Ich verpflichte mich im Zusammenhang mit meiner Tätigkeit im/am AKH/Magistrat der Stadt Wien/Wiener Gesundheitsverbund

1. zu absoluter Verschwiegenheit über alle Tatsachen, die mir anlässlich meiner Tätigkeit bekanntwerden und
2. zur Wahrung des Datengeheimnisses nach dem Datenschutzgesetz.

Das bedeutet, dass ich alle Daten, die mir im Rahmen meiner Tätigkeit bekannt werden

a) geheim halten muss

b) nur im Auftrag eines anordnungsbefugten Bediensteten der Stadt Wien an andere Personen übermitteln darf und

c) auch nach Beendigung meiner Tätigkeit im AKH weiterhin geheim halten muss.

3. die Richtlinie "Informationssicherheit - Vorgaben für EDV- / IKT-Anwender*innen“ http://intranet.akhwien.at/default.aspx?cid=18955 (gem. dem AKH-Erlass AKH/R/21/2018 vom 25.06.2018) zur Kenntnis zu nehmen und die darin festgelegten Regeln und und Anweisungen unbedingt einzuhalten.

Die Pflichten zur Geheimhaltung gelten sowohl für automationsunterstützt verarbeitete als auch für manuell (z.B. im Rahmen eines Aktes oder mittels Dateikartenkästen) geführte Daten.

Ich bestätige hiermit meine Teilnahme und nehme weiter folgende genannten Vorschriften zur Kenntnis (Auszug in der Anlage):

1) Bestimmungen des Strafgesetzbuches
2) Bestimmungen des Datenschutzgesetzes (DSG)
3) Bestimmungen der Datenschutz-Grundverordnung (DSGVO)
4) Bestimmungen des Urheberrechtsgesetzes
5) Information zur Verarbeitung personenbezogener Daten im Rahmen einer Anmeldung/Teilnahme

Dienstgeber*in: ----------

(z.B. Name Firma, Ausbildungsinstitut, MUW etc.)

Berufsgruppe: ----------

(z.B. Pflege, Verwaltung, EDV, dienstzugeteiltes Personal, BeobachterIn, DiplomandIn, StudentIn etc.)

Name (leserlich)	Geb. Datum	Datum	Unterschrift
----------	----------	----------	----------

1. Bestimmungen des Strafgesetzbuches – StGB, BGBl. Nr. 60/1974 idgF

Hinweis: vom Schutzbereich des StGB sind auch nicht personenbezogene Daten umfasst!

Besondere Erschwerungsgründe

§ 33. (1) Ein Erschwerungsgrund ist es insbesondere, wenn der Täter

[…]

8. die Tat unter Missbrauch der personenbezogenen Daten einer anderen Person begangen hat, um das Vertrauen eines Dritten zu gewinnen, wodurch dem rechtmäßigen Identitätseigentümer ein Schaden zugefügt wird.

Andere Begriffsbestimmungen

§ 74. (1) Im Sinn dieses Bundesgesetzes ist

[…]

11. kritische Infrastruktur: Einrichtungen, Anlagen, Systeme oder Teile davon, die eine wesentliche Bedeutung für die Aufrechterhaltung der öffentlichen Sicherheit und der Landesverteidigung, die Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie, die Verhütung oder Bekämpfung von Katastrophen, den öffentlichen Gesundheitsdienst, die öffentliche Versorgung mit Wasser, Energie sowie lebenswichtigen Gütern, des öffentlichen Abfallentsorgungs- und Kanalwesens oder den öffentlichen Verkehr haben.

Widerrechtlicher Zugriff auf ein Computersystem

§ 118a.

(1) Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft,

1. sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder
2. einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe

bis zu 360 Tagessätzen zu bestrafen.

(2) Wer die Tat in Bezug auf ein Computersystem, das ein wesentlicher Bestandteil der kritischen Infrastruktur (§ 74 Abs. 1 Z 11) ist, begeht, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(3) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

(4) Wer die Tat nach Abs. 1 im Rahmen einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu zwei Jahren, wer die Tat nach Abs. 2 im Rahmen einer kriminellen Vereinigung begeht, mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Verletzung des Telekommunikationsgeheimnisses

§ 119. (1) Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Missbräuchliches Abfangen von Daten

§ 119a. (1) Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Missbrauch von Tonaufnahme- oder Abhörgeräten

§ 120.

