HAMBURGISCHES GESETZ- UND VERORDNUNGSBLATT

TEIL I

HmbGVBl. Nr. 38 | FREITAG, DEN 25. OKTOBER | 2019

Gesetz über den Einsatz der Informations- und Kommunikationstechnik bei Gerichten und Staatsanwaltschaften der Freien und Hansestadt Hamburg (IT-Justizgesetz – HmbITJG)

Vom 23. Oktober 2019

Der Senat verkündet das nachstehende von der Bürgerschaft beschlossene Gesetz:

§ 1
Regelungszweck und Geltungsbereich

(1) Bei Organisation und Betrieb von Informations- und Kommunikationstechnik (IT) für die Gerichte und Staatsanwaltschaften sind die richterliche Unabhängigkeit, die sachliche Unabhängigkeit der Rechtspflegerinnen und Rechtspfleger sowie das Legalitätsprinzip in der Strafverfolgung zu beachten und besonders zu schützen. Insbesondere sollen die Integrität und die Vertraulichkeit der Entscheidungsprozesse geschützt werden. Zudem ist die Funktionsfähigkeit der Justiz zu sichern.

(2) Der Einsatz von IT darf nicht zur Ausweitung von Verhaltens- und Leistungskontrollen im richterlichen Bereich führen.

(3) Das Gesetz regelt zur Gewährleistung dieser Ziele organisatorische und rechtliche Rahmenbedingungen des IT-Betriebes für die Gerichte und Staatsanwaltschaften einschließlich des Hamburgischen Verfassungsgerichtes.

(4) Die jeweils anwendbaren datenschutzrechtlichen Regelungen bleiben von diesem Gesetz unberührt. Sie finden auf die Verarbeitung personenbezogener Daten vorrangig Anwendung.

§ 2
Verantwortlichkeit

(1) Die zuständige Behörde stellt durch geeignete Maßnahmen die Einhaltung der Ziele und Vorschriften dieses Gesetzes sicher.

(2) Die Aktenhoheit liegt bei dem jeweils zuständigen Gericht beziehungsweise der jeweils zuständigen Staatsanwaltschaft.

(3) Die Einhaltung der Ziele und Vorschriften dieses Gesetzes wird durch ein unabhängiges Kontrollgremium (IT-Kontrollkommission) überwacht.

§ 3
Zu schützende Daten, Prozesse und Personen; unmittelbar Berechtigte

(1) Zu schützen sind die gesamten Prozesse der richterlichen, rechtspflegerischen oder staatsanwaltschaftlichen Entscheidungsfindung und die Entscheidungen selbst.

(2) Zu den zu schützenden Daten zählen im Rahmen der geschützten Prozesse insbesondere:

1. sämtliche erstellten, erhaltenen oder weiterverarbeiteten elektronischen Dokumente oder sonstigen Daten einschließlich aller Metadaten (Inhaltsdaten),
2. verfahrensbezogene Daten, die in Fachverfahren, in der elektronischen Akte oder in sonstigen Programmen oder Datenspeichern – auch nur zeitlich befristet – erfasst werden (Verfahrensdaten),
3. systemintern automatisch erstellte Daten über die Benutzung der zur Verfügung stehenden IT (Logdaten).

(3) Inhaltsdaten, welche die richterliche, rechtspflegerische oder staatsanwaltschaftliche Entscheidungsfindung ganz oder teilweise dokumentieren, sowie Verfahrensdaten, die Rückschlüsse auf den Prozess der Entscheidungsfindung ermöglichen, sind besonders geschützt. Umfassend geschützt sind Entwürfe zu Urteilen, Beschlüssen und Verfügungen, die Arbeiten zu ihrer Vorbereitung, Annotationen zu Dokumenten und die Dokumente, die Beratungen und Abstimmungen betreffen, sowie die auf die IT-Nutzung durch geschützte Amtsträger bezogenen Log- und Metadaten.

(4) Besonders geschützt sind Richterinnen und Richter, Rechtspflegerinnen und Rechtspfleger, Staatsanwältinnen und Staatsanwälte sowie Amtsanwältinnen und Amtsanwälte (geschützte Amtsträgerinnen und Amtsträger).

