

Weisung zu Nutzung und Abgabe von Informatikmitteln

RRB Nr. 2018/1864 vom 27. November 2018

Der Regierungsrat des Kantons Solothurn

gestützt auf § 54 des Gesetzes über das Staatspersonal (StPG) vom 27. September 1992¹

beschliesst:

Allgemein

1. Zweck

Diese Weisung regelt die Nutzung und Abgabe von Informatikmitteln.

Sie hat zum Zweck, die rechtmässige, wirtschaftliche und sichere Bearbeitung von Daten der kantonalen Verwaltung mit Informatikmitteln zu gewährleisten und die Persönlichkeitsrechte der Mitarbeitenden zu wahren.

2. Geltungsbereich

Mit Ausnahme der Solothurner Spitäler AG, der Fachhochschule Nordwestschweiz, der kantonalen Anstalten und des pädagogischen Bereichs der kantonalen Schulen gilt die Weisung für alle Mitarbeitenden der kantonalen Verwaltung, im folgenden auch Benutzer genannt.

Für die Mitarbeitenden der Polizei Kanton Solothurn (Polizei) gilt die Weisung, soweit sie keine abweichenden Bestimmungen enthält.²

Die Weisung gilt für alle Informatikmittel gem. Ziff. 3, Bst. a).

3. Begriffe

Im Sinne dieser Weisung gelten als:³

- a) Informatikmittel: Sämtliche vom Kanton zur Verfügung gestellte elektronische Infrastruktur der Informations- und Kommunikationstechnologie, welche zur Bearbeitung von Daten der kantonalen Verwaltung dient. Privat beschaffte Informatikmittel sind insofern betroffen, als damit Daten der kantonalen Verwaltung bearbeitet werden. Der Begriff «Bearbeiten» richtet sich nach dem Informations- und Datenschutzgesetz (InfoDG) vom 21. Februar 2001⁴.
- b) Daten: Sach- und Personendaten. Der Begriff «Personendaten» richtet sich nach dem InfoDG.
- c) Leistungserbringer: Zentrale Anlaufstelle für alle Informatikbelange ist das Amt für Informatik und Organisation (AIO) oder weitere von der kantonalen Verwaltung beauftragte Dienstleister. Der Technische Führungsdienst (TFD) ist Leistungserbringer für die Polizei.
- d) SmartCard: Chipkarte, welche dem Zugang und der Identifikation eines Benutzers in der Informatikumgebung dient.
- e) Amtslaufwerk: Im Amtslaufwerk (z.B. Laufwerk H) erfolgt die elektronische Ablage

¹ BGS 126.1

² Absatz eingefügt mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

³ Buchstaben c und h geändert sowie Buchstaben k bis n eingefügt mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

⁴ BGS 114.1

der geschäftlichen Dokumente.

- f) Benutzerlaufwerk: Das Benutzerlaufwerk (z.B. Laufwerk M) ist das persönliche Laufwerk jedes Mitarbeitenden. Auf das Benutzerlaufwerk hat nur der jeweilige Mitarbeitende Zugriff.
- g) GEVER-Software: Mit der GEVER-Software erfolgt die elektronische GESchäftsVERwaltung der kantonalen Verwaltung.
- h) Arbeitsplatzsysteme: Sämtliche IT-Komponenten am Arbeitsplatz der Benutzer (Desktop-PCs, Notebooks, Fat- und Thin Clients, Monitore, Smartphones, Druckersysteme und Telefonie-Services).
- i) Fernzugriff: Zugriff auf die Netzwerke und Systeme der kantonalen Verwaltung aus der Ferne, d.h. von ausserhalb der Räumlichkeiten der kantonalen Verwaltung.
- j) Protokolldaten: Automatisch aufgezeichnete Informationen der Aktivitäten auf einem Computersystem.
- k) Awareness: Bewusstsein der Benutzer für die Sicherheit im Umgang mit Informatikmitteln und Daten.
- l) Phishing-Mail: Betrügerischer Versuch, sich über gefälschte Websites, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner auszugeben um so an Login-Daten zu gelangen oder um eine Schadsoftware zu installieren.
- m) Schadsoftware: Mit schädigender Absicht entwickelte Computerprogramme, die versuchen, sich ohne Wissen der Benutzer Zugang zu deren Informatikmitteln und Daten zu beschaffen.
- n) Makro-/Sicherheitswarnung: Warnmeldung, dass beim Weiterfahren ein automatisiertes Hilfsprogramm ausgelöst oder eine andere Sicherheitsmassnahme übersteuert wird.

4. Verantwortung

Die Benutzer sind verantwortlich für die Nutzung der Informatikmittel nach dieser Weisung und im Rahmen der geltenden Rechtsordnung.

Es liegt in der Verantwortung der oder des Vorgesetzten einer Amtsstelle, den Benutzern diese Weisung und deren Änderungen in geeigneter Form bekannt zu machen.