[…]

(2a) Wer eine im Wege einer Telekommunikation übermittelte und nicht für ihn bestimmte Nachricht in der Absicht, sich oder einem anderen Unbefugten vom Inhalt dieser Nachricht Kenntnis zu verschaffen, aufzeichnet, einem anderen Unbefugten zugänglich macht oder veröffentlicht, ist, wenn die Tat nicht nach den vorstehenden Bestimmungen oder nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, mit Freiheitsstrafe bis zu drei Monaten oder mit Geldstrafe bis zu 180 Tagessätzen zu bestrafen.

(3) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Verletzung von Berufsgeheimnissen

§ 121. (1) Wer ein Geheimnis offenbart oder verwertet, das den Gesundheitszustand einer Person betrifft und das ihm bei berufsmäßiger Ausübung eines gesetzlich geregelten Gesundheitsberufes oder bei berufsmäßiger Beschäftigung mit Aufgaben der Verwaltung einer Krankenanstalt oder eines anderen Gesundheitsdiensteanbieters (§ 2 Z 2 des Gesundheitstelematikgesetzes 2012, BGBl. I Nr. 111/2012) oder mit Aufgaben der Kranken-, der Unfall-, der Lebens- oder der Sozialversicherung ausschließlich kraft seines Berufes anvertraut worden oder zugänglich geworden ist und dessen Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse der Person zu verletzen, die seine Tätigkeit in Anspruch genommen hat oder für die sie in Anspruch genommen worden ist, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(1a) Ebenso ist zu bestrafen, wer widerrechtlich von einer Person die Offenbarung (Einsichtnahme oder Verwertung) von Geheimnissen ihres Gesundheitszustandes in der Absicht verlangt, den Erwerb oder das berufliche Fortkommen dieser oder einer anderen Person für den Fall der Weigerung zu schädigen oder zu gefährden.

(2) Wer die Tat begeht, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

(3) Ebenso ist ein von einem Gericht oder einer anderen Behörde für ein bestimmtes Verfahren bestellter Sachverständiger zu bestrafen, der ein Geheimnis offenbart oder verwertet, das ihm ausschließlich kraft seiner Sachverständigentätigkeit anvertraut worden oder zugänglich geworden ist und dessen Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse der Person zu verletzen, die seine Tätigkeit in Anspruch genommen hat oder für die sie in Anspruch genommen worden ist.

(4) Den Personen, die eine der in den Abs. 1 und 3 bezeichneten Tätigkeiten ausüben, stehen ihre Hilfskräfte, auch wenn sie nicht berufsmäßig tätig sind, sowie die Personen gleich, die an der Tätigkeit zu Ausbildungszwecken teilnehmen.

(5) Der Täter ist nicht zu bestrafen, wenn die Offenbarung oder Verwertung nach Inhalt und Form durch ein öffentliches oder ein berechtigtes privates Interesse gerechtfertigt ist.

(6) Der Täter ist nur auf Verlangen des in seinem Interesse an der Geheimhaltung Verletzten (Abs. 1 und 3) zu verfolgen.

Verletzung eines Geschäfts- oder Betriebsgeheimnisses

§ 122. (1) Wer ein Geschäfts- oder Betriebsgeheimnis (Abs. 3) offenbart oder verwertet, das ihm bei seiner Tätigkeit in Durchführung einer durch Gesetz oder behördlichen Auftrag vorgeschriebenen Aufsicht, Überprüfung oder Erhebung anvertraut oder zugänglich geworden ist, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer die Tat begeht, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

(3) Unter Abs. 1 fällt nur ein Geschäfts- oder Betriebsgeheimnis, das der Täter kraft Gesetzes zu wahren verpflichtet ist und dessen Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse des von der Aufsicht, Überprüfung oder Erhebung Betroffenen zu verletzen.

(4) Der Täter ist nicht zu bestrafen, wenn die Offenbarung oder Verwertung nach Inhalt und Form durch ein öffentliches oder ein berechtigtes privates Interesse gerechtfertigt ist.

(5) Der Täter ist nur auf Verlangen des in seinem Interesse an der Geheimhaltung Verletzten (Abs. 3) zu verfolgen.

Datenbeschädigung

§ 126a.

