§ 26
Datenerhebung

(1) Die allgemeinen Ordnungsbehörden und die Polizei können personenbezogene Daten zur Erfüllung ihrer Aufgaben erheben, wenn

1. die Person in Kenntnis des Zwecks der Erhebung eingewilligt hat oder durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass die Erhebung im Interesse der Person liegt und sie in Kenntnis des Zwecks einwilligen würde,
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder
3. eine Rechtsvorschrift dies erlaubt.

(2) Die allgemeinen Ordnungsbehörden und die Polizei können personenbezogene Daten auch über andere als die in den §§ 4, 5 und 7 genannten Personen erheben, soweit dies

1. zur Gefahrenabwehr (§ 1 Abs. 1 Satz 1),
2. zum Schutz privater Rechte (§ 1 Abs. 3),
3. zur Abwehr von Gefahren durch den Straßenverkehr (§ 1 Abs. 5) oder
4. zur Erfüllung von durch andere Rechtsvorschriften übertragenen Aufgaben (§ 1 Abs. 2, § 9 Abs. 2)

erforderlich ist und die Befugnisse nicht durch dieses Gesetz oder eine andere Rechtsvorschrift gesondert geregelt sind. Die Polizei kann ferner personenbezogene Daten erheben, soweit dies zur Vollzugshilfe (§ 1 Abs. 4) erforderlich ist.

(3) Die Polizei kann personenbezogene Daten über

1. Personen, bei denen durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass sie zukünftig Straftaten begehen,
2. Personen, bei denen durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass sie Opfer von Straftaten werden,
3. Personen im Umfeld einer in besonderem Maß als gefährdet erscheinenden Person,
4. Zeugen, Hinweisgeber und sonstige Auskunftspersonen und
5. Kontakt- und Begleitpersonen,

erheben, soweit dies zur vorbeugenden Bekämpfung von Straftaten (§ 1 Abs. 1 Satz 3) erforderlich ist. Kontakt- und Begleitpersonen im Sinne dieses Gesetzes sind Personen, die

mit einer in Satz 1 Nr. 1 genannten Person in der Weise in Verbindung stehen, dass durch Tatsachen begründete Anhaltspunkte für ihren objektiven Tatbezug sprechen.

(4) Die allgemeinen Ordnungsbehörden und die Polizei können personenbezogene Daten über Personen erheben,

1. die für Anlagen oder Einrichtungen, von denen eine erhebliche Gefahr ausgehen kann, verantwortlich sind,
2. die für gefährdete Anlagen oder Einrichtungen verantwortlich sind,
3. die für Veranstaltungen in der Öffentlichkeit verantwortlich sind, oder
4. deren besondere Kenntnisse und Fähigkeiten zur Gefahrenabwehr benötigt werden,

soweit dies zur Vorbereitung auf die Gefahrenabwehr (§ 1 Abs. 1 Satz 2) erforderlich ist.

(5) Personenbezogene Daten sind offen und beim Betroffenen zu erheben. Sie können bei anderen öffentlichen oder nicht öffentlichen Stellen oder verdeckt erhoben werden, wenn die Erhebung beim Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder die Wahrnehmung ordnungsbehördlicher oder polizeilicher Aufgaben erschwert oder gefährdet würde.

§ 27
Datenerhebung durch den Einsatz technischer Mittel

(1) Die allgemeinen Ordnungsbehörden und die Polizei können personenbezogene Daten in öffentlich zugänglichen Räumen durch den offenen Einsatz technischer Mittel zur Bildübertragung erheben, soweit dies im Einzelfall zur Erfüllung einer Aufgabe nach § 1 Abs. 1 Satz 1 und 3 und Abs. 2 und 5 erforderlich ist. Eine Bildaufzeichnung ist in öffentlich zugänglichen Räumen nur zulässig, soweit dies im Einzelfall

1. zur Abwehr einer Gefahr,
2. zum Schutz gefährdeter öffentlicher Anlagen oder Einrichtungen,
3. zur Abwehr von Gefahren durch den Straßenverkehr oder
4. zur Wahrnehmung von durch andere Rechtsvorschriften übertragenen Aufgaben

erforderlich ist. Die Polizei kann in den Fällen des Satzes 2 Nr. 1 und 2 auch Tonaufzeichnungen anfertigen, wenn die polizeiliche Aufgabenwahrnehmung sonst erschwert oder gefährdet würde.

