichtungen der Europäischen Union besteht, vgl. hierzu bereits die Bundestagsdrucksache 18/6285; S. 52. Die Richtlinie (EU) 2016/680 lässt weitergehende datenschützende Regelungen zu; sie verankert gemäß ihrem Artikel 1 Absatz 3 ausdrücklich nur ein datenschutzrechtliches Mindestniveau.

Das Zustimmungserfordernis entfällt allerdings, wenn der Staat, aus dem die betroffenen personenbezogenen Daten stammen, auf die Zustimmung ausdrücklich verzichtet hat. Dieser Verzicht muss nicht in jedem Einzelfall erklärt werden, sondern kann auch generalisierend erfolgen, zum Beispiel im Zuge von bilateralen Konsultationen der Bundesrepublik Deutschland mit anderen Staaten. Die Ausnahmeregelung will die Rechtspraxis von unnötigen Arbeitsschritten entlasten und beruht damit auf verfahrensökonomischen Erwägungen.

Artikel 35 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680 verlangt zusätzlich, dass die Zustimmung in Einklang mit dem Recht des Ursprungsstaats erteilt werden muss. Diese Voraussetzung richtet sich vor allem an die ausländischen Behörden und wird nicht ins

IRG übernommen. Eine entsprechende Verpflichtung kann im nationalen Recht nicht geregelt werden und ihre Beachtung könnte von den deutschen Behörden auch nur bedingt überprüft werden. Anlassbezogene Nachfragen durch die deutschen Stellen bleiben nach rechtshilferechtlichen Grundsätzen selbstverständlich möglich.

Während der Text der Richtlinie (EU) 2016/680 die Formulierung „zuvor ... genehmigt hat“ verwendet, soll im deutschen Recht in Anlehnung an den eingeführten Sprachgebrauch des IRG (beispielsweise in § 92 Absatz 2 und § 92b Satz 2; dort jeweils „Zustimmung“) von „vorheriger Zustimmung“ gesprochen werden. Inhaltliche Unterschiede sind damit nicht verbunden.

Eine Ausnahmeregelung zu Nummer 3 enthält die Vorschrift in Absatz 4.

#### **Zu Nummer 4**

Mit Nummer 4 wird Artikel 35 Absatz 1 Buchstabe d der Richtlinie (EU) 2016/680 umgesetzt. Die Übermittlung personenbezogener Daten setzt grundsätzlich voraus, dass die Europäische Kommission einen sogenannten Angemessenheitsbeschluss gefasst hat, also einen Beschluss zum angemessenen Datenschutzniveau des Empfängerstaats oder der empfangenden internationalen Stelle. Liegt kein Angemessenheitsbeschluss vor, müssen – im Sinne eines Stufenverhältnisses – geeignete datenschützende Garantien vorliegen oder ein besonderer Ausnahmefall. Das nationale Recht zeichnet dieses Stufenverhältnis nach. Der Begriff „angemessenes Datenschutzniveau“ ist ein eingeführter Rechtsbegriff, der beispielsweise auch in § 61a Absatz 1 Satz 2 und Absatz 3 IRG bereits Verwendung findet.

Auch bei Vorliegen der Voraussetzungen nach Nummer 4, also auch bei Vorliegen eines Angemessenheitsbeschlusses der Europäischen Kommission oder der Voraussetzungen des § 77f IRG-E, bleiben von der übermittelnden deutschen Stelle stets zusätzlich die verfassungsrechtlichen Vorgaben zum Datenschutz zu beachten. Nach der Rechtsprechung des Bundesverfassungsgerichts muss der Empfängerstaat oder die empfangende internationale Stelle über ein angemessenes Datenschutzniveau verfügen und die elementaren Menschenrechte gewährleisten, andernfalls muss eine Übermittlung von personenbezogenen Daten unterbleiben. Neben der Vorschrift in Nummer 4 bleibt bei der Datenübermittlung deshalb auch die Grundsatzregelung des Absatzes 2 zu beachten.

Liegt ein Angemessenheitsbeschluss der Kommission vor, soll die Datenübermittlung gemäß Artikel 36 Absatz 1 Satz 2 der Richtlinie (EU) 2016/680 „keiner besonderen Genehmigung bedürfen“. Erwägungsgrund 36 der Richtlinie (EU) 2016/680 stellt hierzu klar, dass es den Mitgliedstaaten auch bei Vorliegen eines Angemessenheitsbeschlusses (oder der sonstigen Voraussetzungen von Absatz 1 Nummer 4) unbenommen bleibt, die Datenübermittlung unter bestimmte rechtshilferechtliche Bedingungen zu stellen, die nach ihrem nationalen Recht aus Datenschutzgründen erforderlich sind, siehe hierzu auch Absatz 5.

#### **Zu Nummer 5**

Nummer 5 ergänzt die voranstehenden Voraussetzungen um eine Vorgabe, die nicht der Umsetzung der Richtlinie (EU) 2016/680 dient, sondern auf der Rechtsprechung des Bundesverfassungsgerichts zur Datenübermittlung ins Ausland auf der Grundlage des BKAG beruht (siehe hierzu bereits den Allgemeinen Teil der Begründung unter Ziffer II. 1. b)). Das Bundesverfassungsgericht hat ausgeführt, dass jede Übermittlung von personenbezogenen Daten an öffentliche Stellen anderer Staaten eine Zweckänderung darstellt, so dass für die Rechtmäßigkeit der Übermittlung das Kriterium der hypothetischen Datenneuerhebung anzuwenden sei (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 323 ff.). Danach ist eine Datenübermittlung ins Ausland oder an inter-

ationale Organisationen zulässig, soweit die übermittelten Daten auch für den Übermittlungszweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften (a.a.O., Rn. 330). Diese Rechtsprechung zum polizeilichen Datenaustausch ist auf den Datenaustausch in der justiziellen Rechtshilfe in Strafsachen zu übertragen. Die Richtlinie (EU) 2016/680 lässt es zu, zusätzliche Übermittlungsvoraussetzungen im IRG zu verankern, da sie gemäß ihrem Artikel 1 Absatz 3 ausdrücklich nur ein Mindestniveau festschreibt.

### **Zu Absatz 2**

Die Vorschrift setzt Artikel 38 Absatz 2 der Richtlinie (EU) 2016/680 um und formuliert zudem einen allgemeinen datenschützenden Grundsatz, der auf Grund verfassungsrechtlicher Vorgaben im gesamten Rechtshilfeverkehr zur Anwendung gelangt: Ist ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den personenbezogenen Daten im Empfängerstaat oder bei der empfangenden internationalen Einrichtung nicht hinreichend gesichert oder stehen sonst schutzwürdige Interessen der betroffenen Person entgegen, hat die Übermittlung der personenbezogenen Daten auch bei Vorliegen der Voraussetzungen, die in Absatz 1 genannt sind, zu unterbleiben. Daraus, dass Artikel 38 Absatz 2 der Richtlinie (EU) 2016/680 im Kapitel V verortet ist, das den Datenaustausch mit Drittstaaten und internationalen Organisationen betrifft, folgt nicht, dass der datenschützende Grundsatz bei der strafrechtlichen Zusammenarbeit innerhalb der Europäischen Union nicht zur Anwendung gelangt. Auch hier sind selbstverständlich in jedem Fall grundrechtsbezogene Verhältnismäßigkeitsprüfungen zu treffen, was sich bereits aus der Grundrechtecharta der Europäischen Union ergibt. Die Formulierung von Absatz 2 orientiert sich an der Rechtsprechung des Bundesverfassungsgerichts zur Datenübermittlung ins Ausland auf der Grundlage des BKAG, die auch im justiziellen Rechtshilfeverkehr und auch gegenüber Drittstaaten Gültigkeit beansprucht (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 332 und Rn. 350).

### **Zu Absatz 3**

Die Regelung setzt Artikel 39 der Richtlinie (EU) 2016/680 um, soweit dies bereichsspezifisch im IRG erforderlich ist.

Satz 1 lässt abweichend von Absatz 1 Nummer 2 eine Datenübermittlung auch an nicht zuständige öffentliche Stellen oder an nicht-öffentliche Stellen zu, wenn bestimmte Voraussetzungen erfüllt sind, die in den Nummern 1 bis 3 aufgezählt werden. Diese Voraussetzungen müssen zusätzlich zu den sonstigen Voraussetzungen des Absatzes 1 vorliegen. Insbesondere muss es sich bei den in Nummer 1 genannten „zugewiesenen Aufgaben“ um solche handeln, die Strafverfolgungszwecken dienen, und die sich damit im Rahmen der Aufgaben gemäß Absatz 1 Nummer 1 bewegen. Zudem gilt auch hier, dass keine neuen Datenweiterleitungsbefugnisse geschaffen werden. Diese sind vielmehr Voraussetzung der bereichsspezifischen Vorgaben, siehe zu Absatz 1. Praktische Relevanz entfaltet die Vorschrift beispielsweise in Fällen, in denen deutsche Strafverfolgungsbehörden auf direktem Wege Auskünfte zu sogenannten Bestandsdaten bei ausländischen geschäftsmäßigen Anbietern von Telekommunikationsdiensten oder von Telemediendiensten einholen. Die Hinweispflicht aus Artikel 39 Absatz 1 Buchstabe d der Richtlinie (EU) 2016/680 soll hier wegen des Ausnahmecharakters, den die Übermittlung von Daten an andere Stellen als die zuständigen Behörden behalten muss, als echte Übermittlungsvoraussetzung umgesetzt werden (Nummer 3).

Abweichende Regelungen in völkerrechtlichen Verträgen zur Übermittlung von personenbezogenen Daten an nicht-öffentliche Stellen im Ausland haben bereits nach § 1 Absatz 3 IRG Vorrang. Der entsprechende Vorbehalt in Artikel 39 Absätze 1 und 2 der Richtlinie (EU) 2016/680 bedarf daher keiner gesonderten Umsetzung.

Satz 2 enthält eine spezifische Unterrichtungspflicht, die den Vorgaben von Artikel 39 Absatz 1 Buchstabe d der Richtlinie (EU) 2016/680 entspricht.

#### **Zu Absatz 4**

Die Regelung setzt Artikel 35 Absatz 2 der Richtlinie (EU) 2016/680 um.

Satz 1 sieht zwei Ausnahmen für den Fall vor, dass die deutsche Behörde die nach Absatz 1 Nummer 3 erforderliche Zustimmung des Staates, aus dem die personenbezogenen Daten stammen, nicht rechtzeitig einholen kann. Die Daten dürfen dann auch ohne vorherige Zustimmung an andere Staaten oder an zwischen- oder überstaatliche Einrichtungen weitergeleitet werden. Voraussetzung dafür ist allerdings, dass es sich bei diesen personenbezogenen Daten um solche handelt, die aus einem anderen Mitgliedstaat der Europäischen Union, der an der Richtlinie (EU) 2016/680 teilnimmt, oder von einem Schengen-assoziierten Staat stammen (Nummer 1, auch in Verbindung mit Satz 3). Nur in diesem Fall lässt Artikel 35 Absatz 2 der Richtlinie (EU) 2016/680 Ausnahmen zu. Für Daten aus Drittstaaten sowie für Daten von internationalen oder europäischen Organisationen greift die Ausnahmeregelung mangels völkerrechtlicher Grundlage nicht ein. Insofern bleiben die gegebenenfalls bestehenden bilateralen oder internationalen Übereinkommen maßgeblich. In jedem Fall können die deutschen Behörden die zuständigen Behörden in Drittstaaten anlassbezogen darauf hinweisen, dass ein anderer Staat über relevante personenbezogene Daten verfügen könnte. Die beteiligten Staaten können dann unmittelbar miteinander in Kontakt treten.