(1) Wer einen anderen dadurch schädigt, daß er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer durch die Tat an den Daten einen 5 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(3) Wer durch die Tat viele Computersysteme unter Verwendung eines Computerprogramms, eines Computerpasswortes, Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden, beeinträchtigt, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(4) Mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren ist zu bestrafen, wer

1. durch die Tat einen 300 000 Euro übersteigenden Schaden herbeiführt,
2. durch die Tat wesentliche Bestandteile der kritischen Infrastruktur (§ 74 Abs. 1 Z 11) beeinträchtigt, oder
3. die Tat als Mitglied einer kriminellen Vereinigung begeht.

Störung der Funktionsfähigkeit eines Computersystems

§ 126b.

(1) Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer durch die Tat eine längere Zeit andauernde Störung der Funktionsfähigkeit eines Computersystems herbeiführt, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(3) Wer durch die Tat viele Computersysteme unter Verwendung eines Computerprogramms, eines Computerpasswortes, eines Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden, schwer stört, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

(4) Mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren ist zu bestrafen, wer

1. durch die Tat einen 300 000 Euro übersteigenden Schaden herbeiführt,
2. durch die Tat wesentliche Bestandteile der kritischen Infrastruktur (§ 74 Abs. 1 Z 11) beeinträchtigt, oder
3. die Tat als Mitglied einer kriminellen Vereinigung begeht.

Missbrauch von Computerprogrammen oder Zugangsdaten

§ 126c. (1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder
2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen,

mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs. 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a, 126b oder 148a bezeichneten Weise gebraucht werden. Besteht die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.

Schwerer Diebstahl

§ 128. (1) Mit Freiheitsstrafe bis zu drei Jahren ist zu bestrafen, wer einen Diebstahl begeht

[…]

4. an einem wesentlichen Bestandteil der kritischen Infrastruktur (§ 74 Abs. 1 Z 11), oder

[…]

Betrügerischer Datenverarbeitungsmißbrauch

§ 148a. (1) Wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einen anderen dadurch am Vermögen schädigt, daß er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflußt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Wer die Tat gewerbsmäßig begeht oder durch die Tat einen 5 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu drei Jahren, wer durch die Tat einen 300 000 Euro übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

Mißbrauch der Amtsgewalt

§ 302. (1) Ein Beamter, der mit dem Vorsatz, dadurch einen anderen an seinen Rechten zu schädigen, seine Befugnis, im Namen des Bundes, eines Landes, eines Gemeindeverbandes, einer Gemeinde oder einer anderen Person des öffentlichen Rechtes als deren Organ in Vollziehung der Gesetze Amtsgeschäfte vorzunehmen, wissentlich mißbraucht, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.

(2) Wer die Tat bei der Führung eines Amtsgeschäfts mit einer fremden Macht oder einer über- oder zwischenstaatlichen Einrichtung begeht, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen. Ebenso ist zu bestrafen, wer durch die Tat einen 50 000 Euro übersteigenden Schaden herbeiführt.

Verletzung des Amtsgeheimnisses

§ 310. (1) Ein Beamter oder ehemaliger Beamter, der ein ihm ausschließlich kraft seines Amtes anvertrautes oder zugänglich gewordenes Geheimnis offenbart oder verwertet, dessen Offenbarung oder Verwertung geeignet ist, ein öffentliches oder ein berechtigtes privates Interesse zu verletzen, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, mit
Freiheitsstrafe bis zu drei Jahren zu bestrafen.

[…]

2. Bestimmungen des Datenschutzgesetzes – DSG , BGBl. I Nr. 165/1999 idgF

Datengeheimnis

§ 6. (1) Der Verantwortliche, der Auftragsverarbeiter und ihre Mitarbeiter – das sind Arbeitnehmer (Dienstnehmer) und Personen in einem arbeitnehmerähnlichen (dienstnehmerähnlichen) Verhältnis – haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten besteht (Datengeheimnis).

(2) Mitarbeiter dürfen personenbezogene Daten nur auf Grund einer ausdrücklichen Anordnung ihres Arbeitgebers (Dienstgebers) übermitteln. Der Verantwortliche und der Auftragsverarbeiter haben, sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht, diese vertraglich zu verpflichten, personenbezogene Daten aus Datenverarbeitungen nur aufgrund von Anordnungen zu übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses (Dienstverhältnisses) zum Verantwortlichen oder Auftragsverarbeiter einzuhalten.