(5) Unmittelbar berechtigt für jede Art des Umganges mit den jeweiligen Daten sind die mit der Verfahrensbearbeitung betrauten Amtsträgerinnen und Amtsträger der Gerichte und Staatsanwaltschaften im Rahmen ihrer jeweiligen Zuständigkeit (unmittelbar Berechtigte). Zuständigkeiten können sich auf Grund gesetzlicher Vorschriften, aus den Geschäftsverteilungsplänen der Gerichte und aus Regelungen im Rahmen der Organisationshoheit der Leitungen der Gerichte und Staatsanwaltschaften sowie im nichtrichterlichen Bereich der Landesjustizverwaltung ergeben.

§ 4

Technische, betriebliche und organisatorische Maßnahmen

(1) Im Anwendungsbereich des § 3 sind bei der Ausgestaltung der zur Verarbeitung von Daten eingesetzten Anwendungssoftware und dem Betrieb der IT die Grundsätze der Datensparsamkeit und Datenvermeidung zu beachten.

(2) Die in der Datenverarbeitung tätigen Auftragsverarbeiter sowie in der Datenverarbeitung tätige Dienststellen (datenverarbeitende Stellen) haben eine sichere Verarbeitung der zu schützenden Daten unter Beachtung des Standes der Technik zu gewährleisten.

(3) Bei dem Betrieb der IT und der Datenverarbeitung haben sie unter Beachtung des Standes der Technik insbesondere sicherzustellen, dass

1. keine unbefugten Einsichtnahmen und Eingriffe in die richterliche, rechtspflegerische und staatsanwaltschaftliche Tätigkeit erfolgen,
2. unbefugte Übermittlungen und sonstige Verarbeitungen nach § 3 geschützter Daten unterbleiben,
3. keine unbefugten Veränderungen der technischen Zugriffsberechtigungen erfolgen und
4. die Funktionsfähigkeit der IT nicht eingeschränkt wird.

(4) Die datenverarbeitenden Stellen erstellen Sicherheitskonzepte, die eine effektive Kontrolle durch die IT-Kontrollkommission und die zuständige Behörde gewährleisten. Dazu gehört die Etablierung geeigneter Mechanismen zur internen Kontrolle, mittels derer sicherheitsrelevante Betriebsabläufe und Zustände regelmäßig nachvollziehbar daraufhin überprüft werden, ob unbefugte Zugriffe, Unregelmäßigkeiten oder Probleme des ordnungsgemäßen Betriebs aufgetreten sind. Zugriffe durch Administratorinnen und Administratoren sind revisionssicher zu protokollieren, es sei denn, der Zugriff erfolgt mit ausdrücklicher Einwilligung der oder des unmittelbar Berechtigten. Die Einwilligung soll protokolliert werden. Die Konzepte und Protokolle sind der zuständigen Behörde, den Leitungen der Gerichte und Staatsanwaltschaften für ihren jeweiligen Geschäftsbereich sowie der IT-Kontrollkommission auf Verlangen zugänglich zu machen.

(5) Die Inhaberinnen und Inhaber administrativer Zugänge sind der IT-Kontrollkommission sowie für ihren jeweiligen Geschäftsbereich den Leitungen der Gerichte und Staatsanwaltschaften bekanntzugeben.

(6) Sicherheitsrelevante Ereignisse sind der IT-Kontrollkommission, der zuständigen Behörde und den Leitungen der Gerichte und Staatsanwaltschaften innerhalb angemessener Frist zu melden.

(7) Der Senat wird ermächtigt, Einzelheiten zu den technischen Anforderungen, zu internen Kontrollmechanismen, zur Protokollierung und den Aufbewahrungsfristen, zu Meldepflichten im Sinne des Absatzes 6 und zu den Sicherheitskonzepten durch Rechtsverordnung zu regeln. Der Senat kann die Ermächtigung durch Rechtsverordnung auf die zuständige Behörde weiter übertragen. Bei Erlass oder Änderungen der Verordnung nach Satz 1 sind die Leitungen der Gerichte und Staatsanwaltschaften sowie die IT-Kontrollkommission zu beteiligen.

