

Table of contents

[reference to the provisions of the Budapest Convention]

Chapter I – Use of terms

Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Article 2 – Illegal access

Article 3 – Illegal interception

Article 4 – Data interference

Article 5 – System interference

Article 6 – Misuse of devices

Article 7 – Computer-related forgery

Article 8 – Computer-related fraud

Article 9 – Offences related to child pornography

Article 10 – Offences related to infringements of copyright and related rights

Article 11 – Attempt and aiding or abetting

Article 12 – Corporate liability

Article 13 – Sanctions and measures

Section 2 – Procedural law

Article 14 – Scope of procedural provisions

Article 15 – Conditions and safeguards

Article 16 – Expedited preservation of stored computer data

Article 17 – Expedited preservation and partial disclosure of traffic data

Article 18 – Production order

Article 19 – Search and seizure of stored computer data

Article 20 – Real-time collection of traffic data

Article 21 – Interception of content data

Section 3 – Jurisdiction

Article 22 – Jurisdiction

Chapter III – International co-operation

Article 24 – Extradition

Article 25 – General principles relating to mutual assistance

Article 26 – Spontaneous information

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 28 – Confidentiality and limitation on use

Article 29 – Expedited preservation of stored computer data

Article 30 – Expedited disclosure of preserved traffic data

Article 31 – Mutual assistance regarding accessing of stored computer data

Article 32 – Trans-border access to stored computer data with consent or where publicly available

Article 33 – Mutual assistance in the real-time collection of traffic data

Article 34 – Mutual assistance regarding the interception of content data

Article 35 – 24/7 Network

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

State:	
Signature of the Budapest Convention:	23/11/2001
Ratification/accession:	09/03/2009

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
<p>Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”:</p> <p>For the purposes of this Convention:</p> <p>a “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;</p> <p>b “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;</p> <p>c “service provider” means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service</p>	<p><u>Telekommunikationsgesetz -TKG (Telecommunications Act), 2004</u></p> <p>Teil 1 Allgemeine Vorschriften, § 3 Begriffsbestimmungen</p> <p>Im Sinne dieses Gesetzes ist oder sind</p> <p>1. „Anbieter von Telekommunikationsdiensten“ jeder, der Telekommunikationsdienste erbringt;</p> <p>6. „Bestandsdaten“ Daten eines Endnutzers, die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste;</p> <p>7. „Betreiber“ ein Unternehmen, das ein öffentliches Telekommunikationsnetz oder eine zugehörige Einrichtung bereitstellt oder zur Bereitstellung hiervon befugt ist;</p> <p>17. „funktechnische Störung“ eine Störung, die für das Funktionieren eines Funknavigationsdienstes oder anderer sicherheitsbezogener Dienste eine Gefahr darstellt oder die einen Funkdienst, der im Einklang mit dem geltenden internationalen Recht, dem Recht der Europäischen Union oder Vorschriften dieses oder eines anderen Gesetzes betrieben wird, anderweitig schwerwiegend beeinträchtigt, behindert oder wiederholt unterbricht;</p> <p>32. „Netzabschlusspunkt“ der physische Punkt, an dem einem Endnutzer der Zugang zu einem öffentlichen Telekommunikationsnetz bereitgestellt wird; in Netzen, in denen eine Vermittlung oder Leitwegebestimmung erfolgt, wird der Netzabschlusspunkt anhand einer bestimmten Netzadresse bezeichnet, die mit der Nummer oder dem Namen eines Endnutzers verknüpft sein kann;</p> <p>59.„Telekommunikation“ der technische Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels</p>

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

Telekommunikationsanlagen;
60. „Telekommunikationsanlagen“ technische Einrichtungen, Systeme oder Server, die als Nachrichten identifizierbare elektromagnetische oder optische Signale oder Daten im Rahmen der Erbringung eines Telekommunikationsdienstes senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können;
70. „Verkehrsdaten“ Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind;
74. „Zugang“ die Bereitstellung von Einrichtungen oder Diensten für ein anderes Unternehmen unter bestimmten Bedingungen zum Zweck der Erbringung von Telekommunikationsdiensten, auch bei deren Verwendung zur Erbringung von Diensten der Informationsgesellschaft oder Rundfunkinhalten; dies umfasst unter anderem Folgendes:

- a) Zugang zu Netzkomponenten, einschließlich nicht aktiver Netzkomponenten, und zugehörigen Einrichtungen, wozu auch der feste oder nicht feste Anschluss von Geräten gehören kann; dies beinhaltet insbesondere den Zugang zum Teilnehmeranschluss sowie zu Einrichtungen und Diensten, die erforderlich sind, um Dienste über den Teilnehmeranschluss zu erbringen, einschließlich des Zugangs zur Anschaltung und Ermöglichung des Anbieterwechsels des Nutzers und zu hierfür notwendigen Informationen und Daten und zur Entstörung;
- b) Zugang zu physischen Infrastrukturen wie Gebäuden, Leitungsrohren und Masten;
- c) Zugang zu einschlägigen Softwaresystemen, einschließlich Systemen für die Betriebsunterstützung;
- d) Zugang zu informationstechnischen Systemen oder Datenbanken für Vorbestellung, Bereitstellung, Auftragserteilung, Anforderung von Wartungs- und Instandsetzungsarbeiten sowie Abrechnung;
- e) Zugang zur Nummernumsetzung oder zu Systemen, die eine gleichwertige Funktion bieten;
- f) Zugang zu Fest- und Mobilfunknetzen;
- g) Zugang zu Zugangsberechtigungssystemen für Digitalfernsehdienste und
- h) Zugang zu Diensten für virtuelle Telekommunikationsnetze;

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p><u>Strafgesetzbuch – StGB (German Criminal Code)</u>, in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 des Gesetzes vom 22. November 2021 geändert worden ist.</p> <p>Besonderer Teil, Fünfzehnter Abschnitt Verletzung des persönlichen Lebens- und Geheimbereichs, <u>§ 202a Ausspähen von Daten</u></p> <p>(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.</p>
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
<p>Article 2 – Illegal access</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><u>StGB (Criminal Code), 1998 as amended in 2021</u></p> <p>Besonderer Teil, Fünfzehnter Abschnitt Verletzung des persönlichen Lebens- und Geheimbereichs, <u>§ 202a Ausspähen von Daten</u></p> <p>(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.</p>
Article 3 – Illegal interception	<u>StGB (Criminal Code), 1998 as amended in 2021</u>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><u>Besonderer Teil, Fünfzehnter Abschnitt Verletzung des persönlichen Lebens- und Geheimbereichs, § 202b Abfangen von Daten</u></p> <p><u>Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.</u></p>
<p>Article 4 – Data interference</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.</p> <p>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	<p><u>StGB (Criminal Code), 1998 as amended in 2021</u></p> <p>Besonderer Teil, Siebenundzwanzigster Abschnitt Sachbeschädigung</p> <p>§ 303a Datenveränderung</p> <p>(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p> <p>(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.</p>
<p>Article 5 – System interference</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data</p>	<p><u>StGB (Criminal Code), 1998 as amended in 2021</u></p> <p>Besonderer Teil, Siebenundzwanzigster Abschnitt Sachbeschädigung</p> <p>§ 303b Computersabotage</p>

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1.eine Tat nach § 303a Abs. 1 begeht,

2.Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder

3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1.einen Vermögensverlust großen Ausmaßes herbeiführt,

2.gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,

3.durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 6 – Misuse of devices</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>a the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;</p> <p>ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and</p> <p>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.</p> <p>3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.</p>	<p><u>StGB (Criminal Code), 1998 as amended in 2021</u></p> <p>Besonderer Teil, Fünfzehnter Abschnitt Verletzung des persönlichen Lebens- und Geheimbereichs</p> <p>§ 202c Vorbereiten des Ausspärens und Abfangens von Daten</p> <p><u>(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er</u></p> <p style="padding-left: 40px;"><u>1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder</u></p> <p style="padding-left: 40px;"><u>2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,</u></p> <p><u>herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.</u></p> <p><u>(2) § 149 Abs. 2 und 3 gilt entsprechend.</u></p>
Title 2 – Computer-related offences	
<p>Article 7 – Computer-related forgery</p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when</p>	<p><u>StGB (Criminal Code), 1998 as amended in 2021</u></p>

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Besonderer Teil, Dreiundzwanzigster Abschnitt Urkundenfälschung

§ 267 Urkundenfälschung

(1) Wer zur Täuschung im Rechtsverkehr eine unechte Urkunde herstellt, eine echte Urkunde verfälscht oder eine unechte oder verfälschte Urkunde gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1.gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Betrug oder Urkundenfälschung verbunden hat,

2.einen Vermögensverlust großen Ausmaßes herbeiführt,

3.durch eine große Zahl von unechten oder verfälschten Urkunden die Sicherheit des Rechtsverkehrs erheblich gefährdet oder

4.seine Befugnisse oder seine Stellung als Amtsträger oder Europäischer Amtsträger mißbraucht.

(4) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren wird bestraft, wer die Urkundenfälschung als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263 bis 264 oder 267 bis 269 verbunden hat, gewerbsmäßig begeht.