(3) Der Verantwortliche und der Auftragsverarbeiter haben die von der Anordnung betroffenen Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Unbeschadet des verfassungsrechtlichen Weisungsrechts darf einem Mitarbeiter aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen.

(5) Ein zugunsten eines Verantwortlichen bestehendes gesetzliches Aussageverweigerungsrecht darf nicht durch die Inanspruchnahme eines für diesen tätigen Auftragsverarbeiters, insbesondere nicht durch die Sicherstellung oder Beschlagnahme von automationsunterstützt verarbeiteten Dokumenten, umgangen werden.

Strafbestimmungen
Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 63. Wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs. 1 gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.

Verwaltungsstrafbestimmung

§ 62. (1) Sofern die Tat nicht einen Tatbestand nach Art. 83 DSGVO verwirklicht oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 50 000 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenverarbeitung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält,

2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 6) übermittelt, insbesondere Daten, die ihm gemäß §§ 7 oder 8 anvertraut wurden, vorsätzlich für andere unzulässige Zwecke verarbeitet,

3. sich unter Vortäuschung falscher Tatsachen vorsätzlich personenbezogene Daten gemäß § 10 verschafft,

4. eine Bildverarbeitung entgegen den Bestimmungen des 3. Abschnittes des 1. Hauptstücks betreibt oder

5. die Einschau gemäß § 22 Abs. 2 verweigert.

(2) Der Versuch ist strafbar.

[…]

3. Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) des Europäischen Parlaments und des Rates

Artikel 6

Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur

Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in

Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personen-bezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser

Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen,

indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine

rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß

Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in

Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht

oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten

erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der

Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche — um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben

wurden, vereinbar ist — unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des

Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß

Artikel 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten

gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Artikel 12

Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde. […]

(3) Der Verantwortliche stellt der betroffenen Person Informationen über die auf Antrag gemäß den Artikeln 15 bis 22 ergriffenen Maßnahmen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Der Verantwortliche unterrichtet die betroffene Person innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Stellt die betroffene Person den Antrag elektronisch, so ist sie nach Möglichkeit auf elektronischem Weg zu unterrichten, sofern sie nichts anderes angibt.

(4) Wird der Verantwortliche auf den Antrag der betroffenen Person hin nicht tätig, so unterrichtet er die betroffene Person ohne Verzögerung, spätestens aber innerhalb eines Monats nach Eingang des Antrags über die Gründe hierfür und über die Möglichkeit, bei einer Aufsichtsbehörde Beschwerde einzulegen oder einen gerichtlichen Rechtsbehelf einzulegen. […]

Artikel 15

Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 1b darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Artikel 29

Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:
a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;

f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und

k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;

c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.
(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.
(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.
(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.
(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

3. Bestimmungen des Wiener Datenschutzgesetzes - Wr. DSG, LGBl. für Wien Nr. 125/2001

Anwendung von Bestimmungen des Datenschutzgesetzes 2000

§ 4. (1) Hinsichtlich der Verwendung von Daten und der Datensicherheit sind die Bestimmungen des Artikels 2, 2. und 3. Abschnitt des Datenschutzgesetzes 2000 sinngemäß anzuwenden. In den §§ 6, 12 und 13 tritt jedoch an die Stelle des Bundeskanzlers die Landesregierung.

(2) Hinsichtlich der besonderen Verwendungszwecke sind die Bestimmungen des Artikels 2, 8. Abschnitt des Datenschutzgesetzes 2000 mit Ausnahme des § 45 sinngemäß anzuwenden.

(3) Hinsichtlich der Publizität der Datenanwendungen sind die Bestimmungen des Artikels 2, 4. Abschnitt des Datenschutzgesetzes 2000 sinngemäß anzuwenden. Nicht automationsunterstützt geführte Dateien gelten als Datenanwendungen im Sinne des § 4 Z 7 des Datenschutzgesetzes 2000. § 17 des Datenschutzgesetzes 2000 ist mit der Maßgabe anzuwenden, dass die Meldepflicht nur für solche Dateien besteht, deren Inhalt gemäß § 18 Abs. 2 des Datenschutzgesetzes 2000 der Vorabkontrolle unterliegt.

(4) Hinsichtlich der Rechte des Betroffenen sind die Bestimmungen des Artikels 2, 5. Abschnitt des Datenschutzgesetzes 2000 sinngemäß anzuwenden.