Sodann muss die Datenübermittlung zur Gefahrenabwehr erforderlich sein, wobei zwei Fallgestaltungen zu unterscheiden sind:

- Die Datenübermittlung ist erforderlich zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines anderen Staates, gleich, ob es sich hierbei um einen Mitgliedstaat der Europäischen Union, einen schengen-assoziierten Staat oder einen Drittstaat handelt (Nummer 2 Buchstabe a). Die Formulierung „gegenwärtige und erhebliche Gefahr“ lehnt sich an den im IRG eingeführten Sprachgebrauch an (vgl. § 92b IRG) und entspricht der in der deutschen Textfassung der Richtlinie (EU) 2016/680 verwendeten Formulierung „unmittelbare und ernsthafte Gefahr“.
- Die Datenübermittlung ist unerlässlich zur Abwehr einer gegenwärtigen und erheblichen Gefahr für wesentliche Interessen eines Mitgliedstaates der Europäischen Union oder eines Schengen-assoziierten Staates (Nummer 2 Buchstabe b). Wie im Chapeau werden auch hier nur solche Mitgliedstaaten der Europäischen Union erfasst, die an der Richtlinie (EU) 2016/680 teilnehmen, was in Satz 3 klargestellt wird. Die Interessen eines Drittstaates werden hier – anders als in Nummer 2 Buchstabe b, wo Drittstaaten einbezogen sind – in Umsetzung der Vorgaben von Artikel 35 Absatz 2 der Richtlinie (EU) 2016/680 nicht erfasst. Was unter dem Begriff „wesentliche Interessen“ zu verstehen ist, wird in der Richtlinie (EU) 2016/680 nicht näher definiert. Auch Erwägungsgrund 65 der Richtlinie (EU) 2016/680 schweigt dazu. Aus Erwägungsgrund 25 zum Rb Datenschutz, der eine vergleichbare Vorschrift enthielt, ist aber zu entnehmen, dass es um Interessen geht, die in ihrer Bedeutung der öffentlichen Sicherheit gleichkommen. Beispielhaft werden dort die unmittelbare und ernsthafte Bedrohung der kritischen Infrastruktur oder die erhebliche Störung des Finanzsystems eines Staates genannt.

Satz 2 sieht vor, dass die übermittelnde Stelle unverzüglich die zuständige Behörde des betroffenen Mitgliedstaates oder des betroffenen Schengen-assoziierten Staates unterrichten muss, wenn sie personenbezogene Daten ohne vorherige Zustimmung dieser Be-

hörde an Drittstaaten oder an zwischen- oder überstaatliche Einrichtungen weitergeleitet hat.

Satz 3 stellt klar, dass Satz 1 an beiden Stellen, wo die Mitgliedstaaten der Europäischen Union erwähnt werden (Nummer 1 und Nummer 2 Buchstabe b), jeweils nur solche Mitgliedstaaten meint, die an der Richtlinie (EU) 2016/680 teilnehmen, siehe oben.

### **Zu Absatz 5**

Satz 1 enthält eine bereichsspezifische Verantwortlichkeitsregelung für den Datenaustausch im Rahmen des Rechtshilfeverkehrs. Dies schafft nicht nur für die beteiligten nationalen Behörden und Gerichte Transparenz. Die klare Verantwortlichkeitsregelung erleichtert es auch Personen, deren Daten betroffen sind, Rechtsschutz zu suchen.

Die Vorschrift stützt sich sowohl auf den Verantwortungsgedanken aus Artikel 4 Absatz 4 der Richtlinie (EU) 2016/680 als auch auf die verfassungsgerichtliche Rechtsprechung zur Datenübermittlung ins Ausland auf der Grundlage des BKAG (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 352). Für die Prüfung der Zulässigkeit einer grenzüberschreitenden Übermittlung von personenbezogenen Daten ist die Stelle verantwortlich, die die Daten an andere Staaten oder an eine internationale Einrichtung übermittelt. Von der Vorschrift unberührt bleibt die Verantwortung der nationalen datenführenden Stelle für die Frage, ob die Daten innerstaatlich der übermittelnden Stelle zur Verfügung gestellt werden durften. Ebenfalls unberührt bleibt, dass diejenige Stelle, die übermittelte Daten einsehend oder abrufen, die Verantwortung für die Zulässigkeit dieses Vorgangs trägt. Die übermittelnde Stelle soll – abweichend etwa von dem Regelungsansatz der bisherigen § 477 Absatz 4 Satz 1 und § 487 Absatz 3 Satz 2 StPO – auch dann für die Prüfung der Zulässigkeit der Datenübermittlung verantwortlich sein, wenn die Übermittlung auf Ersuchen des Empfängers erfolgt. Dies erscheint für den grenzüberschreitenden Datenaustausch sachgerecht, weil die empfangende Stelle im Ausland letztlich nicht überprüfen kann, ob die Datenübermittlung nach den Vorgaben des deutschen Rechts zulässig ist.

Die Regelung schafft Klarheit insbesondere in den Fällen, in denen die datenführende und die datenübermittelnde Stelle auseinanderfallen. Dies ist in der Rechtshilfe grundsätzlich immer dann gegeben, wenn nicht der unmittelbare Geschäftsweg gilt. Die Frage der Zulässigkeit der Datenübermittlung ist dann durch die datenübermittelnde Stelle zu prüfen. Kann die datenübermittelnde Stelle aus eigener Anschauung nicht oder jedenfalls nicht vollständig beurteilen, ob die Datenübermittlung zulässig ist, muss sie – sofern sich für sie konkrete Anhaltspunkte bieten – ihrer Prüfpflicht nachkommen, indem sie sich gegebenenfalls an die datenführende Stelle wendet und dort Informationen einholt.

Satz 2 stellt klar, dass die Vorschriften des § 77d IRG-E nichts daran ändern, dass Datenübermittlungen nach den allgemeinen Grundsätzen der Rechtshilfe mit Bedingungen versehen werden können. Dies gilt insbesondere auch dann, wenn die Kommission einen Beschluss gemäß § 77d Absatz 1 Nummer 4 IRG-E gefasst hat oder die Voraussetzungen des § 77f IRG-E gegeben sind, siehe hierzu bereits die Anmerkungen zu Absatz 1 Nummer 4 IRG-E. Der Begriff der Bedingung entspricht dem aus § 72 IRG.

### **Zu § 77e (Prüf-, Informations- und Protokollierungspflichten der übermittelnden Stelle)**

#### **Zu Absatz 1**

Absatz 1 enthält für die nationalen übermittelnden Stellen konkrete Handlungsvorgaben. Die zusammenhängende Darstellung aller im Rechtshilfeverkehr zu beachtenden Prüf-, Informations- und Protokollierungspflichten erleichtert der Rechtspraxis die Handhabung. Die Vorgaben sind in Übereinstimmung mit der Richtlinie (EU) 2016/680 zum Teil verbind-

lich und zum Teil als Soll- oder Kann-Vorschriften ausgestaltet. Dagegen wird bezüglich der Pflichten nicht danach differenziert, ob eine Übermittlung oder eine (bloße) Bereitstellung von personenbezogenen Daten erfolgt. Anders als noch der Rb Datenschutz sieht die Richtlinie (EU) 2016/680 insoweit keine Unterscheidung mehr vor, so dass auch im nationalen Recht einheitliche Regelungen erfolgen können, siehe bereits die Anmerkungen zu § 77d IRG-E.

### **Zu Nummer 1**

Nummer 1 setzt Artikel 7 Absatz 2 Satz 1 und 2 der Richtlinie (EU) 2016/680 um. Die übermittelnde Stelle soll vor der grenzüberschreitenden Übermittlung von personenbezogenen Daten deren Qualität überprüfen. Artikel 7 Absatz 2 Satz 1 der Richtlinie (EU) 2016/680 nennt als Qualitätskriterien die Richtigkeit, Vollständigkeit und Aktualität der Daten. Das nationale Recht übernimmt diese Kriterien. Nach Artikel 7 Absatz 2 Satz 2 der Richtlinie (EU) 2016/680 besteht eine Verpflichtung zur Überprüfung nur, soweit dies „durchführbar“ ist (vgl. auch die englische Textfassung: „as far as practicable“). Nummer 1 ist deshalb als Soll-Vorschrift ausgestaltet. Angaben dazu, unter welchen Voraussetzungen eine Überprüfung möglich ist, enthält die Richtlinie (EU) 2016/680 nicht; sie sind auch im nationalen Recht nicht erforderlich. Das nationale Verfahrensrecht ist geprägt von dem Grundsatz der Aktenklarheit und der Aktenwahrheit, der die zuständigen Behörden verpflichtet, Akteninhalte jederzeit auf ihre Richtigkeit und Aktualität zu prüfen. Im Hinblick darauf dürfte es in der Regel genügen, die Daten auf ihre Schlüssigkeit hin zu überprüfen und eine vertiefte Prüfung lediglich anlassbezogen vorzunehmen. Bei der Auslegung der Norm wird die Rechtspraxis den Grundrechtsschutz betroffener Personen ebenso berücksichtigen wie die Belange einer effektiven grenzüberschreitenden Strafverfolgung.

### **Zu Nummer 2**

Mit Nummer 2 wird Artikel 7 Absatz 2 Satz 3 der Richtlinie (EU) 2016/680 umgesetzt. Die übermittelnde Stelle ist bei der Übermittlung der Daten gehalten, Informationen beizufügen, die es der empfangenden Stelle erlauben, die Qualität der Daten zu prüfen. Gegenüber der Vorschrift aus Nummer 1 enthält Nummer 2 ein weiteres Qualitätskriterium: Neben der Richtigkeit, Vollständigkeit und Aktualität wird hier auch die Zuverlässigkeit der Daten genannt, was den europarechtlichen Vorgaben entspricht. Die Zuverlässigkeit von Daten im Sinne einer Vertrauenswürdigkeit oder Belastbarkeit (englischer Text: „reliability“) ist vor allem im Rahmen des Ermittlungs- oder Strafverfahrens von Belang. Deshalb ist es vorrangig die Aufgabe der empfangenden Stelle, die Zuverlässigkeit der Daten zu überprüfen. Die übermittelnde Stelle soll aber möglichst durch Beifügung von entsprechenden Informationen dazu beitragen, dass die empfangende Stelle diese Aufgabe wahrnehmen kann.

### **Zu Nummer 3**

Nach Nummer 3 muss die übermittelnde Stelle bei der Übermittlung der personenbezogenen Daten ausdrücklich darauf hinweisen, dass die Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt wurden. Die Norm basiert nicht auf den Vorgaben der Richtlinie (EU) 2016/680, sondern auf der Rechtsprechung des Bundesverfassungsgerichts zur Datenübermittlung ins Ausland auf der Grundlage des BKAG (siehe dazu bereits den Allgemeinen Teil der Begründung, Ziffer II. 1. b). Danach hat der Gesetzgeber dafür Sorge zu tragen, dass der Grundrechtsschutz durch eine Übermittlung der von deutschen Behörden erhobenen Daten ins Ausland und an internationale Organisationen nicht ausgehöhlt wird. Hierzu gehört, dass durch die übermittelnden deutschen Stellen sicherzustellen ist, dass die empfangende Stelle sich an Zweckbindungen hält. Verwendungsbeschränkungen sind den empfangenden Stellen bei der Übermittlung klar und ausdrücklich mitzuteilen (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 326). Dementsprechend sieht Nummer 3 einen obligatorischen Hinweis vor. In Übereinstim-

mung mit der verfassungsgerichtlichen Rechtsprechung reicht der bloße Hinweis auf die Zweckbindung aus, ohne dass eine förmliche Verpflichtung erforderlich ist (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 352). Es ist nicht erforderlich, dass die übermittelnde deutsche Stelle Zusicherungen der empfangenden Stelle beziehungsweise des Empfangsstaates dazu verlangt, dass die Zweckbindung eingehalten wird. Bestehen freilich Anhaltspunkte dafür, dass die Zweckbindung aufgebrochen wird, sind im Einzelfall Bedingungen zu stellen und Zusicherungen einzuholen. Das rechtshilferechtliche Instrumentarium sieht dies bereits vor. Es entspricht den Grundsätzen der Rechtshilfe, dass die Leistung der Rechtshilfe von Bedingungen wie etwa der Einhaltung des Spezialitätsgrundsatzes abhängig gemacht werden kann, vgl. § 72 IRG und Nummer 22 Absatz 1 Satz 2 der Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (RiVAST). Die Richtlinie (EU) 2016/680 lässt zusätzliche Anforderungen an die übermittelnde Stelle – wie in Nummer 3 vorgesehen – zu, da sie gemäß ihrem Artikel 1 Absatz 3 ausdrücklich nur ein Mindestniveau festschreibt.