§ 269 Fälschung beweisheblicher Daten

(1) Wer zur Täuschung im Rechtsverkehr beweishebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) § 267 Abs. 3 und 4 gilt entsprechend.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <ul style="list-style-type: none"> a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p><u>StGB (Criminal Code), 1998 as amended in 2021</u></p> <p>Besonderer Teil, Zweiundzwanzigster Abschnitt Betrug und Untreue</p> <p>§ 263 Betrug</p> <p>(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p> <p>(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter</p> <ol style="list-style-type: none"> 1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Urkundenfälschung oder Betrug verbunden hat, 2. einen Vermögensverlust großen Ausmaßes herbeiführt oder in der Absicht handelt, durch die fortgesetzte Begehung von Betrug eine große Zahl von Menschen in die Gefahr des Verlustes von Vermögenswerten zu bringen, 3. eine andere Person in wirtschaftliche Not bringt, 4. seine Befugnisse oder seine Stellung als Amtsträger oder Europäischer Amtsträger mißbraucht oder 5. einen Versicherungsfall vortäuscht, nachdem er oder ein anderer zu diesem Zweck eine Sache von bedeutendem Wert in Brand gesetzt oder durch eine Brandlegung ganz oder teilweise zerstört oder ein Schiff zum Sinken oder Stranden gebracht hat. <p>(4) § 243 Abs. 2 sowie die §§ 247 und 248a gelten entsprechend.</p> <p>(5) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren, in minder schweren Fällen mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren wird bestraft, wer den Betrug als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 263 bis 264 oder 267 bis 269 verbunden hat, gewerbsmäßig begeht.</p> <p>(6) Das Gericht kann Führungsaufsicht anordnen (§ 68 Abs. 1).</p> <p>§ 263a Computerbetrug</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.</p> <p>(2) § 263 Abs. 2 bis 6 gilt entsprechend.</p> <p>(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er</p> <ol style="list-style-type: none"> 1. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt oder 2. Passwörter oder sonstige Sicherungscodes, die zur Begehung einer solchen Tat geeignet sind, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, <p>wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.</p>
Title 3 – Content-related offences	
<p>Article 9 – Offences related to child pornography</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p> <ol style="list-style-type: none"> a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 	<p>StGB (Criminal Code), 1998 as amended in 2021</p> <p>Besonderer Teil, Dreizehnter Abschnitt Straftaten gegen die sexuelle Selbstbestimmung</p> <p>§ 184b Verbreitung, Erwerb und Besitz kinderpornographischer Inhalte</p> <p><u>(1) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren wird bestraft, wer</u></p> <ol style="list-style-type: none"> 1. <u>einen kinderpornographischen Inhalt verbreitet oder der Öffentlichkeit zugänglich macht; kinderpornographisch ist ein pornographischer Inhalt (§ 11 Absatz 3), wenn er zum Gegenstand hat:</u> <ol style="list-style-type: none"> a) <u>sexuelle Handlungen von, an oder vor einer Person unter vierzehn Jahren (Kind),</u> b) <u>die Wiedergabe eines ganz oder teilweise unbedeckten Kindes in aufreizend geschlechtsbetonter Körperhaltung oder</u> c) <u>die sexuell aufreizende Wiedergabe der unbedeckten Genitalien oder</u>

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

- a a minor engaged in sexually explicit conduct;
- b a person appearing to be a minor engaged in sexually explicit conduct;
- c realistic images representing a minor engaged in sexually explicit conduct

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

des unbedeckten Gesäßes eines Kindes,

2. es unternimmt, einer anderen Person einen kinderpornographischen Inhalt, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, zugänglich zu machen oder den Besitz daran zu verschaffen,

3. einen kinderpornographischen Inhalt, der ein tatsächliches Geschehen wiedergibt, herstellt oder

4. einen kinderpornographischen Inhalt herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diesen ein- oder auszuführen, um ihn im Sinne der Nummer 1 oder der Nummer 2 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen, soweit die Tat nicht nach Nummer 3 mit Strafe bedroht ist.

Gibt der kinderpornographische Inhalt in den Fällen von Absatz 1 Satz 1 Nummer 1 und 4 kein tatsächliches oder wirklichkeitsnahes Geschehen wieder, so ist auf Freiheitsstrafe von drei Monaten bis zu fünf Jahren zu erkennen.

(2) Handelt der Täter in den Fällen des Absatzes 1 Satz 1 gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, und gibt der Inhalt in den Fällen des Absatzes 1 Satz 1 Nummer 1, 2 und 4 ein tatsächliches oder wirklichkeitsnahes Geschehen wieder, so ist auf Freiheitsstrafe nicht unter zwei Jahren zu erkennen.

(3) Wer es unternimmt, einen kinderpornographischen Inhalt, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, abzurufen oder sich den Besitz an einem solchen Inhalt zu verschaffen oder wer einen solchen Inhalt besitzt, wird mit Freiheitsstrafe von einem Jahr bis zu fünf Jahren bestraft.

(4) Der Versuch ist in den Fällen des Absatzes 1 Satz 2 in Verbindung mit Satz 1 Nummer 1 strafbar.

(5) Absatz 1 Satz 1 Nummer 2 und Absatz 3 gelten nicht für Handlungen, die ausschließlich der rechtmäßigen Erfüllung von Folgendem dienen:

1. staatlichen Aufgaben,

2. Aufgaben, die sich aus Vereinbarungen mit einer zuständigen staatlichen Stelle ergeben, oder

3. dienstlichen oder beruflichen Pflichten.

(6) Absatz 1 Satz 1 Nummer 1, 2 und 4 und Satz 2 gilt nicht für dienstliche Handlungen im Rahmen von strafrechtlichen Ermittlungsverfahren, wenn

1. die Handlung sich auf einen kinderpornographischen Inhalt bezieht, der kein tatsächliches Geschehen wiedergibt und auch nicht unter

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

Verwendung einer Bildaufnahme eines Kindes oder Jugendlichen hergestellt worden ist, und

2. die Aufklärung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

(7) Gegenstände, auf die sich eine Straftat nach Absatz 1 Satz 1 Nummer 2 oder 3 oder Absatz 3 bezieht, werden eingezogen. § 74a ist anzuwenden.

§ 184c Verbreitung, Erwerb und Besitz jugendpornographischer Inhalte

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer

1. einen jugendpornographischen Inhalt verbreitet oder der Öffentlichkeit zugänglich macht; jugendpornographisch ist ein pornographischer Inhalt (§ 11 Absatz 3), wenn er zum Gegenstand hat:

a) sexuelle Handlungen von, an oder vor einer vierzehn, aber noch nicht achtzehn Jahre alten Person,

b) die Wiedergabe einer ganz oder teilweise unbedeckten vierzehn, aber noch nicht achtzehn Jahre alten Person in aufreizend geschlechtsbetonter Körperhaltung oder

c) die sexuell aufreizende Wiedergabe der unbedeckten Genitalien oder des unbedeckten Gesäßes einer vierzehn, aber noch nicht achtzehn Jahre alten Person,

2. es unternimmt, einer anderen Person einen jugendpornographischen Inhalt, der ein tatsächliches oder wirklichkeitsnahes Geschehen wiedergibt, zugänglich zu machen oder den Besitz daran zu verschaffen,

3. einen jugendpornographischen Inhalt, der ein tatsächliches Geschehen wiedergibt, herstellt oder

4. einen jugendpornographischen Inhalt herstellt, bezieht, liefert, vorrätig hält, anbietet, bewirbt oder es unternimmt, diesen ein- oder auszuführen, um ihn im Sinne der Nummer 1 oder 2 zu verwenden oder einer anderen Person eine solche Verwendung zu ermöglichen, soweit die Tat nicht nach Nummer 3 mit Strafe bedroht ist.

(2) Handelt der Täter in den Fällen des Absatzes 1 gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung solcher Taten verbunden hat, und gibt der Inhalt in den Fällen des Absatzes 1 Nummer 1, 2 und 4 ein tatsächliches oder wirklichkeitsnahes Geschehen wieder, so ist auf

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Freiheitsstrafe von drei Monaten bis zu fünf Jahren zu erkennen.</p> <p><u>(3) Wer es unternimmt, einen jugendpornographischen Inhalt, der ein tatsächliches Geschehen wiedergibt, abzurufen oder sich den Besitz an einem solchen Inhalt zu verschaffen, oder wer einen solchen Inhalt besitzt, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.</u></p> <p><u>(4) Absatz 1 Nummer 3, auch in Verbindung mit Absatz 5, und Absatz 3 sind nicht anzuwenden auf Handlungen von Personen in Bezug auf einen solchen jugendpornographischen Inhalt, den sie ausschließlich zum persönlichen Gebrauch mit Einwilligung der dargestellten Personen hergestellt haben.</u></p> <p><u>(5) Der Versuch ist strafbar; dies gilt nicht für Taten nach Absatz 1 Nummer 2 und 4 sowie Absatz 3.</u></p> <p><u>(6) § 184b Absatz 5 bis 7 gilt entsprechend.</u></p>
Title 4 – Offences related to infringements of copyright and related rights	
<p>Article 10 – Offences related to infringements of copyright and related rights</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances</p>	<p>Urheberrechtsgesetz – UrhG (Act on Copyright and Related Rights) vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 25 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist.</p> <p>Teil 2 Verwandte Schutzrechte, Abschnitt 2 Rechtsverletzungen, Unterabschnitt 2 Straf- und Bußgeldvorschriften</p> <p>§ 106 Unerlaubte Verwertung urheberrechtlich geschützter Werke</p> <p>(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.</p> <p>(2) Der Versuch ist strafbar.</p> <p>§ 107 Unzulässiges Anbringen der Urheberbezeichnung</p> <p>(1) Wer</p> <p style="padding-left: 20px;">1. auf dem Original eines Werkes der bildenden Künste die Urheberbezeichnung (§ 10 Abs. 1) ohne Einwilligung des Urhebers</p>

BUDAPEST CONVENTION

and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

DOMESTIC LEGISLATION

anbringt oder ein derart bezeichnetes Original verbreitet,
2. auf einem Vervielfältigungsstück, einer Bearbeitung oder Umgestaltung eines Werkes der bildenden Künste die Urheberbezeichnung (§ 10 Abs. 1) auf eine Art anbringt, die dem Vervielfältigungsstück, der Bearbeitung oder Umgestaltung den Anschein eines Originals gibt, oder ein derart bezeichnetes Vervielfältigungsstück, eine solche Bearbeitung oder Umgestaltung verbreitet,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

(2) Der Versuch ist strafbar.

§ 108 Unerlaubte Eingriffe in verwandte Schutzrechte

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten

1. eine wissenschaftliche Ausgabe (§ 70) oder eine Bearbeitung oder Umgestaltung einer solchen Ausgabe vervielfältigt, verbreitet oder öffentlich wiedergibt,
2. ein nachgelassenes Werk oder eine Bearbeitung oder Umgestaltung eines solchen Werkes entgegen § 71 verwertet,
3. ein Lichtbild (§ 72) oder eine Bearbeitung oder Umgestaltung eines Lichtbildes vervielfältigt, verbreitet oder öffentlich wiedergibt,
4. die Darbietung eines ausübenden Künstlers entgegen den § 77 Abs. 1 oder Abs. 2 Satz 1, § 78 Abs. 1 verwertet,
5. einen Tonträger entgegen § 85 verwertet,
6. eine Funksendung entgegen § 87 verwertet,
7. einen Bildträger oder Bild- und Tonträger entgegen §§ 94 oder 95 in Verbindung mit § 94 verwertet,
8. eine Datenbank entgegen § 87b Abs. 1 verwertet,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

§ 108a Gewerbsmäßige unerlaubte Verwertung

(1) Handelt der Täter in den Fällen der §§ 106 bis 108 gewerbsmäßig, so ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(2) Der Versuch ist strafbar.