(5) Hinsichtlich des Rechtsschutzes sind die Bestimmungen des Artikels 2, 6. Abschnitt des Datenschutzgesetzes 2000 sinngemäß anzuwenden.

Strafbestimmungen

§ 5 (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 18 200 Euro zu ahnden ist, wer

a) sich vorsätzlich widerrechtlichen Zugang zu einer Datei verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder

b) Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 4 Abs. 1 dieses Gesetzes in Verbindung mit § 15 des Datenschutzgesetzes 2000) übermittelt, insbesondere Daten, die ihm gemäß §§ 46 oder 47 des Datenschutzgesetzes 2000 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder

c) Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtig stellt oder nicht löscht oder

d) Daten vorsätzlich entgegen § 4 Abs. 4 dieses Gesetzes in Verbindung mit § 26 Abs. 7 des Datenschutzgesetzes 2000 löscht.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 9 100 Euro zu ahnden ist, wer

a) Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß § 4 Abs. 3 dieses Gesetzes in Verbindung mit § 17 des Datenschutzgesetzes 2000 erfüllt zu haben oder

b) Daten ins Ausland übermittelt oder überlässt, ohne die erforderliche Genehmigung der Landesregierung gemäß § 4 Abs. 1 dieses Gesetzes in Verbindung mit § 13 des Datenschutzgesetzes 2000 eingeholt zu haben oder

c) seine Offenlegungs- oder Informationspflichten gemäß § 4 Abs. 3 dieses Gesetzes in Verbindung mit den §§ 23, 24 oder 25 des Datenschutzgesetzes 2000 verletzt oder

d) die gemäß § 4 Abs. 1 dieses Gesetzes in Verbindung mit § 14 des Datenschutzgesetzes 2000 erforderlichen

e) Sicherheitsmaßnahmen gröblich außer Acht lässt.

(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern kann ausgesprochen werden (§§ 10, 17 und 18 Verwaltungsstrafgesetz 1991 – VStG, BGBl. Nr. 52), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen.

[...]

4. Bestimmungen des Urheberrechtsgesetzes, BGBl. Nr. 111/1936 idgF

Anspruch auf angemessenes Entgelt.

§ 86. (1) Wer unbefugt

1. ein Werk der Literatur oder Kunst auf eine nach den §§ 14 bis 18a dem Urheber vorbehaltene Verwertungsart benutzt,
2. eine Darbietung auf eine nach dem § 68 dem ausübenden Künstler vorbehaltene Verwertungsart benutzt,
3. eine Darbietung auf eine nach dem § 72 dem Veranstalter vorbehaltene Verwertungsart benutzt,
4. ein Lichtbild oder einen Schallträger auf eine nach den §§ 74 oder 76 dem Hersteller vorbehaltene Verwertungsart benutzt,
5. eine Rundfunksendung auf eine nach § 76a dem Rundfunkunternehmer vorbehaltene Verwertungsart benutzt oder
6. eine Datenbank auf eine nach § 76d dem Hersteller vorbehaltene Verwertungsart benutzt,

hat, auch wenn ihn kein Verschulden trifft, dem Verletzten, dessen Einwilligung einzuholen gewesen wäre, ein angemessenes Entgelt zu zahlen.

[…]

Schutz von Computerprogrammen

§ 90b. Der Inhaber eines auf dieses Gesetz gegründeten Ausschließungsrechts an einem Computerprogramm, der sich technischer Mechanismen zum Schutz dieses Programms bedient, kann auf Unterlassung und Beseitigung des dem Gesetz widerstreitenden Zustands klagen, wenn Mittel in Verkehr gebracht oder zu Erwerbszwecken besessen werden, die allein dazu bestimmt sind, die unerlaubte Beseitigung oder Umgehung dieser technischen Mechanismen zu erleichtern. Die §§ 81, 82 Abs. 2 bis 6, §§ 85, 87 Abs. 1 und 2, § 87a Abs. 1, § 88 Abs. 2, §§ 89 und 90 gelten entsprechend.

