Benutzungsreglement Informatikmittel

Vom 16. Dezember 2014 (Stand 1. Juli 2022)

Der Regierungsrat des Kantons Basel-Landschaft,

gestützt auf § 74 Abs. 2 der Verfassung des Kantons Basel-Landschaft vom 17. Mai 1984[1)], das Gesetz über die Organisation des Regierungsrats und der Verwaltung des Kantons Basel-Landschaft vom 28. September 2017[2)] und das Gesetz über die Information und den Datenschutz vom 10. Februar 2011[3)], *

beschliesst:

1 Allgemeine Bestimmungen

§ 1 Geltungsbereich

[1] Dieses Reglement gilt für die Mitarbeitenden der kantonalen Verwaltung (exklusive Schulen), die Mitglieder des Regierungsrats, die Mitarbeitenden der Finanzkontrolle, der Aufsichtsstelle Datenschutz, der Ombudsperson sowie der Gerichte des Kantons Basel-Landschaft (nachfolgend «Mitarbeitende»). *

[2] Das Reglement ist von allen Mitarbeitenden, die Informatikmittel nutzen, zu unterschreiben. Die vorgesetzten Stellen regeln das Vorgehen zur Unterzeichnung.

[3] Änderungen des Reglements sind den Mitarbeitenden in geeigneter Weise zu kommunizieren, haben für diese jedoch auch ohne schriftliche Bestätigung Gültigkeit, sofern nicht ein anderer Erlass dies erfordert.

§ 2 Zweck

[1] Das Reglement ordnet die sichere und rechtmässige Benutzung von Informatikmitteln.

[2] Es hat zum Zweck, die elektronischen Informationen bezüglich Vertraulichkeit, Verfügbarkeit und Integrität zu schützen, den wirtschaftlichen Einsatz der Informatikmittel zu gewährleisten sowie die Persönlichkeitsrechte der Mitarbeitenden zu wahren.

1) SGS 100
2) SGS 140
3) SGS 162

*** Änderungstabellen am Schluss des Erlasses**

§ 3 Verantwortung

[1] Die Mitarbeitenden sind für die Verwendung der durch sie genutzten Informatikmittel im Rahmen der geltenden Rechtsordnung und dieses Reglements persönlich verantwortlich.

[2] Die Vorgesetzten und die Projektleitenden sind verantwortlich für die Kommunikation und Durchsetzung des Reglements.

§ 4 Datenschutz und Informationssicherheit

[1] Beim Einsatz der Informatikmittel gelten insbesondere das Gesetz vom 10. Februar 2011[4)] über die Information und den Datenschutz, die Verordnung vom 4. Dezember 2012[5)] zum Gesetz über die Information und den Datenschutz sowie die Verordnung vom 11. März 2008[6)] über die Informationssicherheit und darauf basierende Regelungen.

§ 5 Begriffe

[1] Im Sinne dieses Reglements gelten als:

a. * «Informatikmittel»: alle Geräte, Programme, Einrichtungen und Dienste, welche die Verarbeitung, Speicherung, Interpretation, Wiedergabe und den Transport von Daten ermöglichen;

b. «Hardware»: sämtliche technischen Geräte, welche die Bearbeitung, die Speicherung oder die Übermittlung von Daten ermöglichen (z. B. Computer, Notebooks, Memory Sticks, Mobiltelefone, Smartphones und Tablets);

c. «Software»: alle auf der Hardware zur Verfügung gestellten Betriebssysteme und Programme;

d. «Daten»: vom Kanton zur Erfüllung seiner Aufgaben bearbeitete oder dabei anfallende Informationen, unabhängig vom Datenträger (z. B. Festplatten, Memory Sticks, Notebooks);

e. «Cloud»: virtuelle Infrastruktur oder Dienstleistungen, die über ein Netzwerk angeboten werden (z.B. Datenspeicher, Rechenkapazität, Anwendungen);

f. «Social Media»: digitale Medien und Technologien, die einen Austausch von Kommunikation, Meinungen und medialen Inhalten einzeln oder in Gemeinschaft ermöglichen;

g. * «Fernzugriff»: der Zugang zu den Netzwerken der kantonalen Verwaltung oder an diese angeschlossenen Systeme von ausserhalb der Räumlichkeiten der kantonalen Verwaltung (z. B. Telearbeitsplatz/Homeoffice, mobiles Arbeiten, Drittgerät/Privatgerät);