#### **Zu Nummer 4**

Nummer 4 setzt Artikel 35 Absatz 1 Buchstabe e der Richtlinie (EU) 2016/680 um und ergänzt die allgemeine Vorschrift aus Nummer 3. Die deutschen Stellen, die personenbezogene Daten in das Ausland übermitteln, müssen die empfangende Stelle, also staatliche Stellen oder internationale Einrichtungen, ausdrücklich darauf hinweisen, dass eine Weiterleitung der Daten an andere Staaten oder internationale Einrichtungen der vorherigen Zustimmung bedarf. Die Norm gilt auch gegenüber Mitgliedstaaten und Einrichtungen der Europäischen Union, siehe die Begründung zu § 97c IRG-E. Ob es sich bei den personenbezogenen Daten um „eigene“ Daten handelt, oder ob die Daten ursprünglich aus einem anderen Staat oder von einer zwischen- oder überstaatlichen Einrichtung stammen, ist unerheblich. Zum Begriff der „vorherigen Zustimmung“ siehe bereits die Anmerkungen zu § 77d Absatz 1 Nummer 3 IRG-E.

Die Regelung einer (bloßen) Hinweispflicht trägt dem Umstand Rechnung, dass die in der Richtlinie (EU) 2016/680 geregelte Weiterleitung der personenbezogenen Daten denklogisch nur durch einen anderen Staat oder eine zwischen- oder überstaatliche Einrichtung erfolgen kann. Die dort zuständigen Stellen müssen das Zustimmungserfordernis beachten; dies kann allerdings nicht im deutschen Recht geregelt werden. Das IRG kann nur mittelbar sicherstellen, dass die Zustimmungspflicht eingehalten wird, indem ein obligatorischer, vorsorglicher Hinweis durch die übermittelnden deutschen Stellen erfolgt. Der Hinweis hat den Charakter einer rechtshilferechtlichen Bedingung. Vorgaben für die übermittelnde deutsche Stelle dazu, was gilt, wenn der Drittstaat oder die zwischen- oder überstaatliche Einrichtung um Zustimmung bittet, enthält § 77g IRG-E.

#### **Zu Nummer 5**

Nummer 5 verpflichtet die übermittelnde deutsche Stelle, die empfangende Stelle auf rechtshilferechtliche Bedingungen hinzuweisen, denen die Datenverarbeitung nach deutschem Recht unterliegt und die – auch durch die empfangende Stelle – einzuhalten sind. Die Norm setzt damit Artikel 9 Absatz 3 und 4 der Richtlinie (EU) 2016/680 um und hat vor allem klarstellende Funktion. Es entspricht den allgemeinen Grundsätzen der Rechtshilfe, dass die Leistung von Rechtshilfe von Bedingungen abhängig gemacht werden kann, siehe bereits die Ausführungen zu Nummer 3. Die Richtlinie (EU) 2016/680, die nach ihrem Artikel 1 Absatz 3 lediglich ein datenschutzrechtliches Mindestniveau festlegen will, ändert daran nichts. Schon in der bisherigen deutschen Rechtspraxis achten die zuständigen Behörden zudem darauf, dass die Leistung von Rechtshilfe nur mit solchen Bedingungen verknüpft wird, die nach ihrem eigenen, innerstaatlichen Recht beachtet werden können und nicht zu einer Sinnlosigkeit der Rechtshilfe führen (Hackner in: Schomburg/Lagodny/Gleß/Hackner, IRG, 5. Auflage, § 72 Rn. 5).

Die in Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680 verwendete Formulierung „Bedingung“ entspricht dem eingeführten Wortgebrauch des § 72 IRG und kann ins nationale Recht übernommen werden. Zu den mitzuteilenden Bedingungen können insbesondere Lösungs- und Lösungsprüffristen gehören, soweit sie die übermittelnde deutsche Stelle binden. Die StPO kennt im Grundsatz keine festen Lösungsfristen. Daten dürfen grundsätzlich nur solange gespeichert werden, wie dies zur Erfüllung bestimmter, gesetzlich festgelegter Zwecke erforderlich ist. Einzelne Regelungen schreiben allerdings unter bestimmten Voraussetzungen eine „unverzögliche“ Löschung vor (siehe etwa § 100a Absatz 4 Satz 3 und § 101 Absatz 8 Satz 1 StPO). Darüber hinaus enthält das nationale Recht Fristen zur Überprüfung, ob ein gespeichertes Datum zu löschen ist, vgl. § 489 Absatz 3 StPO für Daten, die in einer Datei gespeichert sind.

Bedingungen können nicht nur auf Grund der Vorgaben der eigenen Rechtsordnung praktische Relevanz erlangen. Denkbar ist auch, dass deutsche Behörden Daten übermitteln, die sie ihrerseits von einem anderen Staat unter Bedingungen erhalten haben, beispielsweise unter der Bedingung, bestimmte Lösungsfristen einzuhalten. Diese Bedingung wäre dann bei einer etwaigen Weitergabe der Daten an einen anderen Staat dadurch einzuhalten, dass der empfangenden Stelle die entsprechenden Lösungsfristen mitgeteilt werden, siehe Absatz 2.

### **Zu Nummer 6**

Nummer 6 sieht in Umsetzung von Artikel 7 Absatz 3 der Richtlinie (EU) 2016/680 eine Mitteilungspflicht vor, die eingreift, wenn unrichtige personenbezogene Daten übermittelt wurden oder wenn personenbezogene Daten unrichtig übermittelt wurden. Die Regelung erfolgt vor allem aus Klarstellungsgründen. Eine Pflicht, der empfangenden Stelle mitzuteilen, dass Daten unrichtig oder unrechtmäßig übermittelt wurden, ergibt sich für die übermittelnde deutsche Behörde im Grundsatz bereits aus der allgemeinen Rechtsbindung der Verwaltung. Eine bereichsspezifische Regelung im IRG erscheint wegen der datenschützenden Bedeutung aber sachgerecht. Zudem enthält das IRG – beschränkt auf Fälle der Spontanauskünfte – bereits eine vergleichbare Vorschrift, siehe § 61a Absatz 4 IRG (auch in Verbindung mit § 92c Absatz 2 IRG). Der Wortlaut der Norm lehnt sich an § 61a Absatz 4 IRG an. Die empfangende Stelle ist nach den Grundsätzen der Rechtshilfe verpflichtet, auf die Mitteilung zu reagieren, siehe zu Nummer 4.

### **Zu Nummer 7**

Nummer 7 beruht auf den Vorgaben von Artikel 39 Absatz 3 der Richtlinie (EU) 2016/680 und bezieht sich auf § 77d Absatz 3 IRG-E. Die übermittelnde deutsche Stelle muss die zuständige datenschutzrechtliche Aufsichtsbehörde über alle Datenübermittlungen unterrichten, die nicht an die zuständigen öffentlichen Behörden erfolgen, sondern – unter Einhaltung der erforderlichen Voraussetzungen – an andere Stellen. Vorgaben zu den konkreten Modalitäten der Unterrichtung macht die Richtlinie (EU) 2016/680 nicht und sie können auch im nationalen Recht unterbleiben. Die sachgerechte Umsetzung kann der Ausgestaltung durch die Rechtspraxis überlassen bleiben.

### **Zu Nummer 8**

Mit Nummer 8 werden zunächst die Vorgaben des Bundesverfassungsgerichts zur Protokollierung von Datenübermittlungen an das Ausland oder an internationale Organisationen umgesetzt (siehe hierzu bereits den Allgemeinen Teil der Begründung, Ziffer II. 1 b.). Danach setzt eine wirksame aufsichtsbehördliche Kontrolle eine geeignete Protokollierung voraus (BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 340). Zugleich trägt die Regelung den Vorgaben zur Protokollierung von Datenübermittlungen aus Artikel 25, Artikel 37 Absatz 3 und Artikel 38 Absatz 3 der Richtlinie (EU) 2016/680 Rechnung. Deren inhaltliche Anforderungen zu den Gegenständen der Protokollierung müssen hier aber



nicht im Einzelnen aufgezählt werden. Vielmehr kann auf die maßgeblichen innerstaatlichen Protokollierungspflichten Bezug genommen werden, die ihrerseits den Anforderungen des Bundesverfassungsgerichts entsprechen müssen bzw. bis zum Ablauf der Umsetzungsfrist am 6. Mai 2018 an die Vorgaben der Richtlinie (EU) 2016/680 anzupassen sind.

## **Zu Absatz 2**

Die Norm stellt klar, dass die empfangende Stelle auch dann auf Bedingungen hinzuweisen ist, wenn sich diese nicht unmittelbar aus dem deutschen Recht ergeben, sondern daraus, dass die in Frage stehenden personenbezogenen Daten aus dem Ausland oder von einer internationalen Einrichtung stammen und von dort mit Bedingungen versehen wurden, die auch von der empfangenden Stelle (weiterhin) einzuhalten sind, etwa Löschungs- oder Lösungsprüffristen.

## **Zu § 77f (Verfahren bei Fehlen eines Angemessenheitsbeschlusses)**

### **Zu Absatz 1**

Die Regelung betrifft den Fall, dass kein Angemessenheitsbeschluss der Europäischen Kommission nach § 77d Absatz 1 Nummer 4 IRG-E vorliegt. In diesem Fall kommt es im Sinne eines Stufenverhältnisses (sodann) darauf an, ob geeignete datenschützende Garantien im Empfängerstaat oder in der empfangenden internationalen Einrichtung vorliegen. Rechtshilferechtliche Bedingungen bleiben auch bei Vorliegen der Voraussetzungen aus § 77f IRG-E möglich (§ 77d Absatz 5 Satz 2 IRG-E). Auch der Grundsatz aus § 77d Absatz 2 IRG-E bleibt zu beachten, siehe bereits die Anmerkungen zu § 77d Absatz 1 Nummer 4 IRG-E. Die Vorschrift setzt Artikel 35 Absatz 1 Buchstabe d in Verbindung mit Artikel 37 Absatz 1 der Richtlinie (EU) 2016/680 um und sieht entsprechend den europarechtlichen Vorgaben zwei Möglichkeiten vor, die Frage nach den geeigneten Garantien zu beantworten:

Nach Nummer 1 kann auf völkerrechtliche Instrumente, insbesondere völkerrechtliche Verträge, abgestellt werden, die ausreichende datenschützende Vorgaben enthalten und die für den Empfängerstaat oder die internationale Einrichtung verbindlich sind. Während der Wortlaut des umzusetzenden Artikels 37 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/680 insoweit etwas unscharf bleibt, stellt Erwägungsgrund 71 der Richtlinie (EU) 2016/680 klar, dass es sich bei den in der Richtlinie (EU) 2016/680 erwähnten „rechtsverbindlichen Instrumenten“ um völkerrechtliche Verträge handelt und dass diese Verträge gerade für die Empfängerseite verbindlich sein müssen.