Schutz technischer Maßnahmen

§ 90c. (1) Der Inhaber eines auf dieses Gesetz gegründeten Ausschließungsrechts, der sich wirksamer technischer Maßnahmen bedient, um eine Verletzung dieses Rechts zu verhindern oder einzuschränken, kann auf Unterlassung und Beseitigung des dem Gesetz widerstreitenden Zustandes klagen,

1. wenn diese Maßnahmen durch eine Person umgangen werden, der bekannt ist oder den Umständen nach bekannt sein muss, dass sie dieses Ziel verfolgt,
2. wenn Umgehungsmittel hergestellt, eingeführt, verbreitet, verkauft, vermietet und zu kommerziellen Zwecken besessen werden,
3. wenn für den Verkauf oder die Vermietung von Umgehungsmitteln geworben wird oder
4. wenn Umgehungsdienstleistungen erbracht werden.

[…]

Schutz von Kennzeichnungen

§ 90d. (1) Der Inhaber eines auf dieses Gesetz gegründeten Ausschließungsrechts, der Kennzeichnungen im Sinne dieser Bestimmung anwendet, kann auf Unterlassung und Beseitigung des dem Gesetz widerstreitenden Zustandes klagen,

1. wenn solche Kennzeichnungen entfernt oder geändert werden,
2. wenn Vervielfältigungsstücke von Werken oder sonstigen Schutzgegenständen, von beziehungsweise auf denen Kennzeichnungen unbefugt entfernt oder geändert worden sind, verbreitet oder zur Verbreitung eingeführt oder für eine Sendung, für eine öffentliche Wiedergabe oder für eine öffentliche Zurverfügungstellung verwendet werden.

[…]

Eingriff.

§ 91. (1) Wer einen Eingriff der im § 86 Abs. 1, § 90b, § 90c Abs. 1 oder § 90d Abs. 1 bezeichneten Art begeht, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen. Der Eingriff ist jedoch dann nicht strafbar, wenn es sich nur um eine unbefugte Vervielfältigung oder um ein unbefugtes Festhalten eines Vortrags oder einer Aufführung jeweils zum eigenen Gebrauch oder unentgeltlich auf Bestellung zum eigenen Gebrauch eines anderen handelt.

(1a) (Anm.: aufgehoben durch BGBl. I Nr. 32/2003)

(2) Ebenso ist zu bestrafen, wer als Inhaber oder Leiter eines Unternehmens einen im Betrieb des Unternehmens von einem Bediensteten oder Beauftragten begangenen Eingriff dieser Art (Abs. 1 und 1a) nicht verhindert.

(2a) Wer eine nach den Abs. 1, 1a oder 2 strafbare Handlung gewerbsmäßig begeht, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(3) Der Täter ist nur auf Verlangen des in seinem Recht Verletzten zu verfolgen.

(4) § 85 Abs. 1, 3 und 4 über die Urteilsveröffentlichung gilt entsprechend.

(5) Das Strafverfahren obliegt dem Einzelrichter des Gerichtshofes erster Instanz.

5. Information zur Verarbeitung personenbezogener Daten im Rahmen einer Anmeldung / einer Teilnahme an einer Bildungsveranstaltung am Campus Alsergrund

Die Unternehmung Wiener Gesundheitsverbund der Stadt Wien verarbeitet personenbezogene Daten im Zusammenhang mit einer Anmeldung / einer Teilnahme an einer Bildungsveranstaltung am Campus Alsergrund und ist Verantwortlicher im Sinne des Art. 4 Z. 7 Datenschutz-Grundverordnung (DSGVO) .

Die personenbezogenen Daten werden im Rahmen einer Anmeldung / einer Teilnahme an einer Bildungsveranstaltung verarbeitet. Die Verarbeitung erfolgt auf Basis des Bundesgesetzes über die Regelung der gehobenen medizinisch-technischen Dienste (MTD-Gesetz), des Bundesgesetzes über den Hebammenberuf (Hebammengesetz – HebG), des Bundesgesetzes über die Ausübung des ärztlichen Berufes und die Standesvertretung der Ärzt*innen (ÄrzteG), des Bundesgesetzes über medizinische Assistenzberufe und die Ausübung der Trainingstherapie (MABG) und deren jeweilige mitgeltenden Verordnungen sowie dem allgemeinen Sozialversicherungsgesetz (ASVG).

Zweck der Verarbeitung ist, Planung und Abwicklung von berufs- und betriebsrelevanten Bildungsprozessen zu ermöglichen sowie theoretisches Wissen und praktische Erfahrung auf fortgeschrittenem Niveau zu vernetzen, um die professionelle Handlungskompetenz zu fördern.