(2) Die Polizei kann bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, personenbezogene Daten von Teilnehmern durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen erheben, soweit Tatsachen die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit entstehen, insbesondere Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung begangen werden. Eine verdeckte Datenerhebung ist nur zulässig, soweit Tatsachen die Annahme rechtfertigen, dass durch die offene Datenerhebung Straftaten nicht verhindert, sondern lediglich an anderer Stelle, zu anderer Zeit oder auf andere Weise begangen werden.

(3) Die Polizei kann an den in § 10 Abs. 1 Satz 2 Nr. 1 genannten Orten und in den in § 10 Abs. 1 Satz 2 Nr. 2 genannten Objekten sowie in deren unmittelbarer Nähe personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen erheben, soweit Tatsachen die Annahme rechtfertigen, dass Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung begangen werden.

(4) Die Polizei kann in den Fällen des § 18 Abs. 2 Nr. 1 bis 7 in öffentlich zugänglichen Räumen personenbezogene Daten durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen erheben, soweit dies nach den Umständen zum Schutz eines Polizeibeamten oder eines Dritten erforderlich erscheint.

(5) Die Datenerhebung nach den Absätzen 1 bis 4 darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen sind. Die angefertigten Bild- und Tonaufzeichnungen sowie daraus gefertigte Unterlagen sind unverzüglich zu löschen oder zu vernichten, soweit diese nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung, zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten, oder zur Behebung einer bestehenden Beweisnot, erforderlich sind. Die Zweckänderung der Daten muss im Einzelfall festgestellt und dokumentiert werden.

(6) Auf den Umstand einer offenen Datenerhebung, die durchgehend länger als 48 Stunden durchgeführt werden soll, soll in geeigneter Weise hingewiesen werden, soweit dadurch nicht der Zweck der Maßnahme gefährdet wird.

(7) Die örtliche Ordnungsbehörde hat eine Datenerhebung nach Absatz 1 spätestens zwei Wochen vor deren Durchführung der Landesordnungsbehörde und dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit anzuzeigen. Für die Polizei besteht eine entsprechende Anzeigepflicht gegenüber dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit bei einer Datenerhebung nach den Absätzen 1 und 3.

§ 28
Besondere Mittel der verdeckten Datenerhebung

(1) Die Polizei kann personenbezogene Daten durch den Einsatz besonderer Mittel der verdeckten Datenerhebung nach Absatz 2 erheben über

1. die Verantwortlichen nach den §§ 4 und 5 und unter den Voraussetzungen des § 7 über die dort genannten Personen, soweit die Datenerhebung zur Abwehr einer Gefahr für Leib oder Leben erforderlich ist,
2. Personen, bei denen durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass sie zukünftig Straftaten von erheblicher Bedeutung begehen und die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist,
3. Kontakt- und Begleitpersonen (§ 26 Abs. 3 Satz 2), soweit die Datenerhebung zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist, und
4. Personen im Umfeld einer in besonderem Maß als gefährdet erscheinenden Person, soweit die Datenerhebung zur Abwehr der Gefahr erforderlich ist.

Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Besondere Mittel der verdeckten Datenerhebung im Sinne dieses Gesetzes sind

1. die planmäßig angelegte Beobachtung einer Person, die durchgehend länger als 24 Stunden oder über einen Zeitraum von mehr als einer Woche durchgeführt werden soll (längerfristige ~~Observation~~ Terrorisierung/Stalking),
2. der verdeckte Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen sowie zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes,
3. der Einsatz von Polizeibeamten unter einer ihnen auf Dauer angelegten Legende (verdeckte Ermittler),
4. der Einsatz von Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist (Vertrauenspersonen), und
5. der Einsatz technischer Mittel zur Feststellung des jeweiligen Standortes einer Person oder eines Fahrzeuges.