Nach Nummer 2 kann die übermittelnde deutsche Stelle eine Bewertung vornehmen, bei der alle für die Datenübermittlung relevanten Umstände zu berücksichtigen sind. Aus Erwägungsgrund 71 zur Richtlinie (EU) 2016/680 ergibt sich, dass in diese Bewertung allgemeine rechtliche und tatsächliche Aspekte einbezogen werden können, etwa der Umstand, dass Kooperationsabkommen von Eurojust oder Europol mit dem betreffenden Staat oder der betreffenden internationalen Einrichtung existieren, oder die Frage, ob die Todesstrafe oder unmenschliche Behandlung drohen. Dies entspricht der geltenden Rechtshilfepraxis.

### **Zu Absatz 2**

Liegen weder ein Angemessenheitsbeschluss der Europäischen Kommission noch geeignete allgemeine Garantien gemäß Absatz 1 vor, muss eine Datenübermittlung nicht zwingend ausscheiden. Erforderlich ist es dann aber, in einer weiteren Stufe einzelfallbezogen zu prüfen, ob ausnahmsweise eine Datenübermittlung in Betracht kommt. Die Hervorhebung des Einzelfalls verdeutlicht, dass die Vorschrift keine automatisierten oder massen-

haften Datenübermittlungen ermöglichen will. Der Grundsatz aus § 77d Absatz 2 IRG-E bleibt auch hier in jedem Fall zu beachten. Die Vorschrift setzt Artikel 38 Absatz 1 der Richtlinie (EU) 2016/680 um. Dort werden einzelne Fallgruppen aufgeführt, in denen die Datenübermittlung zulässig ist. Absatz 2 bildet alle genannten Fälle ab.

Nummer 1 entspricht Artikel 38 Absatz 1 Buchstabe a der Richtlinie (EU) 2016/680. Die Datenübermittlung kann zum Schutz lebenswichtiger Interessen der betroffenen oder auch einer anderen Person erfolgen. Der Begriff der „lebenswichtigen Interessen“ ist bereits aus dem allgemeinen Datenschutzrecht bekannt, siehe § 4c Absatz 1 Nummer 5 BDSG (= § 80 Absatz 1 Nummer 1 im Gesetzentwurf der Bundesregierung zur Neufassung des BDSG (2018)). Die lebenswichtigen Interessen Dritter können vor allem in Entführungsfällen in Staaten mit geringen rechtsstaatlichen Strukturen praktische Relevanz erlangen.

Nummer 2 stellt geringere Anforderungen als Nummer 1, da hier bereits „schutzwürdige Interessen“ eine Datenübermittlung rechtfertigen können. Es muss aber um die schutzwürdigen Interessen der betroffenen Person selbst gehen; die entsprechenden Interessen Dritter reichen nicht aus. Die Vorschrift setzt Artikel 38 Absatz 1 Buchstabe b der Richtlinie (EU) 2016/680 um. Die dortige Formulierung „berechtigzte Interessen“ wird dabei nicht in das nationale Recht übernommen. In Übereinstimmung mit dem eingeführten Sprachgebrauch beispielsweise des § 61a Absatz 3 IRG wird auf die schutzwürdigen Interessen abgestellt. Eine inhaltliche Abweichung von den europarechtlichen Vorgaben ergibt sich daraus nicht.

Nummer 3 lässt die Datenübermittlung zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Mitgliedstaates der Europäischen Union oder eines Drittstaates zu. Mit der Regelung wird Artikel 38 Absatz 1 Buchstabe c der Richtlinie (EU) 2016/680 umgesetzt. In Übereinstimmung mit dem eingeführten Sprachgebrauch des IRG (vgl. § 92b) wird die europarechtliche Formulierung „unmittelbare und ernsthafte Gefahr“ dabei übersetzt in „gegenwärtige und erhebliche Gefahr“.

Nummer 4 entspricht Artikel 38 Absatz 1 Buchstabe d der Richtlinie (EU) 2016/680. Es handelt sich um eine Auffangregelung, die es zulässt, bei außergewöhnlichen Umständen personenbezogene Daten zu strafrechtlichen Zwecken zu übermitteln. Zur Einbeziehung der „Ordnungswidrigkeiten“ siehe bereits die Anmerkungen zu § 77d Absatz 1 Nummer 1 IRG-E. Zur Einbeziehung des „Vollzugs“ wird ebenfalls auf die Anmerkungen zu § 77d Absatz 1 Nummer 1 IRG-E Bezug genommen. Auch hier erscheint eine klarstellende Erwähnung des Vollzugs sachgerecht, um Rechtsanwendungsfragen zu vermeiden und der Rechtspraxis im Einzelfall ausreichende Handlungsmöglichkeiten einzuräumen.

Nummer 5 setzt Artikel 38 Absatz 1 Buchstabe e der Richtlinie (EU) 2016/680 um. Die Datenübermittlung ist erlaubt, wenn sie erforderlich ist, um Rechtsansprüche im Zusammenhang mit strafrechtlicher Verfolgung oder Vollstreckung durchzusetzen. Eine vergleichbare Regelung ist im deutschen Recht bereits aus § 4c Absatz 1 Nummer 4 BDSG (= § 80 Absatz 1 Nummer 5 im Gesetzentwurf der Bundesregierung zur Neufassung des BDSG (2018)) bekannt.

### **Zu Absatz 3**

Die Vorschrift enthält eine spezielle Unterrichtungspflicht gegenüber der zuständigen Datenaufsichtsbehörde und setzt Artikel 37 Absatz 2 der Richtlinie (EU) 2016/680 um. Die Unterrichtungspflicht greift in Fällen, in denen die Datenübermittlung erfolgt, nachdem die zuständige deutsche Stelle nach Abwägung aller relevanten Umstände entschieden hat, dass geeignete datenschützende Garantien bestehen. Wegen des unmittelbaren Sachzusammenhangs mit der Regelung aus Absatz 1 Nummer 2 und der besseren Wahrnehmbarkeit für die deutsche Rechtspraxis soll eine gesetzliche Umsetzung der Unterrich-

tungspflicht im IRG erfolgen und auf eine – grundsätzlich ebenfalls vorstellbare – Verortung der Norm in den RiVAST verzichtet werden. Zudem kommen Unterrichtungspflichten nach der Rechtsprechung des Bundesverfassungsgerichts wichtige Funktionen bei der Sicherstellung der aufsichtlichen Kontrolle zu (vgl. Urteil vom 20. April 2016, 1 BvR 966/09, Rn. 354). Eine gesetzliche Regelung trägt dieser höchstrichterlichen Rechtsprechung Rechnung.

Die Unterrichtung muss nicht über jede einzelne Datenübermittlung erfolgen, sondern laut der Richtlinie (EU) 2016/680 nur über bestimmte „Kategorien“. Die Richtlinie (EU) 2016/680 lässt offen, was unter dem Begriff der Kategorie zu verstehen ist. Hierfür ist nicht auf die einzelnen Entscheidungen abzustellen, die mitgeteilt werden müssten. Die Einzelfallkontrolle ist nicht Sinn und Zweck der Regelung. Andernfalls müsste diese Kontrolle „erst recht“ bei den Ausnahmefällen des Absatzes 2 erfolgen; hierzu sieht Artikel 38 der Richtlinie (EU) 2016/680 aber keine vergleichbare Regelung vor. Die Vorschrift soll der datenschutzrechtlichen Aufsichtsbehörde ermöglichen, die Entscheidungsfindung generell nachzuvollziehen. Dementsprechend soll hier auf Informationen zu „Fallgruppen“ nach Absatz 1 Nummer 2 abgestellt werden.

### **Zu § 77g (Zustimmung zur Weiterleitung personenbezogener Daten)**

Die Regelung sieht das Prüfprogramm für den Fall vor, dass die übermittelnde deutsche Stelle von einem anderen Staat oder einer internationalen Einrichtung um Erteilung der Zustimmung für eine Weiterleitung von personenbezogenen Daten ersucht wird. Die Regelung gilt nicht nur für solche Fälle, in denen die zuständige deutsche Stelle auf Grund eines Hinweises nach § 77e Absatz 1 Nummer 4 IRG-E kontaktiert wird, sondern auch darüber hinaus, also etwa in Fällen, in denen die ausländische oder internationale Stelle bereits auf Grund der grundsätzlichen rechtshilferechtlichen Spezialitätsbindung um Zustimmung zu einer Zweckänderung ersucht. Die Norm setzt Artikel 35 Absatz 1 Buchstabe e der Richtlinie (EU) 2016/680 um, verzichtet aber auf die wörtliche Wiedergabe von dessen kompliziertem Wortlaut. Es erscheint sinnvoll und praxisgerecht, wenn sich die Anforderungen an eine erstmalige und an eine nachfolgende Übermittlung von personenbezogenen Daten entsprechen. Die Zustimmung zur Datenweiterleitung kann deshalb erteilt werden, wenn auch eine entsprechende unmittelbare Datenübermittlung zulässig wäre. Einen vergleichbaren Ansatz kennt das deutsche Rechtshilferecht bereits aus § 61b Absatz 4 und § 93 Absatz 4 IRG.

### **Zu § 77h (Verwendung von übermittelten personenbezogenen Daten)**

Für personenbezogene Daten, die deutsche Behörden von anderen Staaten oder von zwischen- oder überstaatlichen Einrichtungen erhalten haben, sind bestimmte Verwendungsbeschränkungen vorgesehen. Der Begriff der „Verwendung“ bezeichnet dabei genau wie der Begriff der „Übermittlung“ einen Unterfall der Verarbeitung personenbezogener Daten (siehe die Definition des Verarbeitungsbegriffs in Artikel 3 Nummer 2 der Richtlinie (EU) 2016/680). Wegen der Bedeutung von Zweckbindungen für den Datenschutz und auf Grund des weltweit zunehmenden Datentransfers soll aus Anlass der Umsetzung der Richtlinie (EU) 2016/680 eine gesetzliche Regelung in das IRG aufgenommen werden, auch wenn die Richtlinie (EU) 2016/680 selbst – anders als noch der Rb Datenschutz – nur punktuelle Aussagen zu den Verwendungsbeschränkungen trifft. Der Datenschutz im grenzüberschreitenden Datentransfer berührt ganz wesentlich die Frage, wann die Verwendung bereits erhobener personenbezogener Daten zu verfahrensübergreifenden Zwecken zulässig ist.

### **Zu Absatz 1**

Die Zweckänderung im Rahmen der Verwendung von personenbezogenen Daten, die aus einem anderen Staat oder von einer internationalen Einrichtung stammen, ist nur mit einer

vorherigen Zustimmung der dortigen zuständigen Stellen möglich. Die Zustimmung muss nicht zwingend für jeden Einzelfall gesondert erteilt werden. Vorstellbar wäre beispielsweise auch, dass Vereinbarungen über allgemeine Zustimmungen für bestimmte Weiterverarbeitungskategorien getroffen werden, siehe bereits die Bundestagsdrucksache 18/6285; S. 47. Vom Anwendungsbereich erfasst sind nur echte Fremddaten, siehe die Anmerkungen zu § 77d Absatz 1 Nummer 3 IRG-E. Die Regelung setzt Artikel 4 Absatz 1 Buchstabe b und Absatz 2 sowie Artikel 9 Absatz 1 der Richtlinie (EU) 2016/680 um, die im Grundsatz eine strenge Zweckbindung vorsehen. Dies entspricht auch dem rechtshilferechtlichen Spezialitätsgrundsatz. Schon in der bisherigen Rechtspraxis werden deshalb Zustimmungen eingeholt, vgl. Bundestagsdrucksache 18/6285; S. 52. Eine ausdrückliche Regelung erhöht künftig noch die Transparenz und Wahrnehmbarkeit des Zustimmungserfordernisses und erleichtert der Rechtspraxis damit die Handhabung.