4) GS 37.1165, SGS 162
5) GS 37.1185, SGS 162.11
6) GS 36.0543, SGS 162.51

h. * «Mobilgerät»: Informatikmittel im mobilen Einsatz, die unterschieden werden in:

1. Smartphones und Tablets (geschäftlich wie privat), welche von Mitarbeitenden geschäftlich genutzt werden; diese Geräte sind nicht in der BL-Domäne definiert;
2. BL-Standardgeräte, welche in der BL-Domäne definiert sind und mobil genutzt werden können (z. B. Convertibles);

i * «VDI» (Virtual Desktop Infrastructure): Technologie, die es erlaubt den Benutzer-Arbeitsplatz zentral auf einem Server zu betreiben; auf den Arbeitsplatz wird mittels einer speziellen Anwendung zugegriffen, die auf fast allen Endgeräten installiert und genutzt werden kann.

2 Nutzung der Informatikmittel

§ 6 Sorgfältiger Gebrauch

[1] Die Mitarbeitenden haben die durch sie genutzten Informatikmittel sorgfältig und ressourcenschonend einzusetzen. Insbesondere sind sie dafür verantwortlich, dass die Nutzung keine Schäden an den Informatikmitteln selber, den damit verbundenen Systemen und Netzwerken oder an den darauf gespeicherten Daten zur Folge hat.

[2] Die vom Kanton getroffenen Sicherheitsvorkehrungen dürfen nicht manipuliert oder entfernt werden.

[3] Wenn eine Mitarbeitende bzw. ein Mitarbeitender ein Informatikmittel nicht unmittelbar in Gebrauch hat, ist der Zugang hierzu so zu sperren, dass dieser nur mit der persönlichen Zugangskennung entsperrt werden kann.

[4] Die Mitarbeitenden stellen sicher, dass bei der Nutzung von Informatikmitteln und beim Ausdrucken von Dokumenten besondere Personendaten und andere Informationen mit schützenswertem Inhalt nicht von Unberechtigten eingesehen oder behändigt werden können. *

[5] Das Ausdrucken von geschäftlichen Dokumenten und Daten mit nicht öffentlichem Inhalt ist ausserhalb des betrieblichen Umfelds/Telearbeit untersagt. Im betrieblichen Umfeld ist sicherzustellen, dass nicht öffentliche Daten nicht von unberechtigten Personen eingesehen werden können. *

[6] Nach Beendigung der Arbeit muss der Computer ganz heruntergefahren werden. Damit wird sichergestellt, dass technische und Sicherheits-Updates eingespielt und aktiviert werden. *

§ 7 Umgang mit Benutzerkennung und Passwörtern

[1] Die Mitarbeitenden sind für den sachgerechten Gebrauch der vorhandenen Zugangskontrolleinrichtungen und -massnahmen (z. B. Passwortwahl und –verwahrung, Zertifikate, SmartCard) verantwortlich.

[2] Passwörter zu persönlichen Identifikationsmitteln wie z.B. Benutzerkennungen oder SmartCard sind vertraulich zu behandeln und dürfen nicht weitergegeben werden.

§ 8 Beschaffung, Installation und Rückgabe von Informatikmitteln

[1] Die Informatikmittel werden durch die zuständige Beschaffungsstelle nach den geltenden Richtlinien und Standards beschafft.

[1bis] Sämtliche zur Verfügung gestellten Informatikmittel verbleiben im Eigentum des Kantons. *

[1ter] Für Telearbeit wird kein Vor-Ort-Support geleistet. Es stehen die üblichen Werkzeuge und Prozesse zur Meldung von Störungen und Defekten zur Verfügung. *

[2] Die Installation von Software auf vom Kanton zur Verfügung gestellter Hardware (inklusive VDI) sowie die Installation und Verwendung von nicht vom Kanton zur Verfügung gestellter Hardware am betrieblichen Arbeitsort ist grundsätzlich untersagt. Ausnahmen bedürfen eines Beschlusses der Fachgruppe Informatik, des ITO-Rats oder des Regierungsrats *

[3] Mitarbeitende sind verpflichtet, bei einem Stellenwechsel oder bei einem Wegfall der Gründe, die zur Abgabe von Informatikmitteln geführt haben, diese unaufgefordert zurückzugeben.