BUDAPEST CONVENTION**DOMESTIC LEGISLATION****§ 108b Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen**

(1) Wer

1. in der Absicht, sich oder einem Dritten den Zugang zu einem nach diesem Gesetz geschützten Werk oder einem anderen nach diesem Gesetz geschützten Schutzgegenstand oder deren Nutzung zu ermöglichen, eine wirksame technische Maßnahme ohne Zustimmung des Rechtsinhabers umgeht oder

2. wissentlich unbefugt

a) eine von Rechtsinhabern stammende Information für die Rechtewahrnehmung entfernt oder verändert, wenn irgendeine der betreffenden Informationen an einem Vervielfältigungsstück eines Werkes oder eines sonstigen Schutzgegenstandes angebracht ist oder im Zusammenhang mit der öffentlichen Wiedergabe eines solchen Werkes oder Schutzgegenstandes erscheint, oder

b) ein Werk oder einen sonstigen Schutzgegenstand, bei dem eine Information für die Rechtewahrnehmung unbefugt entfernt oder geändert wurde, verbreitet, zur Verbreitung einführt, sendet, öffentlich wiedergibt oder öffentlich zugänglich macht

und dadurch wenigstens leichtfertig die Verletzung von Urheberrechten oder verwandten Schutzrechten veranlasst, ermöglicht, erleichtert oder verschleiert, wird, wenn die Tat nicht ausschließlich zum eigenen privaten Gebrauch des Täters oder mit dem Täter persönlich verbundener Personen erfolgt oder sich auf einen derartigen Gebrauch bezieht, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer entgegen § 95a Abs. 3 eine Vorrichtung, ein Erzeugnis oder einen Bestandteil zu gewerblichen Zwecken herstellt, einführt, verbreitet, verkauft oder vermietet.

(3) Handelt der Täter in den Fällen des Absatzes 1 gewerbsmäßig, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes vom 31. Mai 2021 (Act to adapt copyright law to the requirements of the Digital Single Market of 31 May 2021), in force since 7 June 2021;

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p><u>Urheberrechts-Diensteanbieter-Gesetz - UrhDaG</u> (Copyright Service Provider Act), in force since 1 August 2021 (unofficial translation);</p> <p>Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie – KunstUrhG (Art Copyright Act) of 9 January 1907, as last amended by Article 3 § 31 of the Law of February 16, 2001 (Federal Law Gazette I p. 266);</p>
Title 5 – Ancillary liability and sanctions	
<p>Article 11 – Attempt and aiding or abetting</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.</p> <p>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p>	<p><u>StGB (Criminal Code), 1998 as amended in 2021</u></p> <p><u>Allgemeiner Teil, Zweiter Titel Versuch</u></p> <p><u>§ 23 Strafbarkeit des Versuchs</u></p> <p><u>(1) Der Versuch eines Verbrechens ist stets strafbar, der Versuch eines Vergehens nur dann, wenn das Gesetz es ausdrücklich bestimmt.</u></p> <p><u>(2) Der Versuch kann milder bestraft werden als die vollendete Tat (§ 49 Abs. 1).</u></p> <p><u>(3) Hat der Täter aus grobem Unverstand verkannt, daß der Versuch nach der Art des Gegenstandes, an dem, oder des Mittels, mit dem die Tat begangen werden sollte, überhaupt nicht zur Vollendung führen konnte, so kann das Gericht von Strafe absehen oder die Strafe nach seinem Ermessen mildern (§ 49 Abs. 2).</u></p> <p>Allgemeiner Teil, Dritter Titel Täterschaft und Teilnahme</p> <p><u>§ 26 Anstiftung</u></p> <p><u>Als Anstifter wird gleich einem Täter bestraft, wer vorsätzlich einen anderen zu dessen vorsätzlich begangener rechtswidriger Tat bestimmt hat.</u></p> <p><u>§ 27 Beihilfe</u></p> <p><u>(1) Als Gehilfe wird bestraft, wer vorsätzlich einem anderen zu dessen</u></p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p><u>vorsätzlich begangener rechtswidriger Tat Hilfe geleistet hat.</u></p> <p><u>(2) Die Strafe für den Gehilfen richtet sich nach der Strafdrohung für den Täter. Sie ist nach § 49 Abs. 1 zu mildern.</u></p>
<p>Article 12 – Corporate liability</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:</p> <ul style="list-style-type: none"> a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. <p>2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.</p>	<p><u>Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung (OWiG) vom 19. Februar 1987 das zuletzt durch Artikel 31 des Gesetzes vom 5. Oktober 2021 geändert worden ist. [Act on regulatory offences, 1987 last amended in 2019]</u></p> <p><u>Erster Teil Allgemeine Vorschriften, Sechster Abschnitt Einziehung des Wertes von Taterträgen</u></p> <p><u>§ 30 Geldbuße gegen juristische Personen und Personenvereinigungen</u></p> <p><u>(1) Hat jemand</u></p> <ul style="list-style-type: none"> <u>1. als vertretungsberechtigtes Organ einer juristischen Person oder als Mitglied eines solchen Organs,</u> <u>2. als Vorstand eines nicht rechtsfähigen Vereins oder als Mitglied eines solchen Vorstandes,</u> <u>3. als vertretungsberechtigter Gesellschafter einer rechtsfähigen Personengesellschaft,</u> <u>4. als Generalbevollmächtigter oder in leitender Stellung als Prokurist oder Handlungsbevollmächtigter einer juristischen Person oder einer in Nummer 2 oder 3 genannten Personenvereinigung oder</u> <u>5. als sonstige Person, die für die Leitung des Betriebs oder Unternehmens einer juristischen Person oder einer in Nummer 2 oder 3 genannten Personenvereinigung verantwortlich handelt, wozu auch die Überwachung der Geschäftsführung oder die sonstige Ausübung von</u>

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

Kontrollbefugnissen in leitender Stellung gehört,

eine Straftat oder Ordnungswidrigkeit begangen, durch die Pflichten, welche die juristische Person oder die Personenvereinigung treffen, verletzt worden sind oder die juristische Person oder die Personenvereinigung bereichert worden ist oder werden sollte, so kann gegen diese eine Geldbuße festgesetzt werden.

(2) Die Geldbuße beträgt

1. im Falle einer vorsätzlichen Straftat bis zu zehn Millionen Euro,

2. im Falle einer fahrlässigen Straftat bis zu fünf Millionen Euro.

Im Falle einer Ordnungswidrigkeit bestimmt sich das Höchstmaß der Geldbuße nach dem für die Ordnungswidrigkeit angedrohten Höchstmaß der Geldbuße. Verweist das Gesetz auf diese Vorschrift, so verzehnfacht sich das Höchstmaß der Geldbuße nach Satz 2 für die im Gesetz bezeichneten Tatbestände. Satz 2 gilt auch im Falle einer Tat, die gleichzeitig Straftat und Ordnungswidrigkeit ist, wenn das für die Ordnungswidrigkeit angedrohte Höchstmaß der Geldbuße das Höchstmaß nach Satz 1 übersteigt.

(2a) Im Falle einer Gesamtrechtsnachfolge oder einer partiellen Gesamtrechtsnachfolge durch Aufspaltung (§ 123 Absatz 1 des Umwandlungsgesetzes) kann die Geldbuße nach Absatz 1 und 2 gegen den oder die Rechtsnachfolger festgesetzt werden. Die Geldbuße darf in diesen Fällen den Wert des übernommenen Vermögens sowie die Höhe der gegenüber dem Rechtsvorgänger angemessenen Geldbuße nicht übersteigen. Im Bußgeldverfahren tritt der Rechtsnachfolger oder treten die Rechtsnachfolger in die Verfahrensstellung ein, in der sich der Rechtsvorgänger zum Zeitpunkt des Wirksamwerdens der Rechtsnachfolge befunden hat.

(3) § 17 Abs. 4 und § 18 gelten entsprechend.

(4) Wird wegen der Straftat oder Ordnungswidrigkeit ein Straf- oder Bußgeldverfahren nicht eingeleitet oder wird es eingestellt oder wird von Strafe abgesehen, so kann die Geldbuße selbständig festgesetzt werden. Durch Gesetz kann bestimmt werden, daß die Geldbuße auch in weiteren Fällen selbständig

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

festgesetzt werden kann. Die selbständige Festsetzung einer Geldbuße gegen die juristische Person oder Personenvereinigung ist jedoch ausgeschlossen, wenn die Straftat oder Ordnungswidrigkeit aus rechtlichen Gründen nicht verfolgt werden kann; § 33 Abs. 1 Satz 2 bleibt unberührt.

(5) Die Festsetzung einer Geldbuße gegen die juristische Person oder Personenvereinigung schließt es aus, gegen sie wegen derselben Tat die Einziehung nach den §§ 73 oder 73c des Strafgesetzbuches oder nach § 29a anzuordnen.

(6) Bei Erlass eines Bußgeldbescheids ist zur Sicherung der Geldbuße § 111e Absatz 2 der Strafprozessordnung mit der Maßgabe anzuwenden, dass an die Stelle des Urteils der Bußgeldbescheid tritt.

Dritter Teil Einzelne Ordnungswidrigkeiten, Vierter Abschnitt

§ 130 Verletzung der Aufsichtspflicht in Betrieben und Unternehmen

(1) Wer als Inhaber eines Betriebes oder Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterläßt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre. Zu den erforderlichen Aufsichtsmaßnahmen gehören auch die Bestellung, sorgfältige Auswahl und Überwachung von Aufsichtspersonen.

(2) Betrieb oder Unternehmen im Sinne des Absatzes 1 ist auch das öffentliche Unternehmen.