Die Vorschrift versteht sich als eine reine Verwendungsregelung. Die Befugnis zur Datenverwendung und auch die Reichweite der Befugnis müssen sich aus den einschlägigen rechtshilferechtlichen Vorschriften ergeben, beispielsweise aus § 59 Absatz 1 und 3 oder § 92c IRG. Die Formulierung „soweit dies gesetzlich vorgesehen ist“ stellt dies klar. Den begrenzenden Rahmen für die Nutzung der Daten zu anderen Zwecken bildet – auch bei Vorliegen der Zustimmung durch den betroffenen anderen Staat – immer die Zuständigkeit der empfangenden deutschen Stelle. Die Vorschrift will keine neuen Zuständigkeiten oder Befugnisse schaffen.

Zum Verhältnis der Verwendungsregelung zu den datenschützenden Vorschriften insbesondere der StPO und des OWiG wird auf die Anmerkungen unter Ziffer II. 1. b) im Allgemeinen Teil der Begründung verwiesen. Zum Verhältnis zu § 92b IRG siehe ebenfalls dort.

### **Zu Absatz 2**

Für deutsche Behörden, die personenbezogene Daten aus dem Ausland empfangen, wird ausdrücklich geregelt, dass Bedingungen, die die übermittelnde Stelle mit Blick auf die Verwendung der Daten gestellt haben, einzuhalten sind. Zu solchen Bedingungen können auch Löschungs- und Lösungsprüffristen zählen. Die Vorschrift setzt Artikel 9 Absatz 3 der Richtlinie (EU) 2016/680 um und hat vor allem klarstellende Funktion. Es entspricht den Grundsätzen der Rechtshilfe, dass Bedingungen anderer Staaten zu beachten sind. Dies gilt sowohl im Rahmen von eingehenden als auch im Rahmen von ausgehenden Rechtshilfeersuchen, siehe § 72 IRG und Nummer 22 Absatz 1 Satz 2 RiVAST. Die Norm soll deshalb nicht nur im Rechtshilfeverkehr innerhalb der Europäischen Union gelten, sondern auch im Verhältnis zu Drittstaaten sowie zu internationalen Einrichtungen.

### **Zu Absatz 3**

Die Regelung übernimmt die besondere Prüfpflicht aus Artikel 8 Absatz 1 Satz 4 des Rb Datenschutz, der sich zwar ausdrücklich nicht mehr in der Richtlinie (EU) 2016/680 findet, aber den datenschutzrechtlichen Grundsätzen aus Artikel 4 Absatz 1 Buchstabe e der Richtlinie (EU) 2016/680 entspricht. Erhalten deutsche Rechtshilfestellen im Wege von sogenannten Spontanübermittlungen Daten aus dem Ausland, müssen sie unverzüglich prüfen, ob die Daten für den Zweck, für den sie übermittelt wurden, tatsächlich benötigt werden. Die Vorschrift trägt der besonderen Datenschutzsituation bei Spontanübermittlungen Rechnung, hat aber letztlich klarstellenden Charakter. Schon bisher folgte aus dem allgemeinen Rechtsbindungsgrundsatz für deutsche Behörden, dass sie Daten, die sie im Wege von Spontanübermittlungen erlangen, darauf überprüfen müssen, ob sie verwendet werden dürfen.

Vorgaben dazu, wie mit personenbezogenen Daten umzugehen ist, die übermittelt wurden und nicht benötigt werden, macht die Vorschrift nicht. Die Behandlung dieser Daten

richtet sich damit nach allgemeinen Vorschriften. In der Praxis bedeutet dies, dass Mitteilungen von anderen Staaten oder von internationalen Einrichtungen mit Blick auf die Gesetzmäßigkeit der Verwaltung und die Grundsätze der Aktenwahrheit und Aktenklarheit regelmäßig veraktet werden, um sodann den Sachverhalt zu prüfen. Stellt sich heraus, dass die übermittelten Daten nicht benötigt werden, weil der übermittelte Sachverhalt zum Beispiel keine Anhaltspunkte für das Vorliegen einer Straftat oder Ordnungswidrigkeit bietet, wird der Vorgang abgeschlossen. Die Aufbewahrungsdauer der Akte und die Speicherdauer der personenbezogenen Daten, die hierzu in der Vorgangsverwaltung erfasst werden, richten sich nach den einschlägigen innerstaatlichen Vorschriften.

#### **Zu Nummer 4 (Folgeänderung)**

Nummer 4 enthält eine Folgeänderung, die durch Änderungen des IRG erforderlich wird, die in Artikel 3 des Zweiten Gesetzes zur Stärkung der Verfahrensrechte von Beschuldigten im Strafverfahren und zur Änderung des Schöffengerichts vom 27. August 2017 (BGBl. I S. 3295) geregelt sind. Diese betreffen im Wesentlichen eine Einfügung eines weiteren Absatzes in § 83c IRG (Absatz 2). Durch die Folgeänderung erübrigt sich die bisher in dem – noch nicht in Kraft getretenen – Fünften Gesetz zur Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen vom 1. Juni 2017 (BGBl. I S. 1414) vorgesehene Anpassung (vgl. Artikel 19, Nummer 5). Diese Anpassung des nunmehrigen § 83c Absatz 4 Satz 3 IRG korrigiert eine Verfahrensregel im Auslieferungs- und Durchlieferungsverkehr mit Mitgliedstaaten der Europäischen Union auf Grundlage eines Europäischen Haftbefehls (vgl. Bundestagsdrucksache 18/11140, S. 41).

Diese betrifft im Wesentlichen eine Einfügung eines weiteren Absatzes (Absatz 2).

#### **Zu Nummer 5 (Einfügung eines Elften Teils)**

##### **Zur Überschrift**

Die Überschrift umfasst den gesamten Rechtshilfeverkehr, also Auslieferungen, Fälle von Vollstreckungshilfe und sonstiger Rechtshilfe, gleichgültig, ob er auf der Grundlage der tradierten Rechtshilfe oder auf der Grundlage des Prinzips der gegenseitigen Anerkennung erfolgt. Abweichend von dem bisherigen Sprachgebrauch im IRG wird bewusst nicht die Formulierung „Rechtshilfe mit den Mitgliedstaaten der Europäischen Union“ verwendet. Damit wird dem Umstand Rechnung getragen, dass die Vorgaben der Richtlinie (EU) 2016/680 auch dann einzuhalten sind, wenn personenbezogene Daten an Einrichtungen der Europäischen Union übermittelt, für diese bereitgestellt oder von diesen empfangen werden. Auf die Anmerkungen zur Überschrift von Abschnitt 2 im Siebten Teil IRG-E wird im Übrigen ergänzend Bezug genommen.

#### **Zu § 97a (Anwendungsbereich)**

##### **Zu Absatz 1**

Absatz 1 definiert den Anwendungsbereich des Elften Teils. Erfasst werden personenbezogene Daten gemäß § 77c IRG-E, die mit den Mitgliedstaaten der Europäischen Union, die an der Richtlinie (EU) 2016/680 teilnehmen, oder mit Einrichtungen der Europäischen Union ausgetauscht werden. Zu dem Begriff der Übermittlung von personenbezogenen Daten siehe die Anmerkungen zu § 77d IRG-E.

Die europäischen „Informationssysteme“, die in Artikel 1 Absatz 2 des Rb Datenschutz noch erwähnt wurden, aber in der Richtlinie (EU) 2016/680 im Anwendungsbereich nicht mehr gesondert aufgeführt werden (siehe aber Artikel 9 Absatz 4), sind von der Formulierung „Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union“ mitumfasst

und unterfallen somit vom dem Anwendungsbereich der Norm. Zu denken ist hier etwa an das Schengener Informationssystem (SIS) oder das Zollinformationssystem (ZIS).

Sofern Dänemark, Irland und das Vereinigte Königreich nicht an der Richtlinie (EU) 2016/680 teilnehmen (siehe Erwägungsgründe 99 und 100), sind sie wie Drittstaaten zu behandeln, siehe bereits die Anmerkungen zum Abschnitt 2 IRG-E. Für Dänemark ist entscheidend, ob ein Beschluss nach Artikel 4 Absatz 1 Satz 1 Protokoll Nummer 22 vorliegt. Für Irland und das Vereinigte Königreich gelten die Bestimmungen der Richtlinie (EU) 2016/680 nach Artikel 6a Protokoll Nummer 21, soweit die beiden Staaten durch Vorschriften zur justiziellen und polizeilichen Zusammenarbeit gebunden sind. Für das Vereinigte Königreich ist in diesem Zusammenhang die Vornahme eines generellen Opt-out und eines partiellen Opt-back-in nach Artikel 10 Absatz 4 Protokoll Nummer 36 in 2014 zu beachten, solange eine Mitgliedschaft in der Europäischen Union besteht. Im Rahmen der anwendbaren Zusammenarbeitsvorschriften müssen auch die Vorgaben der Richtlinie (EU) 2016/680 von Irland und dem Vereinigten Königreich eingehalten werden. Darüber hinaus werden beide Staaten wie Drittstaaten behandelt.

### **Zu Absatz 2**

Die Schengen-assoziierten Staaten Island, Norwegen, Schweiz und Liechtenstein stehen den Mitgliedstaaten der Europäischen Union bei der Anwendung dieses Teils gleich. Die Gleichstellung erfolgt mit Blick auf die Erwägungsgründe 101 bis 103 der Richtlinie (EU) 2016/680.

### **Zu Absatz 3**

Die Vorschrift bestimmt, dass die Regelungen in Abschnitt 2 des Siebten Teils IRG-E gelten, soweit im Elften Teil des IRG-E keine besonderen Regelungen getroffen werden. Der Elfte Teil sieht insgesamt verhältnismäßig wenig datenschützende Sondervorschriften für den Rechtshilfeverkehr innerhalb der Europäischen Union vor. Im Übrigen gilt der Datenschutzstandard, der auch für den Rechtshilfeverkehr mit Drittstaaten sowie mit internationalen Organisationen zur Anwendung kommt. Beispielsweise sollen das Zustimmungserfordernis aus § 77d Absatz 1 Nummer 3 IRG-E und die Verantwortlichkeitsregelung aus § 77d Absatz 5 Satz 1 IRG-E, die nach der Richtlinie (EU) 2016/680 nur für den Rechtshilfeverkehr mit Drittstaaten oder internationalen Organisationen eingreifen, auch im Rechtshilfeverkehr innerhalb der Europäischen Union gelten. Siehe hierzu auch die Anmerkungen zu § 97b IRG-E.

### **Zu § 97b (Übermittlung personenbezogener Daten)**

Die Vorschrift modifiziert die in § 77d IRG-E vorgesehenen Vorschriften zur Datenübermittlung für den Datenaustausch innerhalb der Europäischen Union. Die Modifizierung besteht darin, dass auf bestimmte datenschützende Voraussetzungen des § 77d IRG-E verzichtet werden kann, weil innerhalb der Europäischen Union ein angemessener Datenschutzstandard vorausgesetzt wird.

Nach Nummer 1 ist die Anwendung von § 77d Absatz 1 Nummer 2 IRG-E ausgeschlossen, der eine Datenübermittlung grundsätzlich nur an die zuständigen Stellen zulässt und für eine Datenweiterleitung an andere als die zuständigen Stellen enge Voraussetzungen vorsieht (durch einen Verweis auf Absatz 3). Die begrenzende Norm findet damit im Rechtshilfeverkehr innerhalb der Europäischen Union keine Anwendung. Daraus folgt freilich nicht, dass personenbezogene Daten innerhalb der Europäischen Union ohne jede Einschränkung übermittelt werden dürften. Es gelten insoweit insbesondere die allgemeinen innerstaatlichen Befugnisnormen und Verwendungsbestimmungen sowie auch die weiteren Voraussetzungen des § 77d IRG-E. Als Folgeänderung zum Ausschluss von

Absatz 1 Nummer 2 wird zudem auch die Anwendung von § 77d Absatz 3 IRG-E sowie von § 77e Absatz 1 Nummer 7 ausgeschlossen.