[4] Vor dem Austritt leiten die Mitarbeitenden die geschäftsrelevanten Daten aus ihrer persönlichen (nicht privaten) Ablage an die durch die vorgesetzte Person bezeichnete Stelle weiter. Nach dem Austritt werden Benutzerkonten und E-Mail-Account (wie alle anderen persönlichen und privaten Datenablagen) deaktiviert und anschliessend gelöscht. Die privaten E-Mails und Daten können die Mitarbeitenden mitnehmen.

§ 9 Fernzugriff

[1] Aus betrieblichen oder geschäftlichen Gründen kann die vorgesetzte Person auf Antrag hin eine Bewilligung für den Fernzugriff erteilen. Die Bewilligung von Telearbeit erfolgt gemäss Richtlinie des Personalamts betreffend Telearbeit *

[2] Wird Fernzugriff über ein Drittgerät bewilligt, ist die bzw. der Mitarbeitende für einen funktionierenden und aktuellen Malwareschutz auf diesem Gerät verantwortlich.

[3] Für den Fernzugriff stellt die Zentrale Informatik sichere Zugänge zur Verfügung. *

[3bis] Mitarbeitende, die über ein mobiles Arbeitsplatzgerät (z. B. Convertible) verfügen oder mit einem privaten Endgerät, mit installierter VDI-Client-Software, müssen per Fernzugriff auf das Kantonsnetzwerk und die damit verbundenen Systeme zugreifen. Die Geräte stellen automatisch eine verschlüsselte Verbindung zum Kantonsnetzwerk, über die von der ZI zur Verfügung gestellten Zugänge, her. Diese Verbindung darf nicht angepasst oder in irgendeiner Form verändert werden. *

[3ter] Für die Telearbeit ist durch die Mitarbeitenden eine geeignete Internetverbindung zur Verfügung zu stellen. *

[4] Im Falle eines Fernzugriffs werden den Mitarbeitenden keine Installations- oder Betriebskosten vergütet (Strom, Telefon etc.).

§ 9a * Nutzung von Mobilgeräten

[1] Vertrauliche Telefonate dürfen nur ohne unbefugte Mithörer erfolgen. Intelligente Sprachassistenten (Alexa, Siri etc.) dürfen nicht in Hörweite sein.

[2] Es dürfen keine Bildschirmfotos (Screenshots) von geschäftlichen Daten gemacht werden, wenn diese auf Smartphones/Tablets nicht im geschützten Speicher (BL-Addon) oder auf den Datenablagen der Zentralen Informatikdienste (Convertibles) abgelegt werden.

[3] Benutzerinnen und Benutzer eines Mobilgeräts stellen sicher, dass von privaten Apps und Anwendungen nicht auf die geschäftlichen Kontaktdaten zugegriffen wird und diese nicht synchronisiert werden.

[4] Mobilgeräte dürfen nicht von Dritten genutzt werden; dazu zählen auch Familienangehörige.

§ 10 Nutzung von E-Mail

[1] Die automatische Weiterleitung aus einem persönlichen kantonalen E-Mail-Account an interne oder externe E-Mail-Adressen ist nicht erlaubt.

[2] Bei Abwesenheit wird in der automatischen Abwesenheitsmeldung des kantonalen E-Mail-Accounts eine alternative Ansprechstelle bezeichnet.

[3] Für geschäftliche Tätigkeiten darf ausschliesslich das kantonale E-Mail-Konto genutzt werden. *

[4] Der Versand von Mails mit geschäftlichen Informationen an den eigenen privaten E-Mail-Account (z. B. zur Weiterbearbeitung) ist nicht zulässig. *

§ 11 Versand vertraulicher E-Mails und Daten

[1] Vertrauliche E-Mails sind mit der Vertraulichkeitsoption «Vertraulich» zu markieren und zu versenden.