§ 5

Behandlung der Daten und Prozesse

(1) Einsichtnahmen und Eingriffe in die geschützten Daten und Prozesse sind grundsätzlich nur Berechtigten gestattet, soweit es zur Erfüllung ihrer Aufgabe erforderlich ist. Einsichtnahmen und Eingriffe in die in § 3 Absatz 3 Satz 2 genannten Daten sind im richterlichen Bereich nur zulässig mit Einwilligung der unmittelbar berechtigten Richterinnen und Richter oder auf Grund zwingender technischer Erfordernisse. Die betroffenen Richterinnen und Richter sind über technisch bedingte Eingriffe nach Möglichkeit angemessen zu informieren.

(2) Neben den unmittelbar Berechtigten sind weitere Amtsträgerinnen und Amtsträger der Gerichte und Staatsanwaltschaften sowie die in den datenverarbeitenden Stellen tätigen Beschäftigten nur berechtigt, soweit sich das aus

1. der Einwilligung der unmittelbar Berechtigten,
2. gesetzlichen Vorschriften, insbesondere auch zur Dienstaufsicht, unter Beachtung des Absatzes 3,
3. Erfordernissen des technischen IT-Betriebes oder
4. dem zwingenden Erfordernis, eine unmittelbar bevorstehende Gefahr für die Schutzgüter des § 1 Absatz 1 und des § 3 abzuwehren,

ergibt. Im Einzelfall sowie für regelmäßig wiederkehrende Fälle kann die IT-Kontrollkommission außerhalb des Bereiches des § 3 Absatz 3 Satz 2, höchstens für die Dauer ihrer jeweiligen Amtszeit, aus wichtigen dienstlichen Gründen Eingriffe zulassen, etwa wenn eine Einwilligung wegen der großen Zahl der Betroffenen nicht von allen zuständigen Amtsträgerinnen und Amtsträgern eingeholt werden kann oder wenn unklar ist, welche Personen betroffen sind oder dies nur mit einem unverhältnismäßig hohen Aufwand ermittelt werden kann; die Betroffenen sind hierüber nach Möglichkeit zu informieren.

(3) Statistik im richterlichen Bereich der Justiz darf ausschließlich aus hinreichend aggregierten und anonymisierten Daten im Sinne des § 3 Absatz 2 Nummer 2, soweit sie in Fachverfahren erfasst werden, erstellt werden. Die erforderlichen Daten werden von den jeweiligen Leitungen der Gerichte an das Statistische Amt für Hamburg und Schleswig-Holstein – Anstalt des öffentlichen Rechts – oder an eine andere hierfür unter Beachtung der Grundsätze des § 5 Absatz 2 des Hamburgischen Statistikgesetzes vom 19. März 1991 (HmbGVBl. S. 79, 474), zuletzt geändert am 17. Februar 2009 (HmbGVBl. S. 29, 34), in der jeweils geltenden Fassung bestimmte Stelle übermittelt. An eine andere entsprechende Stelle können die Daten auch vom Statistischen Amt für Hamburg und Schleswig-Holstein – Anstalt des öffentlichen Rechts – weiterübermittelt werden. Eine Weitergabe der übermittelten nicht aggregierten Daten an weitere Stellen oder ein Zugriff auf die übermittelten nicht aggregierten Daten durch sonstige Dritte ist unzulässig. Zu anderen, auch statistischen Zwecken können anonymisierte Daten im Sinne des § 3 Absatz 2 Nummern 1 und 2 von den Leitungen der Gerichte bei hinreichender Beachtung der zu schützenden Interessen übermittelt oder freigegeben werden, wenn diese Daten – soweit möglich – aggregiert sind und sichergestellt ist, dass aus diesen kein Rückschluss auf einzelne Richterinnen und Richter gezogen wird und sie nicht für eine Beobachtung, Analyse und Kontrolle von Verhalten und Leistung der Richterinnen und Richter beziehungsweise Kollegialspruchkörper verwendet werden. Die für die Geschäftsverteilung und die Dienstaufsicht unter Berücksichtigung des § 1 Absätze 1 und 2 erforderlichen Daten gemäß § 3 Absatz 2 Nummer 2 stehen der jeweiligen Leitung des Gerichtes und dem Präsidium im Rahmen ihrer Zuständigkeit zur Verfügung. Entsprechendes gilt für den Kollegialspruchkörper. Über weitergehende interne Auswertungen können die Leitungen der Gerichte mit den Richterräten Dienstvereinbarungen schließen.