Nummer 2 schließt die Anwendung von § 77 Absatz 1 Nummer 4 IRG-E sowie auch den darauf Bezug nehmenden § 77f IRG-E aus, wonach eine Datenübermittlung nur zulässig ist, wenn der Empfängerstaat oder die empfangende Einrichtung über ein angemessenes Datenschutzniveau verfügt, geeignete datenschützende Garantien vorliegen oder einer der in § 77f Absatz 2 IRG-E genannten Ausnahmefälle einschlägig ist. Innerhalb der Europäischen Union wird das Bestehen eines angemessenen Datenschutzniveaus vorausgesetzt.

§ 77d Absatz 1 Nummer 3 IRG-E, der die Weiterleitung von „Fremddaten“ von der vorherigen Zustimmung des Staates oder der internationalen Einrichtung abhängig macht, von dem beziehungsweise der die Daten ursprünglich stammen, bleibt auch im Rechtshilfeverkehr innerhalb der Europäischen Union anwendbar. Zwar sieht die Richtlinie (EU) 2016/680 – anders als noch der Rb Datenschutz – ein solches Zustimmungserfordernis bei Daten, die aus einem anderen Mitgliedstaat der Europäischen Union oder einer europäischen Einrichtung stammen und an einen anderen Mitgliedstaat der Europäischen Union oder an eine andere europäische Einrichtung weitergeleitet werden, nicht mehr vor. In der bisherigen Rechtspraxis wird aber in Fällen der Datenweiterleitung regelmäßig eine Zustimmung der datenführenden Stelle eingeholt, siehe die Anmerkungen zu § 77d Absatz 1 Nummer 3 IRG-E. Hinter diesen datenschützenden Standard soll nicht zurückgegangen werden. Die Richtlinie (EU) 2016/680 lässt dies gemäß ihrem Artikel 1 Absatz 3 zu.

#### **Zu § 97c (Prüf-, Informations- und Protokollierungspflichten der übermittelnden Stelle)**

In Umsetzung von Artikel 30 Absatz 6 der Richtlinie (EU) 2016/680 wird eine spezielle Unterrichtungspflicht vorgesehen, die im Falle von Datenschutzverletzungen im Sinne von Artikel 30 Absatz 1 der Richtlinie (EU) 2016/680 in der Bundesrepublik Deutschland eingreift. Hierüber ist die Stelle eines anderen Mitgliedstaates der Europäischen Union, von der die betroffenen personenbezogenen Daten stammen oder an die diese Daten übermittelt wurden, unverzüglich zu unterrichten. Die Norm verweist bezüglich der Frage, welche Informationen dann im Einzelnen zu übermitteln sind, § 65 Absatz 3 Bundesdatenschutzgesetz, durch den der in Artikel 30 Absatz 6 der Richtlinie (EU) 2016/680 in Bezug genommene Artikel 30 Absatz 3 der Richtlinie (EU) 2016/680 umgesetzt wurde. Die zusammenhängende Darstellung aller Prüf-, Informations- und Unterrichtungspflichten im IRG erleichtern der Rechtspraxis die Handhabung.

Im Übrigen gelten die Anforderungen von § 77e IRG-E auch für den Rechtshilfeverkehr innerhalb der Europäischen Union. Insbesondere kommen der Hinweis auf die Zweckbindung nach § 77e Absatz 1 Nummer 3 IRG-E, das Zustimmungserfordernis vor Datenweiterleitung nach § 77e Absatz 1 Nummer 4 IRG-E und der Hinweis auf die einzuhaltenden Bedingungen nach § 77e Absatz 1 Nummer 5 IRG-E zur Anwendung. Dies ist in der Richtlinie (EU) 2016/680 zwar so nicht ausdrücklich vorgesehen, ein strengeres Datenschutzniveau ist gemäß ihrem Artikel 1 Absatz 3 aber nicht ausgeschlossen. Der Ansatz verstößt auch nicht gegen den Gleichbehandlungsgrundsatz aus Artikel 9 Absatz 4 der Richtlinie (EU) 2016/680, wonach anderen Mitgliedstaaten oder Einrichtungen der Europäischen Union keine Bedingungen gestellt werden dürfen, die nicht auch für entsprechende Datenübermittlungen innerhalb des eigenen Mitgliedstaates gelten. Auch innerhalb der Bundesrepublik Deutschland ist bei der Verwendung von personenbezogenen Daten eine Zweckänderung nur im Einzelfall und unter bestimmten Voraussetzungen zulässig, die in den nationalen Verfahrensordnungen ausdrücklich geregelt werden. Da die zuständigen Behörden anderer Mitgliedstaaten der Europäischen Union oder Einrichtun-

gen der Europäischen Union diese Voraussetzungen nicht kennen können und an das deutsche Recht zudem nicht gebunden sind, ist es Aufgabe der übermittelnden deutschen Stelle, die Einhaltung begrenzender nationaler Vorschriften sicherzustellen. Dies wird über das Zustimmungserfordernis sichergestellt. Entsprechendes gilt hinsichtlich der einzuhaltenden Bedingungen.

#### **Zu Nummer 6 (bisheriger Elfter Teil wird Zwölfter Teil)**

Durch Einfügung des neuen Elften Teils wird der bisherige Elfte Teil nunmehr der Zwölfte Teil.

#### **Zu Artikel 19 (Änderung des Fünften Gesetzes zur Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen)**

Der Artikel enthält Folgeänderungen, die durch die in Artikel 18 geregelten Änderungen des Gesetzes über die internationale Rechtshilfe in Strafsachen erforderlich werden. Diese betreffen im Wesentlichen die Einfügung eines weiteren Teils (Elfter Teil). Durch die Anpassungen des Fünften Gesetzes zur Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen vom 1. Juni 2017 (BGBl. I S. 1414) wird sichergestellt, dass dieses bei seinem (künftigen) Inkrafttreten anwendbar bleibt.

#### **Zu Artikel 20 (Änderung der Eurojust-Anlaufstellen-Verordnung)**

Bei der Änderung von § 2 Absatz 3 Satz 2 handelt es sich im Wesentlichen um eine redaktionelle Anpassung. Der bisherige Verweis in § 2 Absatz 3 Satz 2 der Eurojust-Anlaufstellen-Verordnung auf den bisherigen § 9 BDSG wird ersetzt. Stattdessen wird jetzt auf § 64 BDSG (2018) verwiesen, der dieselbe Funktion erfüllt wie der bisherige § 9 BDSG nebst dessen Anlage. Die Regelung hat – wie bisher – einen ausschließlich klarstellenden Charakter. Der Generalbundesanwalt beim Bundesgerichtshof ist weiterhin auch an andere datenschützende Normen als den § 64 BDSG (2018) gebunden.

Bei der Anpassung von § 5 Absatz 1 handelt es sich um eine Folgeänderung zu den Anpassungen innerhalb der StPO. Da § 489 Absatz 1 Satz 1 und Absatz 2 Satz 1 StPO mit Blick auf die vorrangig eingreifenden allgemeinen Regelungen des BDSG (2018) zu Berichtigungs- und Löschungszwecken entfallen, erübrigt sich ein entsprechender Verweis. Erforderlich bleibt der Verweis damit lediglich im Hinblick auf § 489 Absatz 1 Nummer 3 StPO-E, der über denselben Regelungsinhalt wie der bisherige § 489 Absatz 2 Satz 2 Nummer 3 StPO verfügt. Da § 491 StPO-E nicht mehr in verschiedene Absätze aufgeteilt ist, war auch der entsprechende Verweis anzupassen.

#### **Zu Artikel 21 (Änderung des Auslandsunterhaltsgesetzes)**

§ 19 Absatz 2 des Gesetzes zur Geltendmachung von Unterhaltsansprüchen im Verkehr mit ausländischen Staaten vom 23. Mai 2011 (BGBl. I S. 898) (Auslandsunterhaltsgesetz – AUG) regelt bisher die Löschung von Daten durch das Bundesamt für Justiz, soweit dieses als zentrale Behörde im Bereich des Auslandsunterhaltes tätig wird. Im Einzelnen werden die Voraussetzungen der Löschung und das bei der Löschung zu beachtende Verfahren geregelt. Dies ist nun in den Artikeln 17 und 18 der Datenschutz-Grundverordnung erfasst. § 19 Absatz 2 AUG ist daher als gegenstandslos aufzuheben.

Die Änderung des Absatzes 1 der Bestimmung und die Neufassung der Überschrift sind notwendige redaktionelle Folgeänderungen.



## **Zu Artikel 22 (Änderung des Bürgerlichen Gesetzbuchs – BGB)**

### **Zu Nummer 1 (Änderung von § 55a Absatz 1 Satz 2 BGB)**

Es handelt sich um eine Folgeänderung zur Änderung von § 126 Absatz 1 Satz 2 Nummer 3 GBO. Die dort bislang benannte Anlage wird mit dem vorliegenden Gesetz aufgehoben. An ihrer Stelle wird deklaratorisch auf diejenigen Bestimmungen der Datenschutz-Grundverordnung hingewiesen, die die notwendigen technisch-organisatorischen Maßnahmen regeln.

### **Zu Nummer 2 (Einfügung von § 79a BGB)**

Die Pflichten und Rechte nach den Artikeln 12 bis 22 der Datenschutz-Grundverordnung wurden durch § 10a des Handelsgesetzbuchs (HGB), der mit Artikel 7 des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017 (BGBl. I S. 2541) eingefügt wurde und am 25. Mai 2018 in Kraft treten wird, für das Handelsregister, das Genossenschaftsregister und Partnerschaftsregister beschränkt. Damit wurde von der Möglichkeit nach Artikel 23 der Datenschutz-Grundverordnung Gebrauch gemacht, wonach die Pflichten und Rechte gemäß den Artikeln 12 bis 22 im Wege von Gesetzgebungsmaßnahmen beschränkt werden können, sofern dies der Sicherstellung eines der in Artikel 23 Absatz 1 Buchstabe a bis j genannten Schutzzwecke dient.

### **Zu § 79a des Bürgerlichen Gesetzbuches in der Entwurfsfassung (BGB-E)**

Dieselben Beschränkungen, die für die Handels-, Genossenschafts- und Partnerschaftsregister getroffen wurden, sind auch für das Vereinsregister zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses gemäß Artikel 23 Absatz 1 Buchstabe e erforderlich. Ein funktionsfähiges und verlässliches Vereinsregister mit Publizitätswirkung ist für die Sicherheit und Leichtigkeit des Rechtsverkehrs unerlässlich. Das Vereinsregister dient der verlässlichen Information über Vereine und über die Personen, die Vereine im Rechtsverkehr organschaftlich vertreten können. Der Erwägungsgrund 73 der Datenschutz-Grundverordnung nennt im Zusammenhang mit möglichen Beschränkungen ausdrücklich das Führen öffentlicher Register als allgemeines öffentliches Interesse im Sinne des Artikels 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung. Die vorgesehenen Beschränkungen achten den Wesensgehalt der Grundrechte und Grundfreiheiten und stellen eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme im Sinne des Artikels 23 Absatz 1 der Datenschutz-Grundverordnung dar. Sie führen zu einem angemessenen Ausgleich zwischen dem Interesse der Allgemeinheit an einem sicheren und leichten Rechtsverkehr und dem Recht des Einzelnen auf Schutz seiner personenbezogenen Daten. Dabei ist zu berücksichtigen, dass bereits bei der Erhebung der Daten für das Vereinsregister der Grundsatz der Datensparsamkeit beachtet wird. Personenbezogene Daten werden für das Vereinsregister nur über die Personen erhoben und im Register gespeichert, die Mitglieder von Organen des Vereins und aufgrund ihrer Organstellung zur Vertretung des Vereins berechtigt sind. Erhoben werden nur der Name, das Geburtsdatum und der Wohnort der vertretungsberechtigten Personen.

