Datenschutz-, Datensicherheits- und Verschwiegenheitserklärung
für externe Benutzerinnen und Benutzer
mit Zugriffsrechten auf IT-Systeme des Landes Tirol

Name: …… Geburtsdatum: ……
Begründung der Notwendigkeit des Zugangs zum Tiroler Landesnetz: ……..……
…….....

Die folgende Aufklärung bzw. Belehrung soll externe BenutzerInnen des Tiroler Landesnetzes über die rechtlichen Vorgaben sowie technischen und organisatorischen Sicherheitsmaßnahmen des Landes Tirol informieren und sie bei der Einhaltung dieser unterstützen.

I. Datenschutzrechtliche Aspekte

Für die **Verarbeitung[1] personenbezogener[2] Daten** enthält das Datenschutzrecht besondere Bestimmungen. Datenschutzrechtliche Vorschriften sind Verbotsnormen. Das heißt, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten ist, außer es besteht eine taugliche rechtliche Grundlage nach Art. 6 bzw. 9 der Datenschutz-Grundverordnung der EU.

I.I. Datengeheimnis nach § 6 DSG

1. Das Datengeheimnis gilt sowohl für elektronische Daten, als auch für solche in Papierform.
2. Ich nehme zur Kenntnis, dass ich nach § 6 Abs. 1 des Datenschutzgesetzes i.d.g.F. verpflichtet bin, das Datengeheimnis zu wahren. Ich habe personenbezogene Daten aus Datenverarbeitungen, die mir ausschließlich aufgrund meiner berufsmäßigen Beschäftigung anvertraut oder zugänglich wurden, geheim zu halten (z.B. auch gegenüber Familienangehörigen oder Bekannten sowie unzuständigen KollegInnen, Firmen, Behörden und sonstigen öffentlichen oder privaten Stellen).
3. Darüber hinaus können noch andere bzw. weitergehende gesetzliche Verschwiegenheitspflichten bestehen, die zusätzlich noch einzuhalten sind (z.B. Amtsverschwiegenheit oder Ärztegeheimnis).
4. Die Daten sind nicht geheim zu halten, wenn ein gesetzlicher oder sonstiger rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen personenbezogenen Daten existiert.

---

[1] ***Verarbeitung*** ist etwa das Erheben, das Erfassen, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Lesen, das Abfragen, die Übermittlung, die Verbreitung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

[2] ***Personenbezogen*** sind alle Daten, die geeignet sind, eine bestimmte Person zu identifizieren. Dazu gehören etwa der Name, das Geburtsdatum, die Adresse, die Bankverbindung, Gesundheitsdaten, strafrechtliche Daten, die Sozialversicherungsnummer, Bilder und vieles mehr.

5. Es ist mir untersagt, personenbezogene Daten zu einem anderen als zum rechtmäßigen Zweck zu verarbeiten.
6. Ich verpflichte mich nach § 6 Abs. 2 DSG, personenbezogene Daten aus Datenverarbeitungen nur aufgrund einer ausdrücklichen Anordnung des für die Verarbeitung Verantwortlichen zu übermitteln, außer es besteht dazu eine gesetzliche Verpflichtung.
7. Ich habe das Datengeheimnis auch nach Beendigung des Dienstverhältnisses/ Arbeitsverhältnisses/Arbeitsauftrages einzuhalten.
8. Ich wurde über die für mich geltenden Übermittlungsanordnungen belehrt.
9. Ich weiß, dass Verletzungen des Datengeheimnisses zu strafrechtlicher Verfolgung, arbeits- und dienstrechtlichen Konsequenzen bzw. Schadenersatzpflichten führen können (§ 6 Abs. 3 DSG). Eine Übersicht über die wichtigsten datenschutz- und strafrechtlich relevanten Bestimmungen ist unten in der Anlage angeführt.
10. Ich weiß, dass mir – unbeschadet des verfassungsrechtlichen Weisungsrechts – aus der Verweigerung der Befolgung einer Anordnung zur unzulässigen Datenübermittlung kein Nachteil erwachsen darf (§ 6 Abs. 4 DSG).

I.II. Informationen zur Verarbeitung personenbezogener Daten nach Art. 13 bzw. 14 DSGVO

In der Wissensdatenbank des Landes Tirol (WIKI) im Portal Tirol im Bereich „DSGVO – Durchführung der Datenschutzgrundverordnung“ stehen nähere Informationen zur Verarbeitung personenbezogener Daten von Mitarbeiterinnen und Mitarbeitern zur Verfügung. Diese treffen im Umfang der Nutzung der IT-Infrastruktur des Landes Tirol auch auf mich zu.