(3) Die Ordnungswidrigkeit kann, wenn die Pflichtverletzung mit Strafe bedroht ist, mit einer Geldbuße bis zu einer Million Euro geahndet werden. § 30 Absatz 2 Satz 3 ist anzuwenden. Ist die Pflichtverletzung mit Geldbuße bedroht, so bestimmt sich das Höchstmaß der Geldbuße wegen der Aufsichtspflichtverletzung nach dem für die Pflichtverletzung angedrohten Höchstmaß der Geldbuße. Satz 3 gilt auch im Falle einer Pflichtverletzung, die

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	gleichzeitig mit Strafe und Geldbuße bedroht ist, wenn das für die Pflichtverletzung angedrohte Höchstmaß der Geldbuße das Höchstmaß nach Satz 1 übersteigt.
<p>Article 13 – Sanctions and measures</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.</p> <p>2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.</p>	<p><u>StGB (Criminal Code), 1998 as amended in 2021</u></p> <p>Besonderer Teil, Dritter Abschnitt Rechtsfolgen der Tat, Die Artikel 38 bis 76b <u>Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung (OWiG) vom 19. Februar 1987 das zuletzt durch Artikel 31 des Gesetzes vom 5. Oktober 2021 geändert worden ist. [Act on regulatory offences, 1987 last amended in 2019]</u></p> <p>Erster Teil Allgemeine Vorschriften, Zweiter Abschnitt Grundlagen der Ahndung</p>
Section 2 – Procedural law	
<p>Article 14 – Scope of procedural provisions</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.</p> <p>2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:</p> <ul style="list-style-type: none"> a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. <p>3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies</p>	<p><u>Strafprozeßordnung(StPO)</u> in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 1 des Gesetzes vom 21. Dezember 2021 (BGBl. I S. 5252) geändert worden ist [<u>Code of Criminal Procedure</u> as published on 7 April 1987 (Federal Law Gazette I, p. 1074, 1319), as last amended by Article 3 of the Act of 11 July 2019 (Federal Law Gazette I, p. 1066)]</p> <p>Zweiter Abschnitt Vorbereitung der öffentlichen Klage§ 161 Allgemeine Ermittlungsbefugnis der Staatsanwaltschaft (1) Zu dem in § 160 Abs. 1 bis 3 bezeichneten Zweck 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 in diesem Falle befugt, von allen Behörden</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.</p> <p>b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:</p> <ul style="list-style-type: none"> i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, <p>that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21</p>	<p>Auskunft zu verlangen.</p> <p>(2) Soweit in diesem Gesetz die Löschung personenbezogener Daten ausdrücklich angeordnet wird, ist § 58 Absatz 3 des Bundesdatenschutzgesetzes nicht anzuwenden.</p> <p>(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 personenbezogenen Daten ohne Einwilligung der von der Maßnahme betroffenen Personen zu Beweis Zwecken im Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, zu deren Aufklärung eine solche Maßnahme nach diesem Gesetz hätte angeordnet werden dürfen. § 100e Absatz 6 Nummer 3 bleibt unberührt.</p> <p>(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 zu Beweis Zwecken nur verwendet werden (Artikel 13 Abs. 5 des Grundgesetzes), wenn das Amtsgericht (§ 162 Abs. 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.</p>
<p>Article 15 – Conditions and safeguards</p> <p>1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.</p> <p>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, <i>inter alia</i>, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.</p> <p>3 To the extent that it is consistent with the public interest, in particular the</p>	<p>StPO (1987; 2021)// CCP (1987;2019)</p> <p>Bundesdatenschutzgesetz (BDSG) vom 30. Juni 2017 [BGBl. I S. 2097], das durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist.[<u>Federal Data Protection Act</u> of 30 June 2017, as amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626)]</p> <p>Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 u. 2 Satz 2 des Gesetzes vom 29. September 2020 (BGBl. I S. 2048) geändert worden ist [<u>Basic Law for the Federal Republic of Germany</u> in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by Article 1 of the Act of 29 September 2020 (Federal Law Gazette I p. 2048).]</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.</p>	<p>I. Die Grundrechte. Art 10 (1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. (2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.</p>
<p>Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.</p> <p>2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>StPO (1987; 2021)// CCP (1987;2019)</p> <p>Achter Abschnitt Ermittlungsmaßnahmen § 94 Sicherstellung und Beschlagnahme von Gegenständen zu Beweis Zwecken</p> <p>(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen. (2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme. (3) Die Absätze 1 und 2 gelten auch für Führerscheine, die der Einziehung unterliegen. (4) Die Herausgabe beweglicher Sachen richtet sich nach den §§ 111n und 111o.</p> <p>§ 98 Verfahren bei der Beschlagnahme (1) Beschlagnahmen dürfen nur durch das Gericht, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) angeordnet werden. Die Beschlagnahme nach § 97 Abs. 5 Satz 2 in den Räumen einer Redaktion, eines Verlages, einer Druckerei oder einer Rundfunkanstalt darf nur durch das Gericht angeordnet werden. (2) Der Beamte, der einen Gegenstand ohne gerichtliche Anordnung beschlagnahmt hat, soll binnen drei Tagen die gerichtliche Bestätigung beantragen, wenn bei der Beschlagnahme weder der davon Betroffene noch ein erwachsener Angehöriger anwesend war oder wenn der Betroffene und im Falle seiner Abwesenheit ein erwachsener Angehöriger des Betroffenen gegen die Beschlagnahme ausdrücklichen Widerspruch erhoben hat. Der Betroffene kann</p>

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

jederzeit die gerichtliche Entscheidung beantragen. Die Zuständigkeit des Gerichts bestimmt sich nach § 162. Der Betroffene kann den Antrag auch bei dem Amtsgericht einreichen, in dessen Bezirk die Beschlagnahme stattgefunden hat; dieses leitet den Antrag dem zuständigen Gericht zu. Der Betroffene ist über seine Rechte zu belehren.

(3) Ist nach erhobener öffentlicher Klage die Beschlagnahme durch die Staatsanwaltschaft oder eine ihrer Ermittlungspersonen erfolgt, so ist binnen drei Tagen dem Gericht von der Beschlagnahme Anzeige zu machen; die beschlagnahmten Gegenstände sind ihm zur Verfügung zu stellen.

(4) Wird eine Beschlagnahme in einem Dienstgebäude oder einer nicht allgemein zugänglichen Einrichtung oder Anlage der Bundeswehr erforderlich, so wird die vorgesetzte Dienststelle der Bundeswehr um ihre Durchführung ersucht. Die ersuchende Stelle ist zur Mitwirkung berechtigt. Des Ersuchens bedarf es nicht, wenn die Beschlagnahme in Räumen vorzunehmen ist, die ausschließlich von anderen Personen als Soldaten bewohnt werden.

§ 100g Erhebung von Verkehrsdaten

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer

1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder
2. eine Straftat mittels Telekommunikation begangen hat,

so dürfen Verkehrsdaten (§§ 9 und 12 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und § 2a Absatz 1 des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben) erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Im Fall des Satzes 1 Nummer 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. Die Erhebung gespeicherter (retrograder) Standortdaten ist nach diesem Absatz nur unter den Voraussetzungen des Absatzes 2 zulässig. Im Übrigen ist die Erhebung von Standortdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur im Fall des Satzes 1 Nummer 1 zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>erforderlich ist.</p> <p>(2) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine der in Satz 2 bezeichneten besonders schweren Straftaten begangen hat oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat, und wiegt die Tat auch im Einzelfall besonders schwer, dürfen die nach § 176 des Telekommunikationsgesetzes gespeicherten Verkehrsdaten erhoben werden, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Besonders schwere Straftaten im Sinne des Satzes 1 sind:</p> <p>1. aus dem Strafgesetzbuch:</p> <p style="padding-left: 40px;">e) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Inhalte in den Fällen des § 184b Absatz 1 Satz 1, Absatz 2 und 3 sowie des § 184c Absatz</p> <p>(4) Die Erhebung von Verkehrsdaten nach Absatz 2, auch in Verbindung mit Absatz 3 Satz 2, die sich gegen eine der in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannten Personen richtet und die voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, ist unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und der Löschung der Aufzeichnungen ist aktenkundig zu machen. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannte Person richtet, von dieser Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. § 160a Absatz 3 und 4 gilt entsprechend.</p> <p>(5) Erfolgt die Erhebung von Verkehrsdaten nicht beim Erbringer von Telekommunikationsdiensten, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.</p>
<p>Article 17 – Expedited preservation and partial disclosure of traffic data</p> <p>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <p>a ensure that such expeditious preservation of traffic data is available</p>	<p>StPO (1987; 2021)// CCP (1987;2019)</p> <p>§ 100g Erhebung von Verkehrsdaten</p> <p>(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer</p> <p style="padding-left: 40px;">1. eine Straftat von auch im Einzelfall erheblicher Bedeutung,</p>

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder

2. eine Straftat mittels Telekommunikation begangen hat,

so dürfen Verkehrsdaten (§§ 9 und 12 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und § 2a Absatz 1 des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben) erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Im Fall des Satzes 1 Nummer 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. Die Erhebung gespeicherter (retrograder) Standortdaten ist nach diesem Absatz nur unter den Voraussetzungen des Absatzes 2 zulässig. Im Übrigen ist die Erhebung von Standortdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur im Fall des Satzes 1 Nummer 1 zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine der in Satz 2 bezeichneten besonders schweren Straftaten begangen hat oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat, und wiegt die Tat auch im Einzelfall besonders schwer, dürfen die nach § 176 des Telekommunikationsgesetzes gespeicherten Verkehrsdaten erhoben werden, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Besonders schwere Straftaten im Sinne des Satzes 1 sind:

1. aus dem Strafgesetzbuch:

e) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Inhalte in den Fällen des § 184b Absatz 1 Satz 1, Absatz 2 und 3 sowie des § 184c Absatz

(4) Die Erhebung von Verkehrsdaten nach Absatz 2, auch in Verbindung mit Absatz 3 Satz 2, die sich gegen eine der in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannten Personen richtet und die voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, ist unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden. Aufzeichnungen hierüber

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und der Löschung der Aufzeichnungen ist aktenkundig zu machen. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine Ermittlungsmaßnahme, die sich nicht gegen eine in § 53 Absatz 1 Satz 1 Nummer 1 bis 5 genannte Person richtet, von dieser Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. § 160a Absatz 3 und 4 gilt entsprechend.</p> <p>(5) Erfolgt die Erhebung von Verkehrsdaten nicht beim Erbringer von Telekommunikationsdiensten, bestimmt sie sich nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften.</p>
<p>Article 18 – Production order</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <p>a a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and</p> <p>b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:</p> <p>a the type of communication service used, the technical provisions taken thereto and the period of service;</p> <p>b the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;</p> <p>c any other information on the site of the installation of communication equipment, available on the basis of the service</p>	<p>StPO (1987; 2021)// CCP (1987;2019)</p> <p>Achter Abschnitt Ermittlungsmaßnahmen</p> <p>§ 95 Herausgabepflicht</p> <p>(1) Wer einen Gegenstand der vorbezeichneten Art in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern.</p> <p>(2) Im Falle der Weigerung können gegen ihn die in § 70 bestimmten Ordnungs- und Zwangsmittel festgesetzt werden. Das gilt nicht bei Personen, die zur Verweigerung des Zeugnisses berechtigt sind.</p> <p>§ 100g Erhebung von Verkehrsdaten</p> <p>(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer</p> <ol style="list-style-type: none"> 1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder 2. eine Straftat mittels Telekommunikation begangen hat, <p>so dürfen Verkehrsdaten (§§ 9 und 12 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und § 2a Absatz 1 des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben) erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem</p>

BUDAPEST CONVENTION

agreement or arrangement.