#### **Zu Absatz 1**

Mit § 79a Absatz 1 Satz 1 BGB-E wird das Auskunftsrecht der betroffenen Person nach Artikel 15 der Datenschutz-Grundverordnung für das Vereinsregister und die dazu geführten Registerakten auf die in § 79 BGB und der Vereinsregisterverordnung vorgesehenen Rechte zur Einsicht ins Vereinsregister und die Registerakten sowie den Abruf der Daten aus dem Vereinsregister und den Registerakten über das Registerportal der Länder beschränkt. Die Erfüllung des unbeschränkten Auskunftsrechts nach Artikel 15 Absatz 1 der Datenschutz-Grundverordnung ist für die Vereinsregistergerichte mit vertretbarem Aufwand nicht möglich. Das Vereinsregister besteht aus den Registerblättern für die einge-

tragenen Vereine. Die Registerakten werden zu den einzelnen Registerblättern geführt. Im Vereinsregister kann nach Vereinen gesucht werden, nicht nach natürlichen Personen, zu denen personenbezogene Daten im Register eingetragen sind oder in den Registerakten vorhanden sind. Dasselbe gilt für eine Suche über das Registerportal der Länder.

Den betroffenen Personen sind die Eintragungen im Vereinsregister bekannt, da sie regelmäßig selbst den Antrag zur Eintragung gestellt haben oder daran mitgewirkt haben. Die betroffenen Personen kennen auch den Verein, auf dessen Registerblatt ihre personenbezogenen Daten zu finden sind. Sie können sich über die von ihnen im Vereinsregister gespeicherten personenbezogenen Daten so durch Einsicht im Vereinsregister beim zuständigen Registergericht oder durch Abruf aus dem Registerportal jederzeit schnell und einfach informieren. Für die Vereinsregistergerichte würde demgegenüber die Erfüllung der Pflicht nach Artikel 15 Absatz 3 der Datenschutz-Grundverordnung jeder Person zu bestätigen, ob von ihr personenbezogene Daten im Vereinsregister oder den Registerakten gespeichert sind, einen unverhältnismäßigen Suchaufwand erfordern, weil dem Registergericht eine Personensuche im Vereinsregister oder den Registerakten nicht möglich ist.

§ 79a Absatz 1 Satz 2 BGB-E entspricht inhaltlich § 11a Absatz 1 Satz 2 HGB. Mit der Vorschrift wird klargestellt, dass die Vereinsregistergerichte nicht verpflichtet sind, Personen, deren personenbezogene Daten im Register oder den Registerakten gespeichert sind, Auskunft darüber zu erteilen, wem die Daten offengelegt wurden. Das ist von den registerrechtlichen Einsichts- und Abrufrechten nicht umfasst, auf die das Recht aus Artikel 15 der Datenschutz-Grundverordnung beschränkt wird. Das Vereinsregister und die Registerakten können von jedermann eingesehen oder abgerufen werden, ohne dass in jedem Fall eine Registrierung der Nutzer stattfindet, so dass eine solche Auskunft nicht gegeben werden könnte, ohne dass personenbezogene Daten von jeder Person, die das Vereinsregister einsieht oder Daten aus dem Vereinsregister abrufen, erhoben und gespeichert werden müssten.

### **Zu Absatz 2**

Das Recht der betroffenen Person auf Berichtigung ihrer personenbezogenen Daten nach Artikel 16 der Datenschutz-Grundverordnung wird nach den Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) und der Vereinsregisterverordnung gewährt. Die Berichtigung des Vereinsregisters ist nur im registerrechtlichen Verfahren durch das Registergericht möglich, wenn die Voraussetzungen des § 395 FamFG für eine Löschung oder die Berichtigung nach § 12 Vereinsregisterverordnung (VRV) vorliegen. Die materiell-rechtliche Publizitätswirkung schließt ein Löschen im Sinne des Unkenntlichmachens von Daten aus. Ein Recht auf Löschung nach Artikel 17 Absatz 1 der Datenschutz-Grundverordnung besteht nicht, da die Ausschlussstatbestände nach Artikel 17 Absatz 3 Buchstabe b und e der Datenschutz-Grundverordnung vorliegen. Das Vereinsregister kann seinen Zweck nur erfüllen, wenn dauerhaft aus dem Vereinsregister ersichtlich ist, über welchen Zeitraum welche Eintragungen im Register veröffentlicht waren, auf die der Rechtsverkehr vertrauen konnte, unabhängig davon, ob sie richtig oder unrichtig waren. Dasselbe gilt für die Registerakten, in denen die Dokumente enthalten sind, die die Grundlagen für die Eintragungen ins Vereinsregister bilden. Die Berichtigung von personenbezogenen Daten, die in den zum Register einzureichenden Dokumenten enthalten sind, wird dadurch bewirkt, dass ein zu berichtendes Dokument beim Registergericht neu eingereicht wird.

### **Zu Absatz 3**

Für Eintragungen im Vereinsregister gilt der Grundsatz der Erhaltung der Eintragung, welche den Kern des materiell-rechtlichen Publizitätsprinzips bildet. Diese wird unter anderem dadurch geschützt, dass Eintragungen gemäß § 383 Absatz 3 FamFG nicht mit der

Beschwerde anfechtbar sind (Keidel-Heinemann, FamFG, § 395 Rn.1). Es würde dem Kern des Grundsatzes der Publizitätswirkung widersprechen, sollten Eintragungen über einen längeren Zeitraum nicht einsehbar sein. Die Aufrechterhaltung der Leichtigkeit des Rechts- und Wirtschaftsverkehrs durch uneingeschränkt einsehbare Register ist im allgemeinen öffentlichen Interesse. Ein Widerspruch der betroffenen Person gemäß Artikel 21 der Datenschutz-Grundverordnung, der zu einer Einschränkung der Verarbeitung von Registerdaten führen könnte, wird deshalb durch § 79a Absatz 3 BGB-neu auf der Grundlage des Artikels 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung ausgeschlossen. Auch insoweit bleibt es bei den registerrechtlichen Vorschriften über die Löschung und Berichtigung.

Weitere nicht mit der Funktion der Register vereinbare Rechte und Pflichten aus den Artikeln 13 ff. der Datenschutz-Grundverordnung bestehen im Bereich des Vereinsregisters ebenso wie bei den Handels-, Genossenschafts- und Partnerschaftsregistern nicht (Bundestagsdrucksache 18/12611 Seite 75), weil in der Datenschutz-Grundverordnung vorgesehene Ausnahmen für die Registerführung greifen. Die Informationspflichten nach Artikel 14 Absatz 1 bis 4 der Datenschutz-Grundverordnung bestehen für die registerführenden Gerichte bei Anmeldungen zum Vereinsregister bzw. Eintragungen ins Vereinsregister nicht, da insoweit der Ausnahmetatbestand in Artikel 14 Absatz 5 Buchstabe c der Datenschutz-Grundverordnung greift.

Ein Recht der betroffenen Person auf Löschung von Daten, die im Vereinsregister oder in den Registerakten gespeichert sind, kann nach Artikel 17 Absatz 1 der Datenschutz-Grundverordnung gegenüber dem registerführenden Gericht nicht geltend gemacht werden, da die Daten im Register und den Registerakten zur Wahrnehmung einer Aufgabe im öffentlichen Interesse gespeichert werden, so dass nach Artikel 17 Absatz 3 Buchstabe b der Datenschutz-Grundverordnung ein Recht auf Löschung nicht besteht.

Eine Beschränkung des Rechts der betroffenen Person auf Einschränkung der Verarbeitung nach Artikel 18 Absatz 1 der Datenschutz-Grundverordnung ist nicht erforderlich. Die Verarbeitung personenbezogener Daten im Vereinsregister oder den Registerakten ist auch wenn das Recht geltend gemacht wird, nach Artikel 18 Absatz 2 der Datenschutz-Grundverordnung weiterhin uneingeschränkt möglich. Das Führen des Vereinsregisters ist ein wichtiges öffentliches Interesse (vgl. auch Erwägungsgrund 73 der Datenschutz-Grundverordnung), so dass die Datenverarbeitung nicht eingeschränkt werden muss.

Die registerführenden Gerichte haben auch nicht die Mitteilungspflichten nach Artikel 19 der Datenschutz-Grundverordnung, da die Erfüllung dieser Pflichten stets mit einem unverhältnismäßigen Aufwand verbunden wäre. Personenbezogene Daten, die im Vereinsregister eingetragen sind, werden täglich von einer Vielzahl von Personen eingesehen oder abgerufen. Das registerführende Gericht oder das Registerportal kann derzeit nicht feststellen, welche Personen bestimmte personenbezogene Daten aus dem Vereinsregister eingesehen oder abgerufen haben. Dafür müssten zusätzlich personenbezogene Daten erhoben und ggf. über sehr lange Zeit gespeichert werden. Dies wäre mit einem unverhältnismäßigen Eingriff in das Persönlichkeitsrecht der Personen verbunden, die Vereinsregister einsehen oder Daten aus Vereinsregistern abrufen. Für die registerführenden Gerichte sowie den Betreiber des Registerportals, über das die Vereinsregisterdaten abgerufen werden können, würde dies zudem einen erheblichen zusätzlichen Verwaltungsaufwand bedeuten, der außer Verhältnis zu dem Nutzen einer Mitteilungspflicht stünde. Jedermann kann sich einfach über den aktuellen Inhalt des Vereinsregisters informieren und niemand kann sich darauf verlassen, dass sich der Registerinhalt nicht ändert. Zudem sind Änderungen von Eintragungen im Vereinsregister für Personen, die die Eintragungen zu einem Verein vor einer Änderung eingesehen oder abgerufen haben, nicht von Interesse, wenn sie keine Rechts- oder Geschäftsbeziehungen zu dem Verein unterhalten.

Ein Recht nach Artikel 20 Absatz 1 der Datenschutz-Grundverordnung besteht nicht, da das Führen der Vereinsregister und der Registerakten nach Artikel 20 Absatz 3 Satz 2 für die Wahrnehmung einer öffentlichen Aufgabe erforderlich ist.

### **Zu Nummer 3 (Änderung von § 1563 BGB)**

Dieselben Beschränkungen, die für die Handels-, Genossenschafts- und Partnerschaftsregister im Rahmen des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017 (BGBl. I S. 2541) getroffen wurden und die Nummer 1 für das Vereinsregister vorsieht, sind auch für das Güterrechtsregister zum Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses gemäß Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung erforderlich.

In das Güterrechtsregister werden insbesondere abweichende Vereinbarungen von Ehegatten zum gesetzlichen Güterstand der Zugewinnngemeinschaft eingetragen. Eintragungen im Güterrechtsregister bewirken, dass ein Dritter die eingetragenen Tatsachen im Geschäftsverkehr gegen sich gelten lassen muss (§ 1412 BGB). Auch diese Eintragungen dienen damit der Sicherheit und Vereinfachung des Rechtsverkehrs sowie der Information der Geschäftspartner der Ehegatten.

Wie zu Nummer 1 bereits ausgeführt, nennt Erwägungsgrund 73 der Datenschutz-Grundverordnung im Zusammenhang mit möglichen Beschränkungen ausdrücklich das Führen öffentlicher Register als allgemeines öffentliches Interesse im Sinne des Artikels 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung.