Bei der genannten Verarbeitung werden folgende personenbezogenen Daten am Campus Alsergrund in der BASIS-FSA Schuladministrationsprogramm des Unternehmung Wiener Gesundheitsverbund verarbeitet:

Name (Vorname, Nachname, Geburtsname), Titel, Geburtsdatum, Geschlecht, Geburtsort, Privatanschrift, E-Mail-Adresse, Sozialversicherungsnummer, Staatsangehörigkeit, Familienstand, Ausbildung, Berufstätigkeit, Name und Anschrift der Dienststelle/ des Dienstgebers, Rechnungsadresse und Telefonnummer bei Anmeldung von Personen, die nicht bei der Stadt Wien beschäftigt sind, Daten betreffend der Bildungsveranstaltung [Kursbezeichnung, Anmeldedatum, Kursbeginn und Kursende, Status-Ergebnis (teilgenommen, von Dienstgeber zurückgezogen bzw. vom Veranstalter storniert)].

Soweit dies gesetzlich vorgeschrieben bzw. zum Zweck der Verrechnung erforderlich ist, übermittelt der Wiener Gesundheitsverbund Daten an folgende externe Empfänger: Magistratsabteilung 15, Magistratsabteilung 40, Magistratsabteilung 2, Magistratsabteilung 6, Kontrollamt der Stadt Wien, Stadtrechnungshof.

Eine Übermittlung an Drittländer findet nicht statt.

Die Löschung der Daten erfolgt jahrgangsmäßig 45 Jahre nach Ersterfassung.
Den langen Löschfristen liegt der Normzweck zu Grunde, den Absolvent*innen im Falle des Verlustes eines Qualifikationsnachweises die Erlangung eines Duplikates zu ermöglichen, zum anderen ist der Normzweck der Aufbewahrungsregelungen mit dem öffentlichen Interesse im Bereich der öffentlichen Gesundheit, insbesondere zur Gewährleistung hoher Qualitätsstandards in den Berufsausbildungen und somit des Patient*innenen-Schutzes zu begründen .

Es besteht das Recht auf Auskunft, welche personenbezogenen Daten verarbeitet werden, sowie das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten.

Es besteht das Recht auf Auskunft, welche personenbezogenen Daten verarbeitet werden, sowie das Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten.

Wenn für die Übermittlung von Daten eine Einwilligung erteilt wurde und dies nicht zur Erfüllung des Ausbildungszwecks bzw. zur Vertragserfüllung oder Erfüllung von gesetzlichen Bestimmungen notwendig ist, besteht ein Widerspruchsrecht gegen die Verarbeitung, ohne dass davon die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird.

Die Bereitstellung der personenbezogenen Daten ist gesetzlich vorgeschrieben. Eine Nicht-Bereitstellung hätte die Konsequenz, dass eine Teilnahme an einer Bildungsveranstaltung nicht zustande kommt, da der Wiener Gesundheitsverbund in diesem Fall seinen vorgeschriebenen gesetzlichen Verpflichtungen (MTD-Gesetz, HebG, ÄrzteG, MABG, ASVG) nicht entsprechen kann.

Beschwerden können an die österreichische Datenschutzbehörde gerichtet werden. https://www.dsb.gv.at/

Wenn Sie eines der oben beschriebenen Rechte wahrnehmen möchten, haben Sie die Möglichkeit, sich an folgende Stellen zu wenden:

an den Wiener Gesundheitsverbund, Thomas-Klestil-Platz 7 /1, 1030 Wien – E-Mail: PostDatenschutz@gesundheitsverbund.at oder an die Magistratsabteilung 63 (Gewerberecht, Datenschutz und Personenstand), Wipplingerstr. 6 – 8, 1010 Wien –E-Mail: post@ma63.wien.gv.at

Kontakt:
Wiener Gesundheitsverbund
Campus Alsergrund
1090 Wien, Spitalgasse 23
E-Mail: post_akh_sfzm@akhwien.at
Homepage: https://campus-alsergrund.gesundheitsverbund.at/

Datenschutzbeauftragter der Stadt Wien
E-Mail: datenschutzbeauftragter@wien.gv.at

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 4.5.2016
[2] Erlass betreffend Aufbewahrung von Ausbildungsunterlagen im Lichte der Datenschutzgrundverordnung; Entfall der DVR-Nummer; gesundheitsberufliche Ausbildungen GZ:BMASGK-92250/0031-IX/A/2/2018 vom 24.5.2018