(3) Straftaten von erheblicher Bedeutung im Sinne dieses Gesetzes sind

1. Verbrechen und
2. Vergehen, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, soweit sie
   a) sich gegen Leib, Leben oder Freiheit einer Person oder bedeutende Sach- oder Vermögenswerte richten,
   b) auf den Gebieten des unerlaubten Waffen- oder Betäubungsmittelverkehrs, der Geld- und Wertzeichenfälschung oder des Staatsschutzes (§§ 74 a und 120 des Gerichtsverfassungsgesetzes) begangen werden, oder
   c) gewerbs-, gewohnheits-, serien- oder bandenmäßig oder sonst organisiert begangen werden.

(4) Die Datenerhebung nach Absatz 1 darf nur durch die Behördenleitung oder durch einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden. Sie ist zu befristen und kann wiederholt angeordnet werden. Bei Gefahr im Verzug können besondere Mittel nach Absatz 2 Nr. 2 und 5 vorläufig eingesetzt werden; eine Entscheidung nach Satz 1 ist unverzüglich nachzuholen. Der Einsatz besonderer Mittel nach Absatz 2 Nr. 2 bis 4, der länger als sieben Tage durchgeführt werden soll oder durchgeführt wird, bedarf [eigentlich] der richterlichen Entscheidung. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. § 21 Abs. 1 Satz 3 gilt entsprechend.

(5) Nach Absatz 1 erlangte personenbezogene Daten dürfen für einen anderen Zweck verwendet werden, soweit dies zur Verfolgung von Straftaten von erheblicher Bedeutung (Absatz 3), zur Abwehr einer dringenden Gefahr oder zur vorbeugenden Bekämpfung einer Straftat von erheblicher Bedeutung erforderlich ist. Die Zweckänderung der Daten muss im Einzelfall festgestellt und dokumentiert werden.

(6) Soweit es zur Geheimhaltung der wahren Identität des verdeckten Ermittlers erforderlich ist, dürfen entsprechende Urkunden hergestellt, verändert und gebraucht werden. Ein verdeckter Ermittler darf zur Erfüllung seines Auftrages unter Geheimhaltung seiner wahren Identität am Rechtsverkehr teilnehmen sowie mit Einverständnis des Berechtigten, nicht jedoch unter Vortäuschung eines Zutrittsrechts, dessen Wohnung betreten. Soweit es zur Geheimhaltung der Zusammenarbeit einer Vertrauensperson mit der Polizei erforderlich ist, gilt Satz 1 entsprechend.

§ 29
Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen

(1) Die Polizei kann personenbezogene Daten durch den verdeckten Einsatz technischer Mittel zur Datenerhebung nach § 28 Abs. 2 Nr. 2 in oder aus Wohnungen des Betroffenen zur Abwehr einer dringenden Gefahr für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, erheben über

1. die nach den §§ 4 und 5 Verantwortlichen und unter den Voraussetzungen des § 7 über die dort genannten Personen und
2. Kontakt- und Begleitpersonen (§ 26 Abs. 3 Satz 2), soweit die Datenerhebung zur Verhinderung von besonders schweren Straftaten nach Absatz 2 erforderlich ist.

Die Datenerhebung ist nur zulässig unter den in § 39 a Abs. 2 bezeichneten Voraussetzungen. Die Datenerhebung darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Besonders schwere Straftaten im Sinne dieses Gesetzes sind:

1. aus dem Strafgesetzbuch:
   a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates oder des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80, 81, 82, nach den §§ 94, 95 Abs. 3 und § 96 Abs. 1, jeweils auch in Verbindung mit § 97 b, sowie nach den §§ 97 a, 98 Abs. 1 Satz 2, § 99 Abs. 2 und den §§ 100, 100 a Abs. 4,
   b) Bildung krimineller Vereinigungen nach § 129 Abs. 1 in Verbindung mit Abs. 4 Halbsatz 2 und Bildung terroristischer Vereinigungen nach § 129 a Abs. 1, 2, 4, 5 Satz 1 Alternative 1, jeweils auch in Verbindung mit § 129 b Abs. 1,
   c) Geldfälschung und Wertpapierfälschung in den Fällen der §§ 146, 151, jeweils auch in Verbindung mit § 152, gewerbs- oder bandenmäßige Fälschung von Zahlungskarten, Schecks und Wechseln nach § 152 a Abs. 3 und Fälschung von Zahlungskarten mit Garantiefunktion und Vordrucken für Euroschecks nach § 152 b Abs. 1 bis 4,

d) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176 a Abs. 2 Nr. 2 oder Abs. 3, § 177 Abs. 2 Nr. 2 oder § 179 Abs. 5 Nr. 2,
e) Verbreitung, Erwerb und Besitz kinderpornografischer Schriften in den Fällen des § 184 b Abs. 3,
f) Mord und Totschlag nach §§ 211, 212,
g) Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234 a Abs. 1, 2, §§ 239 a, 239 b und Menschenhandel zum Zweck der sexuellen Ausbeutung und zum Zweck der Ausbeutung der Arbeitskraft nach § 232 Abs. 3, 4 oder Abs. 5, § 233 Abs. 3, jeweils soweit es sich um Verbrechen handelt,
h) Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244 a,
i) schwerer Raub nach § 250 Abs. 1 oder Abs. 2,
j) räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Abs. 4 Satz 2 genannten Voraussetzungen,
k) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260 a,
l) besonders schwerer Fall der Geldwäsche, Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 unter den in § 261 Abs. 4 Satz 2 genannten Voraussetzungen,
m) besonders schwerer Fall der Bestechlichkeit und Bestechung nach § 335 Abs. 1 unter den in § 335 Abs. 2 Nr. 1 bis 3 genannten Voraussetzungen,

2. aus dem Asylverfahrensgesetz:
a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,
b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84 a Abs. 1,

3. aus dem Aufenthaltsgesetz:
a) Einschleusen von Ausländern nach § 96 Abs. 2,
b) gewerbs- und bandenmäßiges Einschleusen nach § 97,

4. aus dem Betäubungsmittelgesetz:
a) besonders schwerer Fall einer Straftat nach § 29 Abs. 1 Satz 1 Nr. 1, 5, 6, 10, 11 oder 13 in Verbindung mit § 29 Abs. 3 Satz 2 Nr. 1,
b) eine Straftat nach §§ 29 a, 30 Abs. 1 Nr. 1, 2, 4, § 30 a,

5. aus dem Gesetz über die Kontrolle von Kriegswaffen:
a) eine Straftat nach § 19 Abs. 2 oder § 20 Abs. 1, jeweils auch in Verbindung mit § 21,
b) besonders schwerer Fall einer Straftat nach § 22 a Abs. 1 in Verbindung mit Abs. 2,

6. aus dem Völkerstrafgesetzbuch:
   a) Völkermord nach § 6,
   b) Verbrechen gegen die Menschlichkeit nach § 7,
   c) Kriegsverbrechen nach den §§ 8 bis 12,
7. aus dem Waffengesetz:
   a) besonders schwerer Fall einer Straftat nach § 51 Abs. 1 in Verbindung mit Abs. 2,
   b) besonders schwerer Fall einer Straftat nach § 52 Abs. 1 Nr. 1 in Verbindung mit Abs. 5.

(3) Die Datenerhebung nach Absatz 1 bedarf [eigentlich] der richterlichen Entscheidung. In der schriftlichen Anordnung sind insbesondere

1. Voraussetzungen und wesentliche Abwägungsgesichtspunkte,
2. soweit bekannt Name und Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,
3. Art, Umfang und Dauer der Maßnahme,
4. die Wohnung oder Räume, in oder aus denen die Daten erhoben werden sollen, und
5. die Art der durch die Maßnahme zu erhebenden Daten zu bestimmen.

Sie ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen.

(4) Das anordnende Gericht ist fortlaufend über den Verlauf, die Ergebnisse und die darauf beruhenden Maßnahmen zu unterrichten. Sofern die Voraussetzungen der Anordnung nicht mehr vorliegen, ordnet es die Aufhebung der Datenerhebung an.

(5) Nach Absatz 1 erlangte personenbezogene Daten sind besonders zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch die Empfänger aufrechtzuerhalten. Solche Daten dürfen für einen anderen Zweck verwendet werden, soweit dies zur

1. Verfolgung von besonders schweren Straftaten, die nach der Strafprozessordnung die Wohnraumüberwachung rechtfertigen,
2. Abwehr einer dringenden Gefahr im Sinne des Absatzes 1 erforderlich ist. Die Zweckänderung muss im Einzelfall festgestellt und dokumentiert werden.