(4) Die datenverarbeitenden Stellen erstellen nach Maßgabe der vorstehenden Bestimmungen Konzepte für die Zuordnung von technischen Berechtigungen und den Zugriff auf Daten und Prozesse nach § 3 durch Administratorinnen und Administratoren. Einzelne geschützte Amtsträgerinnen und Amtsträger, die Leitungen der Gerichte und Staatsanwaltschaften sowie Richter- und Personalräte haben im Einzelfall das Recht, die Konzepte und deren Umsetzung einzusehen, soweit Daten und Prozesse nach § 3 betroffen sind.

(5) Soweit für die Einrichtung und den Betrieb der IT Auftragsverarbeiter, einzelne Dienststellen der Justiz oder Dritte eingeschaltet werden, ist die Einhaltung der Vorschriften dieses Gesetzes, gegebenenfalls vertraglich, sicherzustellen. Bei wesentlichen Veränderungen oder dem Neuabschluss von Verträgen ist die IT-Kontrollkommission zu beteiligen.

(6) Der Senat wird ermächtigt, Einzelheiten der Ausgestaltung der Konzepte gemäß Absatz 4 durch Rechtsverordnung zu regeln. Der Senat kann die Ermächtigung durch Rechtsverordnung auf die zuständige Behörde weiter übertragen. Bei Erlass oder Änderungen der Verordnung nach Satz 1 sind die Leitungen der Gerichte und die Staatsanwaltschaften sowie die IT-Kontrollkommission zu beteiligen.

§ 6
IT-Kontrollkommission

(1) Die IT-Kontrollkommission wird bei der zuständigen Behörde eingerichtet. Diese hält für sie eine Koordinierungsstelle vor, stellt ihr die für die Wahrnehmung ihrer Aufgaben erforderlichen Mittel zur Verfügung und trägt die durch ihre Tätigkeit entstehenden Kosten.

(2) Die IT-Kontrollkommission besteht aus

1. vier Vertreterinnen beziehungsweise Vertretern der Richterschaft,
2. einer Staatsanwältin beziehungsweise einem Staatsanwalt oder einer Amtsanwältin beziehungsweise einem Amtsanwalt sowie
3. einer Rechtspflegerin beziehungsweise einem Rechtspfleger

mit gleichem Stimmrecht. Der Kommission gehören ferner als beratende Mitglieder zwei Vertreterinnen beziehungsweise Vertreter der Gerichtsleitungen sowie zwei Angehörige der zuständigen Behörde (behördliche Mitglieder) an. Zwei der Mitglieder nach Satz 1 Nummer 1 werden gemeinsam von den Richterräten gemäß § 29 Absatz 1 Nummern 1 bis 3 des Hamburgischen Richtergesetzes (HmbRiG) vom 2. Mai 1991 (HmbGVBl. S. 169), zuletzt geändert am 4. April 2017 (HmbGVBl. S. 96, 97), in der jeweils geltenden Fassung, die zwei weiteren gemeinsam von den Richterräten gemäß § 29 Absatz 1 Nummern 4 bis 8 HmbRiG, das Mitglied nach Satz 1 Nummer 2 vom Personalrat der Staatsanwaltschaften, das Mitglied nach Satz 1 Nummer 3 gemeinsam von den Personalräten der Gerichte und Staatsanwaltschaften gewählt. Die Amtszeit der Mitglieder beträgt drei Jahre. Für ausgeschiedene Mitglieder werden entsprechend Satz 3 neue Mitglieder für die restliche Amtszeit nachgewählt. Der Präses der zuständigen Behörde benennt die behördlichen Mitglieder, die Gerichtsleitungen benennen ihre Vertreterinnen beziehungsweise Vertreter.

(3) Für die Beratung konkreter Vorgänge ist auf Antrag mindestens zweier – auch nicht stimmberechtigter – Mitglieder eine Vertreterin beziehungsweise ein Vertreter der Leitung des betroffenen Gerichtes oder der betroffenen Staatsanwaltschaft hinzuzuziehen.

(4) Die IT-Kontrollkommission trifft ihre Entscheidungen mit der Mehrheit der stimmberechtigten Mitglieder. Die IT-Kontrollkommission gibt sich eine Geschäftsordnung. Sie kann durch Beschluss Befugnisse auf einzelne Mitglieder übertragen.