DOMESTIC LEGISLATION

angemessenen Verhältnis zur Bedeutung der Sache steht. Im Fall des Satzes 1 Nummer 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. Die Erhebung gespeicherter (retrograder) Standortdaten ist nach diesem Absatz nur unter den Voraussetzungen des Absatzes 2 zulässig. Im Übrigen ist die Erhebung von Standortdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur im Fall des Satzes 1 Nummer 1 zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.

(2) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine der in Satz 2 bezeichneten besonders schweren Straftaten begangen hat oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat, und wiegt die Tat auch im Einzelfall besonders schwer, dürfen die nach § 176 des Telekommunikationsgesetzes gespeicherten Verkehrsdaten erhoben werden, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

§ 100j Bestandsdatenauskunft

(1) Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist, darf Auskunft verlangt werden

1. über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 des Telekommunikationsgesetzes erhobenen Daten (§ 174 Absatz 1 Satz 1 des Telekommunikationsgesetzes) von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, und
2. über Bestandsdaten gemäß § 2 Absatz 2 Nummer 2 des Telekommunikation-Telemedien-Datenschutz-Gesetzes (§ 22 Absatz 1 Satz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes) von demjenigen, der geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt.

Bezieht sich das Auskunftsverlangen nach Satz 1 Nummer 1 auf Daten, mittelst derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 174 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Bezieht sich das Auskunftsverlangen nach Satz 1 Nummer 2 auf als Bestandsdaten erhobene Passwörter oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 23 des Telekommunikation-Telemedien-Datenschutz-Gesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für ihre Nutzung zur Verfolgung einer besonders schweren Straftat nach § 100b Absatz 2 Nummer 1 Buchstabe a, c, e, f, g, h oder m, Nummer 3 Buchstabe b erste Alternative oder Nummer 5, 6, 9 oder 10 vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 174 Absatz 1 Satz 3, § 177 Absatz 1 Nummer 3 des Telekommunikationsgesetzes und § 22 Absatz 1 Satz 3 und 4 des Telekommunikation-Telemedien-Datenschutz-Gesetzes). Das Vorliegen der Voraussetzungen für ein Auskunftsverlangen nach Satz 1 ist aktenkundig zu machen.

(3) Auskunftsverlangen nach Absatz 1 Satz 2 und 3 dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Im Fall von Auskunftsverlangen nach Absatz 1 Satz 2 kann die Anordnung bei Gefahr im Verzug auch durch die Staatsanwaltschaft oder ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Die Sätze 1 bis 3 finden bei Auskunftsverlangen nach Absatz 1 Satz 2 keine Anwendung, wenn die betroffene Person vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird. Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen.

(4) Die betroffene Person ist in den Fällen des Absatzes 1 Satz 2 und 3 und des Absatzes 2 über die Beauskunftung zu benachrichtigen. Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. Sie unterbleibt, wenn ihr überwiegende schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(5) Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste oder Telemediendienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	unverzöglich zu übermitteln. § 95 Absatz 2 gilt entsprechend.
<p>Article 19 – Search and seizure of stored computer data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <p style="padding-left: 20px;">a a computer system or part of it and computer data stored therein; and</p> <p style="padding-left: 20px;">b a computer-data storage medium in which computer data may be stored</p> <p style="padding-left: 40px;">in its territory.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:</p> <p style="padding-left: 20px;">a seize or similarly secure a computer system or part of it or a computer-data storage medium;</p> <p style="padding-left: 20px;">b make and retain a copy of those computer data;</p> <p style="padding-left: 20px;">c maintain the integrity of the relevant stored computer data;</p> <p style="padding-left: 20px;">d render inaccessible or remove those computer data in the accessed computer system.</p> <p>4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.</p> <p>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>StPO (1987; 2021)// CCP (1987;2019)</p> <p>Achter Abschnitt Ermittlungsmaßnahmen</p> <p>§ 94 Sicherstellung und Beschlagnahme von Gegenständen zu Beweiszwecken</p> <p>(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein können, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.</p> <p>(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der Beschlagnahme.</p> <p>(3) Die Absätze 1 und 2 gelten auch für Führerscheine, die der Einziehung unterliegen.</p> <p>(4) Die Herausgabe beweglicher Sachen richtet sich nach den §§ 111n und 111o.</p> <p>§ 110 Durchsicht von Papieren und elektronischen Speichermedien</p> <p>(1) Die Durchsicht der Papiere des von der Durchsuchung Betroffenen steht der Staatsanwaltschaft und auf deren Anordnung ihren Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) zu.</p> <p>(2) Im Übrigen sind Beamte zur Durchsicht der aufgefundenen Papiere nur dann befugt, wenn der Inhaber die Durchsicht genehmigt. Andernfalls haben sie die Papiere, deren Durchsicht sie für geboten erachten, in einem Umschlag, der in Gegenwart des Inhabers mit dem Amtssiegel zu verschließen ist, an die Staatsanwaltschaft abzuliefern.</p> <p>(3) Nach Maßgabe der Absätze 1 und 2 ist auch die Durchsicht von elektronischen Speichermedien bei dem von der Durchsuchung Betroffenen zulässig. Diese Durchsicht darf auch auf hiervon räumlich getrennte Speichermedien erstreckt werden, soweit auf sie von dem elektronischen Speichermedium aus zugegriffen werden kann, wenn andernfalls der Verlust der gesuchten Daten zu befürchten ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden.</p> <p>(4) Werden Papiere zur Durchsicht mitgenommen oder Daten vorläufig gesichert, gelten die §§ 95a und 98 Absatz 2 entsprechend.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>Article 20 – Real-time collection of traffic data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:</p> <ul style="list-style-type: none"> a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: <ul style="list-style-type: none"> i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>StPO (1987; 2021)// CCP (1987;2019)</p> <p>Achter Abschnitt Ermittlungsmaßnahmen</p> <p>§ 100g Erhebung von Verkehrsdaten</p> <p>(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer</p> <ul style="list-style-type: none"> 1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder 2. eine Straftat mittels Telekommunikation begangen hat, <p>so dürfen Verkehrsdaten (§§ 9 und 12 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und § 2a Absatz 1 des Gesetzes über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben) erhoben werden, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Im Fall des Satzes 1 Nummer 2 ist die Maßnahme nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. Die Erhebung gespeicherter (retrograder) Standortdaten ist nach diesem Absatz nur unter den Voraussetzungen des Absatzes 2 zulässig. Im Übrigen ist die Erhebung von Standortdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur im Fall des Satzes 1 Nummer 1 zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist.</p>
<p>Article 21 – Interception of content data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by</p>	<p>StPO (1987; 2021)// CCP (1987;2019)</p> <p>Achter Abschnitt Ermittlungsmaßnahmen</p>

BUDAPEST CONVENTION

domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

 i to collect or record through the application of technical means on the territory of that Party, or

 ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

DOMESTIC LEGISLATION

§ 100a Telekommunikationsüberwachung

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind:

1. aus dem Strafgesetzbuch:
 - a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80a bis 82, 84 bis 86, 87 bis 89a, 89c Absatz 1 bis 4, 94 bis 100a,
 - b) Bestechlichkeit und Bestechung von Mandatsträgern nach § 108e,
 - c) Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,
 - d) Straftaten gegen die öffentliche Ordnung nach § 127 Absatz 3 und 4 sowie den §§ 129 bis 130,
 - e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4,
 - f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176, 176c, 176d und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,
 - g) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Inhalte nach § 184b, § 184c Absatz 2,

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

- h) Mord und Totschlag nach den §§ 211 und 212,
- i) Straftaten gegen die persönliche Freiheit nach den §§ 232, 232a Absatz 1 bis 5, den §§ 232b, 233 Absatz 2, den §§ 233a, 234, 234a, 239a und 239b,
- j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2, Wohnungseinbruchdiebstahl nach § 244 Absatz 4 und schwerer Bandendiebstahl nach § 244a,
- k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,
- l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,
- m) Geldwäsche nach § 261, wenn die Vortat eine der in den Nummern 1 bis 11 genannten schweren Straftaten ist,
- n) Betrug und Computerbetrug unter den in § 263 Abs. 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2,
- o) Subventionsbetrug unter den in § 264 Abs. 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Abs. 3 in Verbindung mit § 263 Abs. 5,
- p) Sportwettbetrug und Manipulation von berufssportlichen Wettbewerben unter den in § 265e Satz 2 genannten Voraussetzungen,
- q) Vorenthalten und Veruntreuen von Arbeitsentgelt unter den in § 266a Absatz 4 Satz 2 Nummer 4 genannten Voraussetzungen,
- r) Straftaten der Urkundenfälschung unter den in § 267 Abs. 3 Satz 2 genannten Voraussetzungen und im Fall des § 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, sowie nach § 275 Abs. 2 und § 276 Abs. 2,
- s) Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,
- t) Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,
- u) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 Abs. 1 bis 4, des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316c,
- v) Bestechlichkeit und Bestechung nach den §§ 332 und 334,

2. aus der Abgabenordnung:

- a) Steuerhinterziehung unter den in § 370 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzungen, sofern der Täter als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Taten nach § 370 Absatz 1 verbunden hat, handelt, oder unter den in § 370 Absatz 3 Satz 2

[Back to the Table of Contents](#)