(6) Werden technische Mittel ausschließlich zum Schutz der bei einem polizeilichen Einsatz in Wohnungen tätigen Personen verwendet, kann die Datenerhebung nach Absatz 1 durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden. Erkenntnisse aus einem solchen Einsatz dürfen für einen anderen Zweck zur Abwehr einer dringenden Gefahr oder zur Verfolgung von besonders schweren Straftaten, die nach der Strafprozessordnung die Wohnraumüberwachung rechtfertigen, verwendet werden, wenn zuvor die Rechtmäßigkeit der Maßnahme durch den Richter festgestellt wurde. Bei Gefahr im Verzug kann die Verwendung der Daten zu den in Satz 2 genannten Zwecken vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes zugelassen werden; die richterliche Entscheidung ist [eigentlich] unverzüglich nachzuholen.

(7) Zuständiges Gericht im Sinne dieser Vorschrift ist das Oberverwaltungsgericht Rheinland-Pfalz. Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung. Bei Gefahr im Verzug kann die Datenerhebung nach Absatz 1 durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden; die richterliche Entscheidung ist [eigentlich] unverzüglich nachzuholen.

(8) Die Landesregierung unterrichtet den Landtag jährlich über den erfolgten Einsatz technischer Mittel nach den Absätzen 1 und 7, soweit dieser einer richterlichen Anordnung bedarf. Die Parlamentarische Kontrollkommission übt [eigentlich] auf der Grundlage dieses Berichts die parlamentarische Kontrolle aus. § 20 Abs. 1 Satz 2, § 20 Abs. 2 bis 4 und § 21 Abs. 2 und 3 des Landesverfassungsschutzgesetzes gelten entsprechend.

§ 30
Datenerhebung bei Notrufen, Aufzeichnung von Anrufen

(1) Die allgemeinen Ordnungsbehörden und die Polizei können Anrufe über Notrufeinrichtungen aufzeichnen. Im Übrigen ist eine Aufzeichnung von Anrufen nur zulässig, soweit dies im Einzelfall zur Aufgabenerfüllung erforderlich ist; auf die Aufzeichnung soll hingewiesen werden, soweit dadurch die Aufgabenerfüllung nicht gefährdet wird.

(2) Die Polizei kann mit Einwilligung des Anschlussinhabers Anrufe aufzeichnen, soweit dies zur Abwehr einer erheblichen Gefahr erforderlich ist.

(3) Die Aufzeichnungen sind spätestens nach zwei Monaten zu löschen oder zu vernichten, soweit die weitere Speicherung oder Nutzung der personenbezogenen Daten zu einem der in § 33 genannten Zwecke nicht mehr erforderlich ist.

§ 31
Datenerhebung durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation, Auskunft über die Telekommunikation

(1) Die Polizei kann personenbezogene Daten durch den Einsatz technischer Mittel zur Überwachung und Aufzeichnung der Telekommunikation sowie durch Auskünfte über die Telekommunikation zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, erheben über

1. die nach den §§ 4 und 5 Verantwortlichen und unter den Voraussetzungen des § 7 über die dort genannten Personen oder
2. Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach den §§ 4 und 5 Verantwortlichen bestimmte oder von ihnen herrührende Mitteilungen entgegennehmen oder weitergeben.

Die Datenerhebung ist nur zulässig, soweit sie zwingend erforderlich ist und die Voraussetzungen des § 39 a Abs. 3 vorliegen. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Die Datenerhebung nach Absatz 1 kann sich auf die Inhalte der Telekommunikation und auf Verkehrsdaten beziehen. Die Erhebung von Verkehrsdaten kann sich auch auf Zeiträume vor deren Anordnung erstrecken.

(3) Zur Abwehr einer Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, darf die Überwachung und Aufzeichnung der Telekommunikation ohne Wissen der nach den §§ 4 und 5 Verantwortlichen oder der Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach den §§ 4 und 5 Verantwortlichen bestimmte oder von ihnen herrührende Mitteilungen entgegennehmen oder weitergeben, in der Weise erfolgen, dass mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und
2. der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.

Die Datenerhebung ist nur zulässig, soweit die Voraussetzungen des § 39 a Abs. 3 vorliegen. § 31 c Abs. 2 und 4 gilt entsprechend. Im Übrigen bleibt § 31 c unberührt.