II. Sonstige Geheimhaltungspflichten

1. Ich verpflichte mich, auch alle sonstigen Daten und Informationen, die keinen Personenbezug aufweisen, geheim zu halten, vertraulich zu behandeln und nicht an Dritte weiterzugeben bzw. Dritten zugänglich zu machen, soweit sie aus Datenverarbeitungen stammen, die mir ausschließlich aufgrund meiner berufsmäßigen Beschäftigung anvertraut oder zugänglich wurden bzw. mir im Zuge der Nutzung der IT-Systeme des Landes bekannt werden.
2. Zu diesen sonstigen Daten und Informationen zählen insbesondere Betriebs- und Geschäftsgeheimnisse, Persönlichkeitsrechte, Rechte nach dem Urheberrechtsgesetz bzw. nach dem Recht gegen unlauteren Wettbewerb, aber auch sonstige Daten, welche mir im Zuge der Nutzung der IT-Systeme des Landes bekannt werden.
3. Ich darf alle Daten und Informationen – unabhängig davon, ob diese einen Personenbezug aufweisen oder nicht – ausschließlich für den rechtmäßigen Zweck aufgrund meiner berufsmäßigen Beschäftigung verarbeiten. Darunter fallen unter anderem die Erhebung von Daten, jegliche weitere Verarbeitung, die Weitergabe an Dritte, die Veröffentlichung oder aber auch die Löschung.
4. Eine Geheimhaltungsverpflichtung besteht dann nicht, wenn Informationen bereits allgemein bekannt sind. Im Zweifel habe ich mich diesbezüglich mit der Leitung der für mich zuständigen Organisationseinheit des Landes Tirol abzustimmen.
5. Wenn ich in Angelegenheiten, die mit dieser Vertraulichkeitserklärung zusammenhängen, Dritte (etwa MitarbeiterInnen) einbinde, verpflichte ich mich, sämtliche Pflichten aus dieser Erklärung auch auf diese zu überbinden, sofern sie nicht selbst dieser Verpflichtung unterliegen.

6. Sonstige gesetzliche Verschwiegenheitspflichten bleiben unberührt.
7. Auch diese Geheimhaltungsverpflichtung ist nach Beendigung des Dienstverhältnisses/ Arbeitsverhältnisses/Arbeitsauftrages weiterhin einzuhalten.

III. Verpflichtungen betreffend Datensicherheit

Die allgemeinen Vorgaben und Strukturen hinsichtlich der Landes-IT in der jeweils aktuellen Fassung sind einzuhalten, diese Erlässe und IT-Policies sowie weitere Informationen zur Sicherheit am Arbeitsplatz sind übersichtlich zusammengefasst im WIKI im Portal Tirol unter „Mein EDV-Arbeitsplatz“/“IT-Sicherheit“ (für TLR-Benutzer bzw. für TSN- und TGN-Benutzer) abrufbar.

Ich habe sicherzustellen, dass unbefugte Dritte keinen Zugriff auf Daten und Informationen erhalten. Dazu verpflichte ich mich, ausreichende technische und organisatorische Maßnahmen zum Schutz der verarbeiteten Daten und Informationen zu setzen. Folgende Maßnahmen sind jedenfalls zu beachten:

Unbefugter Zugang bzw. Zugriff

- Verbindungen sind zu trennen, sobald sie nicht mehr benötigt werden,
- Räume mit IT-Arbeitsplätzen sind beim Verlassen zu versperren. Dies ist während der Regelarbeitszeit dann nicht erforderlich, wenn aufgrund geeigneter Vorkehrungen davon auszugehen ist, dass nicht zur Organisationseinheit gehörige Personen den Raum nicht betreten können,
- Bildschirmsperren sind zur Absicherung des Zugriffes auf die IT-Infrastruktur zu verwenden,
- Bildschirme sind so aufzustellen, dass keine unbefugte Einsicht möglich ist,
- Datenträger sind vor Einsichtnahme zu schützen.

Passwort und Authentifizierung

Benutzerkonten werden nur für natürliche Personen und nach deren zweifelsfreier Identifizierung (zB mit Lichtbildausweis) eingerichtet.
Jede Weitergabe von Zugangsdaten ist verboten.

Ausdrucke bzw. deren Vernichtung

Kopien bzw. Ausdrucke sind nur in unbedingt notwendigem Ausmaß anzufertigen. Diese sind stets vor Einsichtnahme zu schützen und nicht mehr benötigte Ausdrucke sicher zu vernichten oder der sicheren Vernichtung zuzuführen. Nach Beendigung der Zusammenarbeit sind unabhängig davon alle Kopien bzw. Ausdrucke zurückzustellen oder sicher zu vernichten bzw. der sicheren Vernichtung zuzuführen.