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

- Nummer 5 genannten Voraussetzungen,
 b) gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel nach § 373,
 c) Steuerhhehlerei im Falle des § 374 Abs. 2,
3. aus dem Anti-Doping-Gesetz:
 Straftaten nach § 4 Absatz 4 Nummer 2 Buchstabe b,
4. aus dem Asylgesetz:
 a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,
 b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a,
5. aus dem Aufenthaltsgesetz:
 a) Einschleusen von Ausländern nach § 96 Abs. 2,
 b) Einschleusen mit Todesfolge und gewerbs- und bandenmäßiges Einschleusen nach § 97,
- 5a. aus dem Ausgangsstoffgesetz:
 Straftaten nach § 13 Absatz 3,
6. aus dem Außenwirtschaftsgesetz:
 vorsätzliche Straftaten nach den §§ 17 und 18 des Außenwirtschaftsgesetzes,
7. aus dem Betäubungsmittelgesetz:
 a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,
 b) Straftaten nach den §§ 29a, 30 Abs. 1 Nr. 1, 2 und 4 sowie den §§ 30a und 30b,
8. aus dem Grundstoffüberwachungsgesetz:
 Straftaten nach § 19 Abs. 1 unter den in § 19 Abs. 3 Satz 2 genannten Voraussetzungen,
9. aus dem Gesetz über die Kontrolle von Kriegswaffen:
 a) Straftaten nach § 19 Abs. 1 bis 3 und § 20 Abs. 1 und 2 sowie § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21,
 b) Straftaten nach § 22a Abs. 1 bis 3,
- 9a. aus dem Neue-psychoaktive-Stoffe-Gesetz:
 Straftaten nach § 4 Absatz 3 Nummer 1 Buchstabe a,
10. aus dem Völkerstrafgesetzbuch:
 a) Völkermord nach § 6,
 b) Verbrechen gegen die Menschlichkeit nach § 7,
 c) Kriegsverbrechen nach den §§ 8 bis 12,
 d) Verbrechen der Aggression nach § 13,
11. aus dem Waffengesetz:

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

- a) Straftaten nach § 51 Abs. 1 bis 3,
- b) Straftaten nach § 52 Abs. 1 Nr. 1 und 2 Buchstabe c und d sowie Abs. 5 und 6.

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.

(4) Auf Grund der Anordnung einer Überwachung und Aufzeichnung der Telekommunikation hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) diese Maßnahmen zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. § 95 Absatz 2 gilt entsprechend.

(5) Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass

1. ausschließlich überwacht und aufgezeichnet werden können:
 - a) die laufende Telekommunikation (Absatz 1 Satz 2), oder
 - b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),
2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und
3. 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.

- (6) 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,

[Back to the Table of Contents](#)

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

3. die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und
4. die Organisationseinheit, die die Maßnahme durchführt.

§ 100b Online-Durchsuchung

(1) Auch ohne Wissen des Betroffenen darf mit technischen Mitteln in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung), wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,
2. die Tat auch im Einzelfall besonders schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Besonders schwere Straftaten im Sinne des Absatzes 1 Nummer 1 sind:

1. aus dem Strafgesetzbuch:

- a) Straftaten des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 81, 82, 89a, 89c Absatz 1 bis 4, nach den §§ 94, 95 Absatz 3 und § 96 Absatz 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Absatz 1 Satz 2, § 99 Absatz 2 und den §§ 100, 100a Absatz 4,
- b) Betreiben krimineller Handelsplattformen im Internet in den Fällen des § 127 Absatz 3 und 4, sofern der Zweck der Handelsplattform im Internet darauf ausgerichtet ist, in den Buchstaben a und c bis o sowie in den Nummern 2 bis 10 genannte besonders schwere Straftaten zu ermöglichen oder zu fördern,
- c) Bildung krimineller Vereinigungen nach § 129 Absatz 1 in Verbindung mit Absatz 5 Satz 3 und Bildung terroristischer Vereinigungen nach § 129a Absatz 1, 2, 4, 5 Satz 1 erste Alternative, jeweils auch in Verbindung mit § 129b Absatz 1,
- d) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Absatz 3 und § 152b Absatz 1 bis 4,
- e) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des §

[Back to the Table of Contents](#)

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

176 Absatz 1 und der §§ 176c, 176d und, unter den in § 177 Absatz 6 Satz 2 Nummer 2 genannten Voraussetzungen, des § 177,

f) Verbreitung, Erwerb und Besitz kinderpornografischer Inhalte in den Fällen des § 184b Absatz 1 Satz 1 und Absatz 2,

g) Mord und Totschlag nach den §§ 211, 212,

h) Straftaten gegen die persönliche Freiheit in den Fällen des § 232 Absatz 2 und 3, des § 232a Absatz 1, 3, 4 und 5 zweiter Halbsatz, des § 232b Absatz 1 und 3 sowie Absatz 4, dieser in Verbindung mit § 232a Absatz 4 und 5 zweiter Halbsatz, des § 233 Absatz 2, des § 233a Absatz 1, 3 und 4 zweiter Halbsatz, der §§ 234 und 234a Absatz 1 und 2 sowie der §§ 239a und 239b,

i) Bandendiebstahl nach § 244 Absatz 1 Nummer 2 und schwerer Bandendiebstahl nach § 244a,

j) schwerer Raub und Raub mit Todesfolge nach § 250 Absatz 1 oder Absatz 2, § 251,

k) räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Absatz 4 Satz 2 genannten Voraussetzungen,

l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260, 260a,

m) besonders schwerer Fall der Geldwäsche nach § 261 unter den in § 261 Absatz 5 Satz 2 genannten Voraussetzungen, wenn die Vortat eine der in den Nummern 1 bis 7 genannten besonders schweren Straftaten ist,

n) Computerbetrug in den Fällen des § 263a Absatz 2 in Verbindung mit § 263 Absatz 5,

o) besonders schwerer Fall der Bestechlichkeit und Bestechung nach § 335 Absatz 1 unter den in § 335 Absatz 2 Nummer 1 bis 3 genannten Voraussetzungen,

2. aus dem Asylgesetz:

a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Absatz 3,

b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a Absatz 1,

3. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Absatz 2,

b) Einschleusen mit Todesfolge oder gewerbs- und bandenmäßiges Einschleusen nach § 97,

[Back to the Table of Contents](#)

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

4. aus dem Außenwirtschaftsgesetz:
- a) Straftaten nach § 17 Absatz 1, 2 und 3, jeweils auch in Verbindung mit Absatz 6 oder 7,
 - b) Straftaten nach § 18 Absatz 7 und 8, jeweils auch in Verbindung mit Absatz 10,
5. aus dem Betäubungsmittelgesetz:
- a) besonders schwerer Fall einer Straftat nach § 29 Absatz 1 Satz 1 Nummer 1, 5, 6, 10, 11 oder 13, Absatz 3 unter der in § 29 Absatz 3 Satz 2 Nummer 1 genannten Voraussetzung,
 - b) eine Straftat nach den §§ 29a, 30 Absatz 1 Nummer 1, 2, 4, § 30a,
6. aus dem Gesetz über die Kontrolle von Kriegswaffen:
- a) eine Straftat nach § 19 Absatz 2 oder § 20 Absatz 1, jeweils auch in Verbindung mit § 21,
 - b) besonders schwerer Fall einer Straftat nach § 22a Absatz 1 in Verbindung mit Absatz 2,
7. aus dem Grundstoffüberwachungsgesetz:
Straftaten nach § 19 Absatz 3,
8. aus dem Neue-psychoaktive-Stoffe-Gesetz:
Straftaten nach § 4 Absatz 3 Nummer 1,
9. aus dem Völkerstrafgesetzbuch:
- a) Völkermord nach § 6,
 - b) Verbrechen gegen die Menschlichkeit nach § 7,
 - c) Kriegsverbrechen nach den §§ 8 bis 12,
 - d) Verbrechen der Aggression nach § 13,
10. aus dem Waffengesetz:
- a) besonders schwerer Fall einer Straftat nach § 51 Absatz 1 in Verbindung mit Absatz 2,
 - b) besonders schwerer Fall einer Straftat nach § 52 Absatz 1 Nummer 1 in Verbindung mit Absatz 5.
- (3) Die Maßnahme darf sich nur gegen den Beschuldigten richten. Ein Eingriff in informationstechnische Systeme anderer Personen ist nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass
- 1. der in der Anordnung nach § 100e Absatz 3 bezeichnete Beschuldigte informationstechnische Systeme der anderen Person benutzt, und
 - 2. die Durchführung des Eingriffs in informationstechnische Systeme des Beschuldigten allein nicht zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Mitbeschuldigten führen wird.
- Die Maßnahme darf auch durchgeführt werden, wenn andere Personen

[Back to the Table of Contents](#)

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>unvermeidbar betroffen werden. (4) § 100a Absatz 5 und 6 gilt mit Ausnahme von Absatz 5 Satz 1 Nummer 1 entsprechend.</p>
Section 3 – Jurisdiction	
<p>Article 22 – Jurisdiction</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:</p> <ul style="list-style-type: none"> a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. <p>2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.</p> <p>3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.</p> <p>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.</p> <p>When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.</p>	<p><u>StGB (Criminal Code), 1998 as amended in 2021</u></p> <p><u>Allgemeiner Teil, Erster Abschnitt Das Strafgesetz, Erster Titel</u></p> <p><u>§ 3 Geltung für Inlandstaaten</u> <u>Das deutsche Strafrecht gilt für Taten, die im Inland begangen werden.</u></p> <p><u>§ 4 Geltung für Taten auf deutschen Schiffen und Luftfahrzeugen</u> <u>Das deutsche Strafrecht gilt, unabhängig vom Recht des Tatorts, für Taten, die auf einem Schiff oder in einem Luftfahrzeug begangen werden, das berechtigt ist, die Bundesflagge oder das Staatszugehörigkeitszeichen der Bundesrepublik Deutschland zu führen.</u></p> <p><u>§ 7 Geltung für Auslandstaaten in anderen Fällen</u></p> <p><u>(1) Das deutsche Strafrecht gilt für Taten, die im Ausland gegen einen Deutschen begangen werden, wenn die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt.</u></p> <p><u>(2) Für andere Taten, die im Ausland begangen werden, gilt das deutsche Strafrecht, wenn die Tat am Tatort mit Strafe bedroht ist oder der Tatort keiner Strafgewalt unterliegt und wenn der Täter</u></p> <ul style="list-style-type: none"> <u>1. zur Zeit der Tat Deutscher war oder es nach der Tat geworden ist oder</u> <u>2. zur Zeit der Tat Ausländer war, im Inland betroffen und, obwohl das Auslieferungsgesetz seine Auslieferung nach der Art der Tat zuließe, nicht ausgeliefert wird, weil ein Auslieferungersuchen innerhalb angemessener Frist nicht gestellt oder abgelehnt wird oder die Auslieferung nicht ausführbar ist.</u>