(5) Die Beratungen der IT-Kontrollkommission sind grundsätzlich vertraulich, Einzelheiten regelt die Geschäftsordnung. Die Mitglieder der IT-Kontrollkommission sind zur Verschwiegenheit verpflichtet, soweit das zum Schutz der Rechte Einzelner, zum Schutz von Betriebs- und Geschäftsgeheimnissen oder zur Gewährleistung der IT-Sicherheit erforderlich ist. Absatz 3 sowie § 7 Absätze 3 und 4 sowie § 8 bleiben unberührt.

(6) Die Mitglieder der IT-Kontrollkommission mit Ausnahme der Vertreterinnen beziehungsweise Vertreter der Gerichtsleitungen sind von ihrer dienstlichen Tätigkeit teilweise freizustellen, wenn und soweit es zur ordnungsgemäßen Durchführung ihrer Aufgaben erforderlich ist; für nicht freigestellte Mitglieder ist eine angemessene Aufwandsentschädigung nach § 3 Nummer 12 des Einkommensteuergesetzes in der Fassung vom 8. Oktober 2009 (BGBl. I S. 3369, 3862), zuletzt geändert am 25. März 2019 (BGBl. I S. 357), in der jeweils geltenden Fassung vorzusehen.

(7) Der Senat wird ermächtigt, weitere Einzelheiten der Wahl und der Amtszeit der Mitglieder nach Absatz 2 Satz 1 Nummern 1 bis 3, der Bestimmung und der Amtszeit der beratenden Mitglieder, der Beschlussfassung in der IT-Kontrollkommission sowie der Freistellung und der Aufwandsentschädigung der Mitglieder der Kommission durch Rechtsverordnung zu regeln. Der Senat kann die Ermächtigung durch Rechtsverordnung auf die zuständige Behörde weiter übertra-

gen. Bei Erlass oder Änderungen der Verordnung nach Satz 1 sind die Leitungen der Gerichte und die Staatsanwaltschaften sowie die IT-Kontrollkommission zu beteiligen.

§ 7

Kontrollrechte der IT-Kontrollkommission

(1) Die IT-Kontrollkommission kann sowohl anlassbezogen als auch verdachtsunabhängig, zur Aufdeckung von Verstößen und Missbrauch oder vorbeugend, Einsicht in alle Datenverarbeitungsvorgänge gemäß §§ 4 und 5 nehmen und alle dabei anfallenden Daten zur Erfüllung ihrer Aufgaben nach diesem Gesetz verarbeiten. Sie kann ferner Einsicht in alle die IT betreffenden Verträge und Konzepte nehmen sowie auch Inaugenscheinnahmen der IT-Einrichtungen vornehmen. Soweit erforderlich kann sie auch Auskünfte von den datenverarbeitenden Stellen einholen. Einsichtnahmen in geschützte Daten und Prozesse im Sinne des § 3 Absatz 2 Nummer 1 und Absatz 3 Satz 2 sind unbeschadet des § 5 Absatz 1 nur gestattet, soweit sie zur Aufgabenerfüllung geboten sind. Die Rechte nach den Sätzen 1 bis 3 stehen auch einer Minderheit von mindestens zwei stimmberechtigten Mitgliedern zu.

(2) Die Ergebnisse der Überprüfungen nach § 4 Absatz 4 Satz 2 sind der IT-Kontrollkommission auf Verlangen zugänglich zu machen.

(3) Soweit dies zur ordnungsgemäßen Erfüllung ihrer Aufgaben erforderlich ist, kann die IT-Kontrollkommission sachkundige Dritte, auch aus den Gerichtsverwaltungen oder der zuständigen Behörde, hinzuziehen. Soweit die Hinzuziehung externer Sachverständiger im Einzelfall erforderlich ist, vergibt die zuständige Behörde unter Beteiligung der IT-Kontrollkommission die Aufträge und trägt die Kosten; Rückgriffsforderungen nach sonstigen Vorschriften bleiben unbenommen.

(4) Stellt die IT-Kontrollkommission Verstöße gegen die Bestimmungen dieses Gesetzes fest, so unterrichtet sie die zuständige Behörde, die betroffene Dienststelle sowie gegebenenfalls den jeweiligen IT-Dienstleister und, sofern sie das für geboten erachtet, die Betroffenen. Ferner fordert sie die verantwortlichen Stellen unter Setzung einer angemessenen Frist zur Beseitigung auf. Handelt es sich um einen erheblichen Verstoß oder erfolgt keine fristgerechte Beseitigung, so spricht die IT-Kontrollkommission eine Beanstandung aus. Die zuständige Behörde ist verpflichtet, auf Beanstandungen im Rahmen ihrer Zuständigkeit angemessen zu reagieren und die IT-Kontrollkommission sowie die Leitungen der Gerichte und Staatsanwaltschaften über ergriffene Maßnahmen zu unterrichten.