(4) Die Datenerhebung bedarf [eigentlich] der richterlichen Entscheidung. In der schriftlichen Anordnung sind insbesondere

1. Voraussetzungen und wesentliche Abwägungsgesichtspunkte,
2. die Person, gegen die sich die Datenerhebung richtet, soweit möglich mit Name und Anschrift,
3. Art, Umfang und Dauer der Datenerhebung unter Benennung des Endzeitpunkts,
4. soweit möglich die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, und
5. im Fall des Absatzes 3 möglichst genau das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, sowie das technische Mittel

zu bestimmen. Die Maßnahme ist auf höchstens drei Monate, im Fall des Absatzes 3 auf höchstens zwei Monate, zu befristen. Eine Verlängerung um jeweils nicht mehr als denselben Zeitraum ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen.

(5) Zuständiges Gericht im Sinne dieser Vorschrift ist das Oberverwaltungsgericht Rheinland-Pfalz. Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung. Bei Gefahr im Verzug kann die Maßnahme vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden; die richterliche Entscheidung ist [eigentlich] unverzüglich nachzuholen.

(6) Aufgrund der Anordnung hat jeder, der geschäftsmäßig Telekommunikationsdienstleistungen erbringt oder daran mitwirkt, unverzüglich der Polizei die Überwachung oder Aufzeichnung der Telekommunikation zu ermöglichen sowie Auskünfte über Verkehrsdaten zu erteilen. Von der Auskunftspflicht sind auch Verkehrsdaten erfasst, die nach der Anordnung anfallen. Ob und in welchem Umfang dafür Vorkehrungen zu treffen sind, richtet sich nach dem Telekommunikationsgesetz und den auf seiner Grundlage erlassenen Rechtsverordnungen zur technischen und organisatorischen Umsetzung von Überwachungsmaßnahmen. § 12 Abs. 5 gilt entsprechend.

(7) § 29 Abs. 5 findet entsprechende Anwendung. Soweit sich die Datenerhebung auf die Inhalte der Telekommunikation bezieht, gilt § 29 Abs. 8 entsprechend.

§ 31 a
Identifizierung und Lokalisierung von mobilen Telekommunikationsendgeräten

(1) Die Polizei kann durch den verdeckten Einsatz technischer Mittel spezifische Kennungen, insbesondere die Geräte- und Kartennummer von mobilen Telekommunikationsendgeräten, oder den Standort eines mobilen Telekommunikationsendgeräts ermitteln von

1. den Verantwortlichen nach den §§ 4 und 5 und unter den Voraussetzungen des § 7 von den dort genannten Personen, soweit die Datenerhebung zur Abwehr einer Gefahr für Leib oder Leben erforderlich ist,
2. Personen, bei denen durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass sie zukünftig Straftaten von erheblicher Bedeutung begehen (§ 28 Abs. 3) und die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist, und
3. Kontakt- und Begleitpersonen (§ 26 Abs. 3 Satz 2), soweit die Datenerhebung zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist.

(2) Personenbezogene Daten Dritter dürfen anlässlich einer Maßnahme nach Absatz 1 nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. Über den Datenabgleich

zur Ermittlung der spezifischen Kennung oder des Standorts eines mobilen Telekommunikationsendgeräts hinaus dürfen sie nicht verwendet werden.

(3) Die Datenerhebung nach Absatz 1 bedarf [eigentlich] der richterlichen Entscheidung. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. § 21 Abs. 1 Satz 3 und § 31 Abs. 4 Satz 2 bis 4 gelten entsprechend. Bei Gefahr im Verzug kann die Maßnahme durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden; mit Ausnahme einer Datenerhebung nach Absatz 1 Nr. 1 zur Ermittlung des Aufenthaltsortes einer vermissten, suizidgefährdeten oder sonstigen hilflosen Person ist die richterliche Entscheidung [eigentlich] unverzüglich nachzuholen.

(4) Unter den Voraussetzungen des Absatzes 1 hat jeder, der geschäftsmäßig Telekommunikationsdienstleistungen erbringt oder daran mitwirkt, unverzüglich der Polizei Auskunft über spezifische Kennungen, insbesondere die Geräte- und Kartennummer von mobilen Telekommunikationsendgeräten, oder den Standort des mobilen Telekommunikationsendgeräts zu erteilen. Absatz 3 und § 31 Abs. 6 Satz 2 bis 4 gelten entsprechend.