[2] Vertrauliche Daten, insbesondere Personendaten, dürfen nur verschlüsselt oder passwortgeschützt an E-Mail-Adressen ausserhalb der Verwaltung versendet werden. Es sind dafür die vom Kanton angebotenen Techniken zu verwenden.

§ 12 Versand privater E-Mails

[1] Private E-Mails sind mit der Vertraulichkeitsoption «Privat» zu kennzeichnen und unter den Voraussetzungen von § 17 ohne kantonale Signatur zu versenden.

[2] Die Ablage privater E-Mails hat im Verzeichnis «Privat» zu erfolgen.

[3] Die kantonale E-Mail-Adresse darf nicht für private Newsletter, Bestellungen, Wettbewerbe, soziale Netzwerke oder ähnliches verwendet werden.

§ 13 E-Mail-Versand an alle Mitarbeitenden

[1] Jeder Massenversand an alle Mitarbeitenden der kantonalen Verwaltung bedarf der Bewilligung der für den Inhalt verantwortlichen Generalsekretärin bzw. des Generalsekretärs, der Landschreiberin bzw. des Landschreibers, der Leitungen der Finanzkontrolle und der Aufsichtsstelle Datenschutz, der Ombudsperson oder der Gerichtsverwaltung. *

[2] Die Generalsekretären-Konferenz legt fest, wer die technische Berechtigung für einen solchen Versand erhält.

§ 14 Nutzung des Kalenders

[1] Private und vertrauliche Kalendertermine sind mit der Vertraulichkeitsoption «Privat» zu kennzeichnen.

[2] Vertrauliche Dokumente dürfen nur «Privat» markierten Kalenderterminen angehängt werden.

§ 15 Nutzung des Internets

[1] Alle an die Netzwerke der kantonalen Verwaltung angeschlossenen Geräte verwenden ausschliesslich den zentral angebotenen Internetzugang.

[2] Es besteht kein Rechtsanspruch auf Zugang zum Internet.

[3] Der Regierungsrat behält sich das Recht vor, Informationen/Publikationen mit ungeeignetem Inhalt (z.B. pornografisch, rassendiskriminierend, unethisch, unmoralisch) zu sperren oder zu filtern.

[4] Definitive Sperrungen aufgrund von sicherheitsrelevanten oder technischen Erfordernissen benötigen die Bewilligung der zuständigen IT-Gremien.

§ 16 Unangemessene Nutzung

[1] Die Nutzung der Informatikmittel muss unter Einhaltung der geltenden Rechtsordnung sowie unter Berücksichtigung der Interessen des Kantons erfolgen.

[2] Es ist insbesondere verboten, auf Daten mit widerrechtlichem, urheberrechtsverletzendem, rassistischem, beleidigendem, pornografischem oder herabwürdigendem Inhalt zuzugreifen oder solche zu verbreiten.

§ 17 Private Nutzung

[1] Die private Nutzung der Informatikmittel ist erlaubt, sofern die beanspruchten Ressourcen (Arbeitszeit, Netzwerkkapazität, Speicherplatz, Verbindungszeit und -volumen) vernachlässigbar sind.

[2] Die private Nutzung während der Arbeitszeit darf die Erfüllung zugewiesener Aufgaben nicht beeinträchtigen und ist auf das absolut Notwendige zu beschränken.

[3] … *

[4] Die Kosten für die private Nutzung im Ausland sind von den Mitarbeitenden zu übernehmen und gemäss Instruktionen der Finanz- und Kirchendirektion abzurechnen. *

§ 18 Datentransport, -ablage und -speicherung *

[1] Daten, die nicht öffentlich oder zur Veröffentlichung bestimmt sind, müssen auf den Datenablagen der Zentralen Informatik gespeichert werden. Insbesondere ist es untersagt, solche Daten auf privaten Datenträgern (Festplatte im PC oder extern, auf Mobilgeräten oder anderen Massenspeichern, USB etc.) oder im Internet zu speichern (z. B. auf einer Website, einer Social Media-Plattform oder mittels eines persönlich eröffneten oder von Dritten zur Verfügung gestellten Cloud-Accounts wie Dropbox, iCloud etc.). *

[2] Ausnahmen bedürfen der Bewilligung durch den ITO-Rat auf der Basis einer Risikoanalyse.