BUDAPEST CONVENTION

DOMESTIC LEGISLATION

Chapter III – International co-operation

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and

Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist [Act on International Mutual Assistance in Criminal Matters, as amended by Article 4 of the Act of 10 December 2019 (Federal Law Gazette I, p. 2128)]

StPO (1987; 2021)// **CCP** (1987;2019)

Zweiter Abschnitt Regelungen über die Datenverarbeitung

§ 487 Übermittlung gespeicherter Daten; Auskunft

(1) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen den zuständigen Stellen übermittelt werden, soweit dies für die in diesen Vorschriften genannten Zwecke, für Zwecke eines Gnadenverfahrens, des Vollzugs von freiheitsentziehenden Maßnahmen oder der internationalen Rechtshilfe in Strafsachen erforderlich ist. § 479 Absatz 1 und 2 und § 485 Satz 3 gelten entsprechend. Bewährungshelfer und Führungsaufsichtsstellen dürfen personenbezogene Daten von Verurteilten, die unter Aufsicht gestellt sind, an die Einrichtungen des Justiz- und Maßregelvollzugs übermitteln, wenn diese Daten für den Vollzug der Freiheitsentziehung, insbesondere zur Förderung der Vollzugs- und Behandlungsplanung oder der Entlassungsvorbereitung, erforderlich sind; das Gleiche gilt für Mitteilungen an Vollstreckungsbehörden, soweit diese Daten für die in § 477 Absatz 2 Nummer 1 oder 3 genannten Zwecke erforderlich sind.

(2) Außerdem kann, unbeschadet des § 57 des Bundesdatenschutzgesetzes, Auskunft 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.

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.</p> <p>7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.</p> <p>b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure</p>	<p>nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zu einer weitergehenden Prüfung der Zulässigkeit der Übermittlung besteht.</p> <p>(4) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen auch für wissenschaftliche Zwecke übermittelt werden. § 476 gilt entsprechend.</p> <p>(5) Besondere gesetzliche Bestimmungen, die die Übermittlung von Daten aus einem Strafverfahren anordnen oder erlauben, bleiben unberührt.</p> <p>(6) Die Daten dürfen nur zu dem Zweck verwendet werden, für den sie übermittelt worden sind. Eine Verwendung für andere Zwecke ist zulässig, soweit die Daten auch dafür hätten übermittelt werden dürfen.</p>
<p>Article 25 – General principles relating to mutual assistance</p> <p>1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.</p> <p>2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.</p> <p>3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.</p> <p>4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.</p>	<p><u>Gesetz über die internationale Rechtshilfe in Strafsachen (IRG)</u> in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist [<u>Act on International Mutual Assistance in Criminal Matters</u>, as amended by Article 4 of the Act of 10 December 2019 (Federal Law Gazette I, p. 2128)]</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.</p>	
<p>Article 26 – Spontaneous information</p> <p>1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.</p> <p>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.</p>	<p><u>Gesetz über die internationale Rechtshilfe in Strafsachen (IRG)</u> in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist [<u>Act on International Mutual Assistance in Criminal Matters</u>, as amended by Article 4 of the Act of 10 December 2019 (Federal Law Gazette I, p. 2128)]</p>
<p>Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</p> <p>1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.</p>	<p><u>Gesetz über die internationale Rechtshilfe in Strafsachen (IRG)</u> in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist [<u>Act on International Mutual Assistance in Criminal Matters</u>, as amended by Article 4 of the Act of 10 December 2019 (Federal Law Gazette I, p. 2128)]</p>

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

- b The central authorities shall communicate directly with each other;
- c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;
- d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.
- 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
- 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
- b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
- 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
- 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
- 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
- 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
- 9 a In the event of urgency, requests for mutual assistance or