(5) Die erlangten personenbezogenen Daten dürfen für einen anderen Zweck verwendet werden, soweit dies zur Verfolgung von Straftaten von erheblicher Bedeutung (§ 28 Abs. 3), zur Abwehr einer dringenden Gefahr oder zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung erforderlich ist. Die Zweckänderung der Daten muss im Einzelfall festgestellt und dokumentiert werden.

§ 31 b
Auskunft über Nutzungsdaten

(1) Die Polizei kann Auskünfte über Nutzungsdaten (§ 15 Abs. 1 des Telemediengesetzes) verlangen zur Abwehr einer Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, über

1. die nach den §§ 4 und 5 Verantwortlichen und unter den Voraussetzungen des § 7 über die dort genannten Personen oder

2. Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach den §§ 4 und 5 Verantwortlichen bestimmte oder von ihnen herrührende Mitteilungen entgegennehmen oder weitergeben.

Die Datenerhebung ist nur zulässig, soweit sie zwingend erforderlich ist und die Voraussetzungen des § 39 a Abs. 3 vorliegen. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Die Auskunft kann auch über zukünftige Nutzungsdaten angeordnet werden.

(2) Aufgrund der Anordnung hat jeder, der geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang vermittelt, unverzüglich der Polizei Auskunft über die Nutzungsdaten zu erteilen. § 31 Abs. 4 und 5 gilt entsprechend.

(3) Die Daten sind unverzüglich auf dem von der Polizei bestimmten Weg durch den Verpflichteten nach Absatz 2 Satz 1 zu übermitteln. § 12 Abs. 5 gilt entsprechend.

(4) § 29 Abs. 5 findet entsprechende Anwendung.

§ 31 c
Datenerhebung durch den Einsatz technischer Mittel in informationstechnischen Systemen

(1) Die Polizei kann ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, über

1. die nach den §§ 4 und 5 Verantwortlichen oder
2. Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach den §§ 4 und 5 Verantwortlichen bestimmte oder von ihnen herrührende Mitteilungen entgegennehmen oder weitergeben.

Die Maßnahme ist nur zulässig, soweit die Aufgabenerfüllung nach Satz 1 auf andere Weise nicht möglich erscheint oder wesentlich erschwert wäre und die Voraussetzungen des § 39 a Abs. 3 vorliegen. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Es ist technisch sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) Unter den Voraussetzungen des Absatzes 1 dürfen technische Mittel eingesetzt werden, um zur Vorbereitung einer Maßnahme nach Absatz 1 die erforderlichen Daten, wie insbesondere spezifische Kennungen, sowie den Standort eines informationstechnischen Systems zu ermitteln. Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist.

(4) Bei jedem Einsatz des technischen Mittels sind zu protokollieren:

1. die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
2. die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

Die Protokolldaten dürfen nur verwendet werden, um dem Betroffenen oder einer dazu befugten öffentlichen Stelle die Prüfung zu ermöglichen, ob die Maßnahme nach Absatz 1 rechtmäßig durchgeführt worden ist. Sie sind unverzüglich zu löschen, soweit sie für den in Satz 2 genannten Zweck nicht mehr erforderlich sind.

(5) Die Datenerhebung bedarf [eigentlich] der richterlichen Entscheidung. In der schriftlichen Anordnung sind insbesondere

1. Voraussetzungen und wesentliche Abwägungsgesichtspunkte,
2. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,

3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunkts und
4. möglichst genau das informationstechnische System, in das zur Datenerhebung eingegriffen werden soll, sowie das technische Mittel

zu bestimmen. Zuständiges Gericht ist das Oberverwaltungsgericht Rheinland-Pfalz. Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung. Die Maßnahme ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen.

(6) § 29 Abs. 5 und 8 findet entsprechende Anwendung.

§ 31 d
Unterbrechung oder Verhinderung der Telekommunikation

(1) Die Polizei kann durch den Einsatz technischer Mittel Telekommunikationsverbindungen zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, unterbrechen oder verhindern von

1. den Verantwortlichen nach den §§ 4 und 5 und unter den Voraussetzungen des § 7 von den dort genannten Personen oder
2. Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für die nach den §§ 4 und 5 Verantwortlichen bestimmte oder von ihnen herrührende Mitteilungen entgegennehmen oder weitergeben.