Hard- und Software bzw. mobile Datenspeicher

Hard- und Software darf nur von speziell dazu ermächtigten Mitarbeitern des Landes Tirol installiert und konfiguriert werden.
Durch die Verwendung von mobilen Datenspeichern (z.B. USB-Stick) existieren eine Menge potentieller Gefährdungen (u.a. die Gefahr des Vertraulichkeits- oder Integritätsverlustes von Daten).
Folgende Maßnahmen sind daher einzuhalten:

- Die Verwendung von individuellen Datenspeichern (vertrauenswürdige Geräte) bedarf Regelungen. Sind solche Regelungen nicht vorhanden, dürfen grundsätzlich keine externen Datenspeicher verwendet werden.
- Ist die Herkunft bzw. Sicherheit eines USB-Datenträgers/Gerätes nicht bekannt, so handelt es sich um ein „nicht vertrauenswürdiges Gerät“ und die Verwendung ist keinesfalls gestattet, da sich Schadprogramme auf diesem Weg verbreiten können.

Soziale Medien

Werden soziale Medien im dienstlichen und/oder privaten Umfeld verwendet, so ist darauf zu achten, dass im Sinne des Datenschutzes keine dienstlichen Informationen weitergegeben werden.

Maßnahmen bei Sicherheitsverletzungen

Organisatorische bzw. technische Sicherheitsvorfälle und -probleme, wie etwa der Befall oder der Verdacht des Befalls durch Schadprogramme sowie der Verlust oder Diebstahl bereitgestellter Hardware sind unverzüglich der Landes-IT zu melden.

IV. Verstoß

Im Fall des Verstoßes gegen Verpflichtungen aus dieser Erklärung hafte ich nach den allgemein gültigen schadenersatzrechtlichen Regelungen des Allgemeinen Bürgerlichen Gesetzbuches (§§ 1293ff ABGB).

V. Schlussbestimmungen

Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der restlichen Bestimmungen nicht.
Für sämtliche Streitigkeiten aus diesem Auftrag wird die Zuständigkeit des sachlich in Betracht kommenden Gerichtes in Innsbruck vereinbart. Es gilt österreichisches Recht, internationale oder nicht österreichische Rechtsnormen werden ausdrücklich ausgeschlossen.

Mit meiner Unterschrift

- **bestätige ich, die „Datenschutz-, Datensicherheits- und Verschwiegenheitserklärung für externe Benutzerinnen und Benutzer mit Zugriffsrechten auf IT-Systeme des Landes Tirol“ zur Kenntnis genommen und eine Kopie ausgehändigt bekommen zu haben.**
- **verpflichte ich mich, die vorgenannten Verpflichtungen, insbesondere die Bestimmungen zum Datengeheimnis, zu den sonstigen Geheimhaltungspflichten sowie zur Gewährleistung der Datensicherheit einzuhalten.**

……. ……...

Innsbruck, am Unterschrift

ANLAGE

Datenschutz- und datensicherheitsrechtliche Grundlagen, Strafbestimmungen

Stand: DSGVO: VO (EU) 2016/67, DSG: BGBl. I Nr. 165/1999 idF BGBl. I Nr. 14/2019, StGB: BGBl. Nr. 60/1974 idF BGBl. I Nr. 111/2019

§ 1 DSG – Grundrecht auf Datenschutz

(1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;

2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

Artikel 4 DSGVO – Begriffsbestimmungen (Auszug)

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. ***„personenbezogene Daten“*** alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

2. ***„Verarbeitung“*** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. ***„Einschränkung der Verarbeitung“*** die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. ***„Profiling“*** jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. ***„Pseudonymisierung“*** die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

6. ***„Dateisystem“*** jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. ***„Verantwortlicher“*** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

8. ***„Auftragsverarbeiter“*** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

9. ***„Empfänger“*** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

10. ***„Dritter“*** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

Artikel 5 DSGVO – Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Artikel 25 DSGVO - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Artikel 32 DSGVO – Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

§ 6 DSG – Datengeheimnis

(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.

§ 62 DSG – Verwaltungsstrafbestimmung

(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) Gegen juristische Personen können bei Verwaltungsübertretung nach Abs. 1 und 2 Geldbußen nach Maßgabe des § 30 verhängt werden.

(4) Die Strafe des Verfalls von Datenträgern und Programmen sowie Bildübertragungs- und Bildaufzeichnungsgeräten kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 in Zusammenhang stehen.

(5) Die Datenschutzbehörde ist zuständig für Entscheidungen nach Abs. 1 bis 4.

§ 63 DSG – Datenverarbeitung in Gewinn- oder Schädigungsabsicht

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.

§ 121 StGB – Verletzung von Berufsgeheimnissen

(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.

§ 126a StGB – Datenbeschädigung

(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.

§ 126b StGB – Störung der Funktionsfähigkeit eines Computersystems

(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. die Tat gegen ein Computersystem verübt, das ein wesentlicher Bestandteil der kritischen Infrastruktur (§ 74 Abs. 1 Z 11) ist, oder

3. die Tat als Mitglied einer kriminellen Vereinigung begeht.

§ 126c StGB – Missbrauch von Computerprogrammen oder Zugangsdaten

(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.

§ 148a StGB – Betrügerischer Datenverarbeitungsmißbrauch

(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.