(5) Einzelne geschützte Amtsträgerinnen und Amtsträger, die Leitungen der Gerichte und Staatsanwaltschaften sowie Richter- und Personalräte haben das Recht, sich in Verdachtsfällen oder mit konkreten Beschwerden an die IT Kontrollkommission zu wenden.

(6) Außerhalb der bei den Gerichten im Rahmen ihrer justitiellen Tätigkeit vorgenommenen Datenverarbeitung wird die IT-Kontrollkommission zum Schutz personenbezogener Daten nicht tätig.

§ 8

Berichte

(1) Die IT-Kontrollkommission erstellt jährlich zum 31. Oktober einen Bericht über die Organisation und den Einsatz der IT in den Gerichten und Staatsanwaltschaften. Der Bericht enthält auch eine Darstellung zur Gewährleistung der Ziele dieses Gesetzes. Die IT-Sicherheit und die Rechte Einzelner sind bei der Erstellung des Berichtes zu beachten.

(2) Der Bericht ist den Richter- und Personalvertretungen, den Leitungen der Gerichte und Staatsanwaltschaften sowie der zuständigen Behörde unverzüglich zuzuleiten.

(3) Besteht nach Auffassung der zuständigen Behörde, der Leitung eines Gerichts, der Leitung einer Staatsanwaltschaft oder eines zuständigen Richter- oder Personalrates die Besorgnis einer über einen Einzelfall hinausgehenden Verletzung der in § 1 Absatz 1 genannten Schutzgüter, so ist auch außerhalb der Frist nach Absatz 1 zu berichten.

§ 9

Verhältnis zu anderen Regelungen, Übergangsregelungen, Evaluation

(1) Die Vorschriften des Hamburgischen Richtergesetzes und des Hamburgischen Personalvertretungsgesetzes zur Mitbestimmung, diejenigen des Hamburgischen Beamtengesetzes zur Verbändebeteiligung sowie der Dataport-Staatsvertrag vom 27. August 2003 (HmbGVBl. S. 590), zuletzt geändert vom 6. August 2013 bis 27. September 2013 (HmbGVBl. 2014 S. 52), bleiben unberührt.

(2) Spätestens vier Jahre nach seinem Inkrafttreten überprüft der Senat dieses Gesetz im Hinblick auf seine Anwendung und Auswirkungen, berücksichtigt dabei die Berichte der IT-Kontrollkommission und berichtet der Bürgerschaft über das Ergebnis.

(3) Ist zum Zeitpunkt des Erlasses oder der Änderung einer Verordnung nach § 4 Absatz 7 Satz 1, § 5 Absatz 6 Satz 1 und § 6 Absatz 7 Satz 1 eine IT-Kontrollkommission noch nicht gebildet, so treten an ihre Stelle die Richter- und Personalräte der Gerichte sowie der Personalrat der Staatsanwaltschaften. Gleiches gilt für die Zulassung von Eingriffen nach § 5 Absatz 2 Satz 2.

(4) Soweit zum Zeitpunkt des Inkrafttretens dieses Gesetzes Vorgaben wegen bestehender technischer Gegebenheiten noch nicht vollständig verwirklicht werden können, wirken die jeweiligen datenverarbeitenden Stellen auf die möglichst baldige Umsetzung hin.

Ausgefertigt Hamburg, den 23. Oktober 2019.

Der Senat

Herausgegeben von der Justizbehörde der Freien und Hansestadt Hamburg.
Druck, Verlag und Ausgabestelle Lütcke & Wulff, Rondenbarg 8, 22525 Hamburg, — Telefon: 23 51 29-0 — Telefax: 23 51 29 77.
Bestellungen nimmt der Verlag entgegen. Bezugspreis für Teil I und II zusammen jährlich 75,– Euro. Einzelstücke je angefangene vier Seiten 0,26 Euro (Preise einschließlich 7 % Mehrwertsteuer).