Die Maßnahme darf auch durchgeführt werden, wenn Telekommunikationsverbindungen Dritter unvermeidbar unterbrochen oder verhindert werden.

(2) Die Polizei kann unter den Voraussetzungen des Absatzes 1 Telekommunikationsverbindungen auch ohne Kenntnis der Rufnummer oder einer anderen Kennung des betreffenden Anschlusses oder des Endgeräts unterbrechen oder verhindern, sofern anderenfalls die Erreichung des Zwecks der Maßnahme nach Absatz 1 erheblich erschwert wäre.

(3) Die Maßnahme bedarf [eigentlich] der richterlichen Entscheidung. In der schriftlichen Anordnung sind insbesondere

1. Voraussetzungen und wesentliche Abwägungsgesichtspunkte,
2. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Name und Anschrift,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunkts,
4. soweit möglich die Rufnummer oder eine andere Kennung des Anschlusses oder des Endgeräts, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, und
5. im Fall des Absatzes 2 die möglichst genaue räumliche und zeitliche Bezeichnung der Telekommunikationsverbindungen, die unterbrochen oder verhindert werden sollen,

zu bestimmen. Zuständiges Gericht ist das Oberverwaltungsgericht Rheinland-Pfalz. Das Oberverwaltungsgericht entscheidet nach Maßgabe der Verwaltungsgerichtsordnung. Bei Gefahr im Verzug kann die Maßnahme vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden; die richterliche Entscheidung ist [eigentlich] unverzüglich nachzuholen. Die Maßnahme ist auf höchstens 24 Stunden zu befristen. Eine Verlängerung um jeweils nicht mehr als denselben Zeitraum ist zulässig, sofern die jeweiligen Voraussetzungen der Anordnung weiterhin vorliegen.

§ 31 e
Funkzellenabfrage

(1) Die Polizei kann zur Abwehr einer gegenwärtigen Gefahr für Leib oder Leben einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt, Auskunft über Verkehrsdaten ohne Kenntnis der Rufnummer oder einer anderen Kennung des zu überwachenden Anschlusses oder des Endgeräts verlangen, sofern andernfalls die Erreichung des Zwecks der Maßnahme erheblich erschwert wäre.

(2) § 31 Abs. 4 gilt entsprechend mit der Maßgabe, dass abweichend von § 31 Abs. 4 Satz 2 Nr. 4 in der richterlichen Anordnung möglichst genau die Telekommunikation räumlich und zeitlich zu bestimmen ist, über die Verkehrsdaten erhoben werden sollen. Im Übrigen gelten § 31 Abs. 5 und 6 Satz 2 bis 4 entsprechend; § 29 Abs. 5 findet entsprechende Anwendung.

§ 32
Polizeiliche Beobachtung

(1) Die Polizei kann personenbezogene Daten, insbesondere die Personalien einer Person sowie das Kennzeichen des von ihr benutzten oder eingesetzten Kraftfahrzeuges zur Mitteilung über das Antreffen (polizeiliche Beobachtung) ausschreiben, wenn Tatsachen die Annahme rechtfertigen, dass die Person eine Straftat von erheblicher Bedeutung (§ 28 Abs. 3) begehen wird und die polizeiliche Beobachtung zur vorbeugenden Bekämpfung dieser Straftat erforderlich ist.

(2) Im Falle eines Antreffens der Person oder des von ihr benutzten oder eingesetzten Kraftfahrzeuges können Erkenntnisse über das Antreffen sowie über etwaige Begleiter und mitgeführte Sachen an die ausschreibende Dienststelle übermittelt werden.

(3) Eine Maßnahme nach Absatz 1 darf nur durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden. Die Maßnahme ist auf höchstens zwölf Monate zu befristen. Eine Verlängerung der Maßnahme um jeweils nicht mehr als denselben Zeitraum ist zulässig, sofern die Voraussetzungen der Anordnung weiterhin vorliegen. Die Verlängerung der Maßnahme bedarf [eigentlich] der richterlichen Entscheidung. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeidienststelle ihren Sitz hat. § 21 Abs. 1 Satz 3 gilt entsprechend.

(4) § 28 Abs. 5 gilt entsprechend.