[3] Der Transport vertraulicher Daten, insbesondere Personendaten, auf Datenträgern darf nur verschlüsselt erfolgen. Diese Datenträger sind bei der zuständigen Beschaffungsstelle zu beziehen.

[4] Private Daten sind (unter den Voraussetzungen von § 17) in einem mit dem Namen «Privat» bezeichneten Ordner abzulegen.

§ 19 Datenzugriff bei unvorhersehbaren Abwesenheiten

[1] Kommt es zu einer unvorhersehbaren Abwesenheit einer bzw. eines Mitarbeitenden und muss in dieser Zeit auf dessen bzw. deren Geschäftsdaten zugegriffen werden, muss ein solcher Datenzugriff durch die Generalsekretärin bzw. den Generalsekretär, die Landschreiberin bzw. den Landschreiber, die Leitungen der Finanzkontrolle und der Aufsichtsstelle Datenschutz, die Ombudsperson oder die Gerichtsverwaltung im Einzelfall bewilligt werden. *

[2] Der Zugriff erfolgt durch die vorgesetzte Person sowie eine weitere Person nach dem 4-Augen-Prinzip.

[3] Der Vorgang wird protokolliert. Das Protokoll wird der abwesenden Person nach deren Rückkehr ausgehändigt.

[4] Falls möglich, ist die abwesende Person vorgängig über den Zugriff zu informieren.

3 Meldepflicht

§ 20 Technische Mängel und sicherheitsrelevante Vorkommnisse

[1] Feststellungen über technische Mängel und sicherheitsrelevante Vorkommnisse mit Bezug zu Informatikmitteln (z. B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verdacht auf Missbrauch der eigenen Benutzerkennung usw.) sind unverzüglich dem Service Desk zu melden. *

[2] Könnte die Information des Service Desk zu einem Interessenkonflikt führen oder ist dieser nicht erreichbar, ist die bzw. der Vorgesetzte zu informieren.

§ 21 Verlust

[1] Bei Verlust eines Geräts ist zwingend der Helpdesk zu informieren und bei der zuständigen Polizeibehörde eine Diebstahl- oder Verlustanzeige zu erstatten. *

[2] Die SIM-Card ist durch die Mitarbeitende bzw. den Mitarbeitenden umgehend vom Mobildienstanbieter sperren zu lassen. *

[3] Eine allfällige Schadensbeteiligung des bzw. der Mitarbeitenden richtet sich nach dem Gesetz vom 24. April 2008[7)] über die Haftung des Kantons und der Gemeinden.

7) GS 36.0732, SGS 105

4 Kontroll- und Überwachungsmassnahmen

§ 22 Protokollierung

[1] Protokolldaten dienen ausschliesslich der Datensicherheit und zur Sicherstellung eines ordnungsgemässen Betriebes, zu Zwecken der Datenschutzkontrolle und der IT-Revision. Sie werden nicht für eine präventive Verhaltens- oder Leistungsbewertung verwendet.

[2] Die Protokollierung berücksichtigt die kantonalen Erlasse zu Datenschutz und Informationssicherheit und weitere Bestimmungen zur Aufbewahrung von Dokumenten.

§ 23 Kontrollen

[1] Die von der Generalsekretärin bzw. dem Generalsekretär, der Landschreiberin bzw. dem Landschreiber, der Leitungen der Finanzkontrolle und der Aufsichtsstelle Datenschutz, der Ombudsperson und der Gerichtsverwaltung bezeichneten Stellen prüfen periodisch eine summarische, anonyme Auswertung (ohne Rückschluss auf bestimmte Personen) der Benutzung der Systeme, der Anwendungen, der Netzwerke, des E-Mail-Verkehrs, des Fernzugriffs und des Internetzugangs sowie die auf den Servern abgelegten Datenbestände. *

[2] Ergibt sich aus der Überprüfung ein Verdacht auf Verstoss gegen dieses Reglement, so bleiben angemessene personenbezogene Prüfungen vorbehalten.

[3] Eine präventive personenbezogene Kontrolle ist nicht erlaubt.