Die vorgesehenen Beschränkungen achten auch für das Güterrechtsregister den Wesensgehalt der Grundrechte und Grundfreiheiten und stellen eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme im Sinne des Artikels 23 Absatz 1 der Datenschutz-Grundverordnung dar. Sie führen zu einem angemessenen Ausgleich zwischen dem Interesse der Allgemeinheit an einem sicheren und leichten Rechtsverkehr und dem Recht des Einzelnen auf Schutz seiner personenbezogenen Daten. Dabei ist zu berücksichtigen, dass bereits bei der Erhebung der Daten für das Güterrechtsregister der Grundsatz der Datensparsamkeit beachtet wird. Personenbezogene Daten werden grundsätzlich nur auf Antrag der betreffenden Personen erhoben und nur in einem dem Antrag entsprechenden Umfang im Register gespeichert.

### **Zu Buchstabe a**

Da die Vorschrift um einen neuen Regelungsgehalt ergänzt wird, ist die Überschrift anzupassen.

### **Zu Buchstabe b**

Es handelt sich um eine redaktionelle Änderung.

### **Zu Buchstabe c**

### **Zu Absatz 2**

Mit § 1563 Absatz 2 Satz 1 BGB-E wird das Auskunftsrecht der betroffenen Person nach Artikel 15 der Datenschutz-Grundverordnung für das Güterrechtsregister und die dazu geführten Registerakten auf die in Absatz 1 der Vorschrift vorgesehenen Rechte zur Einsicht in das Register und die Registerakten beschränkt. Wie bereits zum Vereinsregister dargelegt ist die Erfüllung des unbeschränkten Auskunftsrechts nach Artikel 15 Absatz 1 der Datenschutz-Grundverordnung für die Registergerichte mit vertretbarem Aufwand nicht möglich. Das Einsichtsrecht ist daher nach Artikel 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung einzuschränken. Erwägungsgrund 73 der Datenschutz-

Grundverordnung erwähnt im Zusammenhang mit möglichen Beschränkungen ausdrücklich das Führen öffentlicher Register als allgemeines öffentliches Interesse im Sinne dieses Artikels.

Das Güterrechtsregister besteht aus den Registerblättern für die jeweiligen Eintragungen eines Ehepaares, teilweise wird das Register noch in Buchform geführt. Ergänzend werden Registerakten zu den einzelnen Registerblättern bzw. Eintragungen in den Büchern geführt. In das Güterrechtsregister werden grundsätzlich nur solche Daten der betroffenen Ehepartner eingetragen, die von diesen in ihrem gemeinsamen Antrag zur Verfügung gestellt werden. § 1561 Absatz 2 BGB sieht wenige Ausnahmen vor, in denen ein Ehepartner die Eintragung allein beantragen kann und dabei Daten seines Partners angibt. Zumeist handelt es sich dabei um die Wiederholung einer früher gemeinsam beantragten Eintragung in einem anderen Amtsgerichtsbezirk oder um die Eintragung einer Vereinbarung aus einem Ehevertrag oder einer gerichtlichen Entscheidung zum Güterstand (Ziffer 1 und 2). Darüber hinaus gibt es nur wenige Fälle, in denen ein Partner einseitig eine Eintragung ins Güterrechtsregister beantragen kann und in diesem Zusammenhang auch Daten des anderen Partners angibt. Dies betrifft lediglich die in der Praxis kaum mehr relevanten Fälle eines Widerspruchs gegen den selbständigen Betrieb eines Erwerbsgeschäfts durch den anderen Ehegatten oder die Beschränkung bzw. Ausschließung der Berechtigung des anderen Partners, Geschäfte mit Wirkung für den Antragsteller zu besorgen nach § 1357 Absatz 2 BGB. Über alle Eintragungen und ihren Inhalt werden beide Ehepartner informiert. Unabhängig hiervon können sich die Ehepartner über die im Güterrechtsregister gespeicherten sie betreffenden personenbezogenen Daten durch Einsicht in das Register beim zuständigen Registergericht jederzeit schnell und einfach vergewissern.

§ 1563 Absatz 2 Satz 2 BGB-E entspricht inhaltlich § 11a Absatz 1 Satz 2 HGB und dem unter Nummer 1 vorgesehenen § 79a Absatz 1 Satz 1 BGB-E. Mit der Vorschrift wird klargestellt, dass die für die Führung des Güterrechtsregisters zuständigen Gerichte nicht verpflichtet sind, Personen, deren personenbezogene Daten im Register oder den Registerakten gespeichert sind, Auskunft darüber zu erteilen, wem die Daten offengelegt wurden. Das ist von den registerrechtlichen Einsichts- und Abrufrechten nicht umfasst, auf die das Recht aus Artikel 15 der Datenschutz-Grundverordnung beschränkt wird. Das Güterrechtsregister und die Registerakten können von jedermann eingesehen werden, ohne dass in jedem Fall eine Registrierung der Nutzer erforderlich ist. Eine solche Auskunft könnte daher nicht erfolgen, ohne dass personenbezogene Daten von jeder Person, die das Güterrechtsregister einsieht, erhoben und gespeichert werden müssten. Im Übrigen streben die Betroffenen mit der – freiwilligen – Eintragung in das Güterrechtsregister gerade die möglichst breite Publikation ihrer vom gesetzlichen Güterstand abweichenden Vereinbarungen an Dritte an, um eine umfassende Schutzwirkung nach § 1412 BGB zu erreichen.

### **Zu Absatz 3**

Absatz 3 sieht vor, dass auf das Güterrechtsregister darüber hinaus die Vorschriften des § 79a Absatz 2 und 3 BGB-E entsprechend angewandt werden.

Die Berichtigung des Güterrechtsregisters ist – wie die des Vereinsregisters – nur im registerrechtlichen Verfahren durch das Registergericht möglich, wenn die Voraussetzungen des § 395 FamFG für eine Löschung vorliegen. Das Recht auf Berichtigung nach Artikel 16 der Datenschutz-Grundverordnung wird daher nach den Vorschriften des FamFG gewährt.

Auch für das Güterrechtsregister schließt die materiell-rechtliche Publizitätswirkung ein Löschen im Sinne des Unkenntlichmachens von Daten aus. Ein Recht auf Löschung nach Artikel 17 Absatz 1 der Datenschutz-Grundverordnung besteht daher ebenfalls nicht. Wie

das Vereinsregister kann das Güterrechtsregister seinen Zweck nur erfüllen, wenn dauerhaft aus dem Register ersichtlich ist, über welchen Zeitraum welche Eintragungen im Register veröffentlicht waren, auf die der Rechtsverkehr vertrauen konnte, unabhängig davon, ob sie richtig oder unrichtig waren. Dasselbe gilt für die Registerakten, in denen die Dokumente enthalten sind, die die Grundlagen für die Eintragungen ins Register bilden. Die Berichtigung von personenbezogenen Daten, die in den zum Register einzureichenden Dokumenten enthalten sind, wird ebenfalls dadurch bewirkt, dass ein zu berichtendes Dokument beim Registergericht neu eingereicht wird.

Des Weiteren gilt auch für Eintragungen im Güterrechtsregister der Grundsatz der Erhaltung der Eintragung. Ein Widerspruch gemäß Artikel 21 der Datenschutz-Grundverordnung, der zu einer Einschränkung der Verarbeitung von Registerdaten führen könnte, wird deshalb entsprechend der für das Vereinsregister geschaffenen Vorschrift des § 79a Absatz 3 BGB-E auf der Grundlage des Artikels 23 Absatz 1 Buchstabe e der Datenschutz-Grundverordnung ausgeschlossen. Auch für das Güterrechtsregister bleibt es bei den registerrechtlichen Vorschriften über die Löschung und Berichtigung.

Weitere nicht mit der Funktion der Register vereinbare Rechte und Pflichten aus den Artikeln 13 ff. der Datenschutz-Grundverordnung bestehen im Bereich des Güterrechtsregisters ebenso wie beim Vereinsregister nicht. Insoweit wird auf die auch für das Güterrechtsregister zutreffenden weiteren Ausführungen zu Nummer 1 verwiesen.

#### **Zu Artikel 23 (Änderung der Luftfahrzeugpfandrechtsregisterverordnung)**

Es handelt sich um eine Folgeänderung zur Änderung von § 126 Absatz 1 Satz 2 Nummer 3 GBO. Die dort bislang benannte Anlage wird mit dem vorliegenden Gesetz aufgehoben. An ihrer Stelle wird deklaratorisch auf diejenigen Bestimmungen der Datenschutz-Grundverordnung hingewiesen, die die notwendigen technisch-organisatorischen Maßnahmen regeln.

#### **Zu Artikel 24 (Folgeänderungen)**

##### **Zu Absatz 1 (Änderung des Bundespolizeigesetzes)**

Aufgrund der Neufassung von § 160 StPO-E ist der Verweis in § 28a Absatz 4 des Bundespolizeigesetzes anzupassen. Aus diesem Anlass erfolgt eine Anpassung an den Wortlaut der entsprechenden Regelung in § 16 Absatz 3 Satz 3 BKAG bzw. § 34 Absatz 4 Satz 3 des Bundeskriminalamtgesetzes in der durch das Gesetz zur Neustrukturierung des Bundeskriminalamtgesetzes vom 1. Juni 2017 (BGBl. I S. 1354) geänderten Fassung.

##### **Zu Absatz 2 (Änderung des Anti-Doping-Gesetzes)**

Es handelt sich um eine Folgeänderung anlässlich der Neufassung der §§ 477 bis 480 StPO-E, mit der die bisherigen Verweise entsprechend aktualisiert werden.

##### **Zu Absatz 3 (Änderung des IStGH-Gesetzes)**

Es handelt sich um eine Folgeänderung anlässlich der Neufassung der §§ 477 bis 480 StPO-E, mit der der bisherige Verweis entsprechend aktualisiert wird.

##### **Zu Absatz 4 (Änderung des Schwarzarbeitsbekämpfungsgesetzes)**

Es handelt sich um eine Folgeänderung anlässlich der Neufassung der §§ 477 bis 480 StPO-E, mit der der bisherige Verweis entsprechend aktualisiert wird.

**Zu Absatz 5 (Änderung des Gesetzes über Ordnungswidrigkeiten)**

Es handelt sich um eine Folgeänderung anlässlich der Neufassung der §§ 477 bis 480 StPO-E, mit der die bisherigen Verweise entsprechend aktualisiert werden. Die bisherigen Verweise auf den bisherigen § 480 StPO entfallen hierbei ersatzlos, da eine ausdrückliche Klarstellung innerhalb der StPO-E entbehrlich ist. Eine Änderung der Rechtslage ist hiermit weder für die StPO-E, noch für das Ordnungswidrigkeitengesetz in der Entwurfsfassung (OWiG-E) verbunden. Besondere gesetzliche Bestimmungen, die die Übermittlung personenbezogener Daten aus Bußgeldverfahren anordnen oder erlauben, bleiben daher auch nach den Anpassungen innerhalb der §§ 49a und 49b OWiG-E unberührt.

**Zu Absatz 6 (Änderung des ZIS-Ausführungsgesetzes)**

Es handelt sich um eine Folgeänderung anlässlich der Neufassung der §§ 477 bis 480 StPO-E, mit der der bisherige Verweis entsprechend aktualisiert wird.

**Zu Artikel 25 (Inkrafttreten)**

Die Regelung bestimmt, dass das Gesetz am 25. Mai 2018 in Kraft treten soll. Da auch die Neufassung des BDSG an diesem Tag in Kraft treten wird, ist damit ein vollständiger Gleichlauf der aufeinander aufbauenden Regelungen gewährleistet.