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.</p> <p>b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).</p> <p>c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.</p> <p>d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.</p> <p>e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.</p>	
<p>Article 28 – Confidentiality and limitation on use</p> <p>1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.</p> <p>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:</p> <p>a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or</p> <p>b not used for investigations or proceedings other than those stated in the request.</p> <p>3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.</p>	<p><u>Gesetz über die internationale Rechtshilfe in Strafsachen (IRG)</u> in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist [<u>Act on International Mutual Assistance in Criminal Matters</u>, as amended by Article 4 of the Act of 10 December 2019 (Federal Law Gazette I, p. 2128)]</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.</p>	
<p>Article 29 – Expedited preservation of stored computer data</p> <p>1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.</p> <p>2 A request for preservation made under paragraph 1 shall specify:</p> <ul style="list-style-type: none"> a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. <p>3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.</p> <p>4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.</p> <p>5 In addition, a request for preservation may only be refused if:</p> <ul style="list-style-type: none"> a the request concerns an offence which the requested Party 	<p><u>Gesetz über die internationale Rechtshilfe in Strafsachen (IRG)</u> in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist [<u>Act on International Mutual Assistance in Criminal Matters</u>, as amended by Article 4 of the Act of 10 December 2019 (Federal Law Gazette I, p. 2128)]</p> <p><u>StPO</u> (1987; 2021)// <u>CCP</u> (1987;2019)</p> <p>Zweiter Abschnitt Regelungen über die Datenverarbeitung</p> <p>§ 487 Übermittlung gespeicherter Daten; Auskunft</p> <p>(1) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen den zuständigen Stellen übermittelt werden, soweit dies für die in diesen Vorschriften genannten Zwecke, für Zwecke eines Gnadenverfahrens, des Vollzugs von freiheitsentziehenden Maßnahmen oder der internationalen Rechtshilfe in Strafsachen erforderlich ist. § 479 Absatz 1 und 2 und § 485 Satz 3 gelten entsprechend. Bewährungshelfer und Führungsaufsichtsstellen dürfen personenbezogene Daten von Verurteilten, die unter Aufsicht gestellt sind, an die Einrichtungen des Justiz- und Maßregelvollzugs übermitteln, wenn diese Daten für den Vollzug der Freiheitsentziehung, insbesondere zur Förderung der Vollzugs- und Behandlungsplanung oder der Entlassungsvorbereitung, erforderlich sind; das Gleiche gilt für Mitteilungen an Vollstreckungsbehörden, soweit diese Daten für die in § 477 Absatz 2 Nummer 1 oder 3 genannten Zwecke erforderlich sind.</p> <p>(2) Außerdem kann, unbeschadet des § 57 des Bundesdatenschutzgesetzes, Auskunft 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.</p> <p>(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>considers a political offence or an offence connected with a political offence, or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p> <p>6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.</p> <p>4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.</p>	<p>nur, ob das Übermittlungersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zu einer weitergehenden Prüfung der Zulässigkeit der Übermittlung besteht.</p> <p>(4) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen auch für wissenschaftliche Zwecke übermittelt werden. § 476 gilt entsprechend.</p> <p>(5) Besondere gesetzliche Bestimmungen, die die Übermittlung von Daten aus einem Strafverfahren anordnen oder erlauben, bleiben unberührt.</p> <p>(6) Die Daten dürfen nur zu dem Zweck verwendet werden, für den sie übermittelt worden sind. Eine Verwendung für andere Zwecke ist zulässig, soweit die Daten auch dafür hätten übermittelt werden dürfen.</p>
<p>Article 30 – Expedited disclosure of preserved traffic data</p> <p>1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.</p> <p>2 Disclosure of traffic data under paragraph 1 may only be withheld if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p>	<p><u>Gesetz über die internationale Rechtshilfe in Strafsachen (IRG)</u> in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist [<u>Act on International Mutual Assistance in Criminal Matters</u>, as amended by Article 4 of the Act of 10 December 2019 (Federal Law Gazette I, p. 2128)]</p> <p><u>StPO</u> (1987; 2021)// <u>CCP</u> (1987;2019)</p> <p>Zweiter Abschnitt Regelungen über die Datenverarbeitung</p> <p>§ 487 Übermittlung gespeicherter Daten; Auskunft</p> <p>(1) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen den zuständigen Stellen übermittelt werden, soweit dies für die in diesen Vorschriften genannten Zwecke, für Zwecke eines Gnadenverfahrens, des Vollzugs von freiheitsentziehenden Maßnahmen oder der internationalen Rechtshilfe in Strafsachen erforderlich ist. § 479 Absatz 1 und 2 und § 485 Satz 3 gelten entsprechend. Bewährungshelfer und Führungsaufsichtsstellen dürfen personenbezogene Daten von Verurteilten, die unter Aufsicht gestellt sind, an die Einrichtungen des Justiz- und Maßregelvollzugs übermitteln, wenn diese Daten für den Vollzug der Freiheitsentziehung, insbesondere zur Förderung der</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Vollzugs- und Behandlungsplanung oder der Entlassungsvorbereitung, erforderlich sind; das Gleiche gilt für Mitteilungen an Vollstreckungsbehörden, soweit diese Daten für die in § 477 Absatz 2 Nummer 1 oder 3 genannten Zwecke erforderlich sind.</p> <p>(2) Außerdem kann, unbeschadet des § 57 des Bundesdatenschutzgesetzes, Auskunft 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.</p> <p>(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zu einer weitergehenden Prüfung der Zulässigkeit der Übermittlung besteht.</p> <p>(4) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen auch für wissenschaftliche Zwecke übermittelt werden. § 476 gilt entsprechend.</p> <p>(5) Besondere gesetzliche Bestimmungen, die die Übermittlung von Daten aus einem Strafverfahren anordnen oder erlauben, bleiben unberührt.</p> <p>(6) Die Daten dürfen nur zu dem Zweck verwendet werden, für den sie übermittelt worden sind. Eine Verwendung für andere Zwecke ist zulässig, soweit die Daten auch dafür hätten übermittelt werden dürfen.</p>
<p>Article 31 – Mutual assistance regarding accessing of stored computer data</p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.</p> <p>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <p>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</p> <p>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</p>	<p><u>StPO</u> (1987; 2021)// <u>CCP</u> (1987;2019)</p> <p>Zweiter Abschnitt Regelungen über die Datenverarbeitung</p> <p>§ 487 Übermittlung gespeicherter Daten; Auskunft</p> <p>(1) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen den zuständigen Stellen übermittelt werden, soweit dies für die in diesen Vorschriften genannten Zwecke, für Zwecke eines Gnadenverfahrens, des Vollzugs von freiheitsentziehenden Maßnahmen oder der internationalen Rechtshilfe in Strafsachen erforderlich ist. § 479 Absatz 1 und 2 und § 485 Satz 3 gelten entsprechend. Bewährungshelfer und Führungsaufsichtsstellen dürfen personenbezogene Daten von Verurteilten, die unter Aufsicht gestellt sind, an die Einrichtungen des Justiz- und Maßregelvollzugs übermitteln, wenn diese Daten für den Vollzug der Freiheitsentziehung, insbesondere zur Förderung der Vollzugs- und Behandlungsplanung oder der Entlassungsvorbereitung,</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>erforderlich sind; das Gleiche gilt für Mitteilungen an Vollstreckungsbehörden, soweit diese Daten für die in § 477 Absatz 2 Nummer 1 oder 3 genannten Zwecke erforderlich sind.</p> <p>(2) Außerdem kann, unbeschadet des § 57 des Bundesdatenschutzgesetzes, Auskunft 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.</p> <p>(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zu einer weitergehenden Prüfung der Zulässigkeit der Übermittlung besteht.</p> <p>(4) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen auch für wissenschaftliche Zwecke übermittelt werden. § 476 gilt entsprechend.</p> <p>(5) Besondere gesetzliche Bestimmungen, die die Übermittlung von Daten aus einem Strafverfahren anordnen oder erlauben, bleiben unberührt.</p> <p>(6) Die Daten dürfen nur zu dem Zweck verwendet werden, für den sie übermittelt worden sind. Eine Verwendung für andere Zwecke ist zulässig, soweit die Daten auch dafür hätten übermittelt werden dürfen.</p>
<p>Article 32 – Trans-border access to stored computer data with consent or where publicly available</p> <p>A Party may, without the authorisation of another Party:</p> <p>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</p> <p>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.</p>	<p><u>Gesetz über die internationale Rechtshilfe in Strafsachen (IRG)</u> in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist [<u>Act on International Mutual Assistance in Criminal Matters</u>, as amended by Article 4 of the Act of 10 December 2019 (Federal Law Gazette I, p. 2128)]</p> <p><u>StPO</u> (1987; 2021)// <u>CCP</u> (1987;2019)</p> <p>Zweiter Abschnitt Regelungen über die Datenverarbeitung</p> <p>§ 487 Übermittlung gespeicherter Daten; Auskunft</p> <p>(1) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen den zuständigen Stellen übermittelt werden, soweit dies für die in diesen Vorschriften genannten Zwecke, für Zwecke eines Gnadenverfahrens, des Vollzugs von freiheitsentziehenden Maßnahmen oder der internationalen Rechtshilfe in</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>Strafsachen erforderlich ist. § 479 Absatz 1 und 2 und § 485 Satz 3 gelten entsprechend. Bewährungshelfer und Führungsaufsichtsstellen dürfen personenbezogene Daten von Verurteilten, die unter Aufsicht gestellt sind, an die Einrichtungen des Justiz- und Maßregelvollzugs übermitteln, wenn diese Daten für den Vollzug der Freiheitsentziehung, insbesondere zur Förderung der Vollzugs- und Behandlungsplanung oder der Entlassungsvorbereitung, erforderlich sind; das Gleiche gilt für Mitteilungen an Vollstreckungsbehörden, soweit diese Daten für die in § 477 Absatz 2 Nummer 1 oder 3 genannten Zwecke erforderlich sind.</p> <p>(2) Außerdem kann, unbeschadet des § 57 des Bundesdatenschutzgesetzes, Auskunft 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.</p> <p>(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zu einer weitergehenden Prüfung der Zulässigkeit der Übermittlung besteht.</p> <p>(4) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen auch für wissenschaftliche Zwecke übermittelt werden. § 476 gilt entsprechend.</p> <p>(5) Besondere gesetzliche Bestimmungen, die die Übermittlung von Daten aus einem Strafverfahren anordnen oder erlauben, bleiben unberührt.</p> <p>(6) Die Daten dürfen nur zu dem Zweck verwendet werden, für den sie übermittelt worden sind. Eine Verwendung für andere Zwecke ist zulässig, soweit die Daten auch dafür hätten übermittelt werden dürfen.</p>
<p>Article 33 – Mutual assistance in the real-time collection of traffic data</p> <p>1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.</p> <p>2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a</p>	<p><u>Gesetz über die internationale Rechtshilfe in Strafsachen (IRG)</u> in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert worden ist [<u>Act on International Mutual Assistance in Criminal Matters</u>, as amended by Article 4 of the Act of 10 December 2019 (Federal Law Gazette I, p. 2128)]</p> <p><u>StPO</u> (1987; 2021)// <u>CCP</u> (1987;2019)</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
similar domestic case.	<p>Zweiter Abschnitt Regelungen über die Datenverarbeitung</p> <p>§ 487 Übermittlung gespeicherter Daten; Auskunft</p> <p>(1) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen den zuständigen Stellen übermittelt werden, soweit dies für die in diesen Vorschriften genannten Zwecke, für Zwecke eines Gnadenverfahrens, des Vollzugs von freiheitsentziehenden Maßnahmen oder der internationalen Rechtshilfe in Strafsachen erforderlich ist. § 479 Absatz 1 und 2 und § 485 Satz 3 gelten entsprechend. Bewährungshelfer und Führungsaufsichtsstellen dürfen personenbezogene Daten von Verurteilten, die unter Aufsicht gestellt sind, an die Einrichtungen des Justiz- und Maßregelvollzugs übermitteln, wenn diese Daten für den Vollzug der Freiheitsentziehung, insbesondere zur Förderung der Vollzugs- und Behandlungsplanung oder der Entlassungsvorbereitung, erforderlich sind; das Gleiche gilt für Mitteilungen an Vollstreckungsbehörden, soweit diese Daten für die in § 477 Absatz 2 Nummer 1 oder 3 genannten Zwecke erforderlich sind.</p> <p>(2) Außerdem kann, unbeschadet des § 57 des Bundesdatenschutzgesetzes, Auskunft 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.</p> <p>(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zu einer weitergehenden Prüfung der Zulässigkeit der Übermittlung besteht.</p> <p>(4) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen auch für wissenschaftliche Zwecke übermittelt werden. § 476 gilt entsprechend.</p> <p>(5) Besondere gesetzliche Bestimmungen, die die Übermittlung von Daten aus einem Strafverfahren anordnen oder erlauben, bleiben unberührt.</p> <p>(6) Die Daten dürfen nur zu dem Zweck verwendet werden, für den sie übermittelt worden sind. Eine Verwendung für andere Zwecke ist zulässig, soweit die Daten auch dafür hätten übermittelt werden dürfen.</p>
<p>Article 34 – Mutual assistance regarding the interception of content data</p> <p>The Parties shall provide mutual assistance to each other in the real-time</p>	<p>Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 29 des Gesetzes vom 5. Oktober 2021 (BGBl. I S. 4607) geändert</p>

BUDAPEST CONVENTION**DOMESTIC LEGISLATION**

collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

worden ist [Act on International Mutual Assistance in Criminal Matters, as amended by Article 4 of the Act of 10 December 2019 (Federal Law Gazette I, p. 2128)]

StPO (1987; 2021)// **CCP** (1987;2019)

Zweiter Abschnitt Regelungen über die Datenverarbeitung

§ 487 Übermittlung gespeicherter Daten; Auskunft

(1) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen den zuständigen Stellen übermittelt werden, soweit dies für die in diesen Vorschriften genannten Zwecke, für Zwecke eines Gnadenverfahrens, des Vollzugs von freiheitsentziehenden Maßnahmen oder der internationalen Rechtshilfe in Strafsachen erforderlich ist. § 479 Absatz 1 und 2 und § 485 Satz 3 gelten entsprechend. Bewährungshelfer und Führungsaufsichtsstellen dürfen personenbezogene Daten von Verurteilten, die unter Aufsicht gestellt sind, an die Einrichtungen des Justiz- und Maßregelvollzugs übermitteln, wenn diese Daten für den Vollzug der Freiheitsentziehung, insbesondere zur Förderung der Vollzugs- und Behandlungsplanung oder der Entlassungsvorbereitung, erforderlich sind; das Gleiche gilt für Mitteilungen an Vollstreckungsbehörden, soweit diese Daten für die in § 477 Absatz 2 Nummer 1 oder 3 genannten Zwecke erforderlich sind.

(2) Außerdem kann, unbeschadet des § 57 des Bundesdatenschutzgesetzes, Auskunft 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.

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zu einer weitergehenden Prüfung der Zulässigkeit der Übermittlung besteht.

(4) Die nach den §§ 483 bis 485 gespeicherten Daten dürfen auch für wissenschaftliche Zwecke übermittelt werden. § 476 gilt entsprechend.

(5) Besondere gesetzliche Bestimmungen, die die Übermittlung von Daten aus einem Strafverfahren anordnen oder erlauben, bleiben unberührt.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(6) Die Daten dürfen nur zu dem Zweck verwendet werden, für den sie übermittelt worden sind. Eine Verwendung für andere Zwecke ist zulässig, soweit die Daten auch dafür hätten übermittelt werden dürfen.
<p>Article 35 – 24/7 Network</p> <p>1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:</p> <p>a the provision of technical advice;</p> <p>b the preservation of data pursuant to Articles 29 and 30;</p> <p>c the collection of evidence, the provision of legal information, and locating of suspects.</p> <p>2 a A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.</p> <p>b If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.</p> <p>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	<p>Bundeskriminalamt, Fachbereich SO42-1 SO 42 (High Technology Crime) Working Languages: German, English</p> <p>Address: Bundeskriminalamt, Thaerstr. 11 65193 Wiesbaden, Germany</p>
<p>Article 42 – Reservations</p> <p>By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.</p>	<p><u><i>Reservation regarding Art. 42</i></u></p>