[4] Grundsätzlich werden die Mitarbeitenden im Voraus darüber informiert, wenn eine personenbezogene Prüfung vorgenommen wird. Auf die Vorankündigung kann verzichtet werden, wenn

a. die Datensicherheit, insbesondere die Verfügbarkeit des Systems, nicht mehr garantiert werden kann, oder
b. Anhaltspunkte für ein rechtswidriges, insbesondere strafbares Handeln vorliegen.

[5] Wird aufgrund der personenbezogenen Prüfung ein Missbrauch festgestellt, wird die zuständige Dienststelle bzw. die Strafverfolgungsbehörde informiert.

[6] Die vorgesetzte Person darf die geschäftlichen Daten überprüfen, soweit dies für ihre Aufsichtstätigkeit notwendig ist. Besondere Geheimhaltungsbestimmungen sowie die Bestimmungen über das Amtsgeheimnis bleiben vorbehalten.

5 Schlussbestimmungen

§ 24 Aufhebung bisherigen Rechts

[1] Das Benutzungsreglement Informatik-Mittel vom 17. Dezember 2002[8)] wird aufgehoben.

§ 25 In-Kraft-Treten

[1] Dieses Reglement tritt am 1. Januar 2015 in Kraft.

8) GS 34.0771, SGS 140.551

Änderungstabelle - Nach Beschlussdatum

Beschlussdatum	Inkraft seit	Element	Wirkung	Publiziert mit
16.12.2014	01.01.2015	Erlass	Erstfassung	GS 2014.123
06.06.2017	01.07.2017	§ 5 Abs. 1, Bst. a.	geändert	GS 2017.031
06.06.2017	01.07.2017	§ 17 Abs. 3	aufgehoben	GS 2017.031
06.06.2017	01.07.2017	§ 17 Abs. 4	geändert	GS 2017.031
28.06.2022	01.07.2022	Ingress	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 1 Abs. 1	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 5 Abs. 1, Bst. g.	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 5 Abs. 1, Bst. h.	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 5 Abs. 1, Bst. i	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 6 Abs. 4	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 6 Abs. 5	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 6 Abs. 6	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 8 Abs. 1bis	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 8 Abs. 1ter	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 8 Abs. 2	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 9 Abs. 1	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 9 Abs. 3	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 9 Abs. 3bis	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 9 Abs. 3ter	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 9a	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 10 Abs. 3	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 10 Abs. 4	eingefügt	GS 2022.068
28.06.2022	01.07.2022	§ 13 Abs. 1	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 18	Titel geändert	GS 2022.068
28.06.2022	01.07.2022	§ 18 Abs. 1	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 19 Abs. 1	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 20 Abs. 1	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 21 Abs. 1	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 21 Abs. 2	geändert	GS 2022.068
28.06.2022	01.07.2022	§ 23 Abs. 1	geändert	GS 2022.068

Änderungstabelle - Nach Paragraf

Element	Beschlussdatum	Inkraft seit	Wirkung	Publiziert mit
Erlass	16.12.2014	01.01.2015	Erstfassung	GS 2014.123
Ingress	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 1 Abs. 1	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 5 Abs. 1, Bst. a.	06.06.2017	01.07.2017	geändert	GS 2017.031
§ 5 Abs. 1, Bst. g.	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 5 Abs. 1, Bst. h.	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 5 Abs. 1, Bst. i	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 6 Abs. 4	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 6 Abs. 5	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 6 Abs. 6	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 8 Abs. 1bis	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 8 Abs. 1ter	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 8 Abs. 2	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 9 Abs. 1	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 9 Abs. 3	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 9 Abs. 3bis	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 9 Abs. 3ter	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 9a	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 10 Abs. 3	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 10 Abs. 4	28.06.2022	01.07.2022	eingefügt	GS 2022.068
§ 13 Abs. 1	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 17 Abs. 3	06.06.2017	01.07.2017	aufgehoben	GS 2017.031
§ 17 Abs. 4	06.06.2017	01.07.2017	geändert	GS 2017.031
§ 18	28.06.2022	01.07.2022	Titel geändert	GS 2022.068
§ 18 Abs. 1	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 19 Abs. 1	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 20 Abs. 1	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 21 Abs. 1	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 21 Abs. 2	28.06.2022	01.07.2022	geändert	GS 2022.068
§ 23 Abs. 1	28.06.2022	01.07.2022	geändert	GS 2022.068