Das AIO informiert über die Weisung und deren Änderungen im Intranet.

5. Datenschutz und Datensicherheit

Bei der Verwendung der Informatikmittel haben die Benutzer das Informations- und Datenschutzgesetz (InfoDG) vom 21. Februar 2001⁵ sowie die Informations- und Datenschutzverordnung (InfoDV) vom 10. Dezember 2001⁶ zu beachten.

Sie haben insbesondere sicherzustellen, dass Daten oder Dokumente nicht von Unberechtigten eingesehen, bzw. behündigt werden können.

Nutzung

6. Sorgfältige Nutzung

Die Benutzer haben die verwendeten Informatikmittel sorgfältig einzusetzen. Insbesondere sind sie dafür verantwortlich, im Rahmen ihrer Möglichkeiten Vorkehrungen zu treffen, damit die Nutzung keine Schäden an den Informatikmitteln selber, den damit verbundenen Systemen und Netzwerken oder an den darauf gespeicherten Daten zur Folge hat.

7. Umgang mit Benutzererkennung und Passwörtern

Die Benutzer sind für den Gebrauch der vorhandenen Zugangskontrolleinrichtungen

⁵ BGS 114.1

⁶ BGS 114.2

und -massnahmen (z. B. Passwortwahl und -verwahrung, Zertifikate, SmartCard) verantwortlich.

Passwörter zu persönlichen Identifikationsmitteln, wie z.B. Benutzerkennungen oder SmartCard, sind geheim zu halten und dürfen nicht weitergegeben werden.

Wenn ein Benutzer ein Informatikmittel nicht unmittelbar in Gebrauch hat, ist der Zugang hierzu so zu sperren, dass dieser nur mit der persönlichen Zugangskennung entsperrt werden kann.

8. Datenablage und -speicherung

Geschäftliche Daten werden nach Anweisung der Amtsleitungen bzw. den internen Organisationsvorschriften in der GEVER-Software, im Amtslaufwerk oder in einer Fachanwendung gespeichert. Davon ausgenommen sind geschäftliche Daten mit vertraulichem Inhalt, die im persönlichen Benutzerlaufwerk aufbewahrt werden können.

9. Limitierungen

Die den Benutzern zur Verfügung stehenden Ressourcen (z.B. Bandbreite Internet, Speicherkapazität) können durch den Leistungserbringer limitiert werden, um beschränkt vorhandene Ressourcen zu verteilen oder um Geschäftsprozesse optimal zu unterstützen.

Administrative Rechte auf den Arbeitsplatzsystemen werden nicht gewährt.

10. Rückgabe von Informatikmitteln

Die Benutzer sind verpflichtet, bei einem Stellenwechsel oder bei einem Wegfall der Gründe, die zur Abgabe von Informatikmitteln geführt haben, diese unaufgefordert zurückzugeben. Weitergehende Regelungen finden sich in den Richtlinien des AIO.

Nicht mehr benötigte oder defekte Datenträger (CD, DVD, USB-Stick, SD-Card, externe Harddisk, etc.) müssen beim zuständigen Leistungserbringer abgegeben werden.

11. Verlust und Diebstahl

Der Verlust oder Diebstahl eines Informatikmittels muss umgehend dem zuständigen Leistungserbringer gemeldet werden. Weitergehende Regelungen finden sich in den Richtlinien des AIO, beziehungsweise des Polizeikommandos.⁷

12. Fernzugriff

Aus geschäftlichen Gründen kann der oder die Vorgesetzte einer Amtsstelle auf Antrag hin eine Bewilligung für den Fernzugriff erteilen.

Für den Fernzugriff stellt der Leistungserbringer sichere Zugänge zur Verfügung.

13. Nutzung von E-Mail

Die Benutzer sind für den Inhalt ihrer elektronischen Mitteilungen verantwortlich, welche von ihrem geschäftlichen E-Mail-Konto übermittelt werden.

Geschäftliche E-Mails müssen über das geschäftliche E-Mail-Konto versendet werden.

Die Aufbewahrung von E-Mails in der kantonalen Verwaltung und deren automatische Löschung erfolgen nach der Weisung zur Aufbewahrung von E-Mails in der kantonalen

⁷ Absatz geändert mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

Verwaltung⁸. Für die Mitarbeitenden der Polizei gilt die vom Polizeikommando erlassene Weisung.⁹

Besonders schützenswerte Personendaten oder besonders vertrauliche Informationen dürfen nicht mit dem Mailsystem an Personen ausserhalb des kantonalen Netzwerkes versendet werden, sofern keine Verschlüsselung erfolgt.

14. Nutzung von Internet

Über das Netzwerk der kantonalen Verwaltung wird ein beschränkter Internet-Zugang zur Verfügung gestellt. Der Leistungserbringer definiert die Sperrvorgaben für den beschränkten Internetzugang.

Der oder die Vorgesetzte einer Amtsstelle kann einen erweiterten Internet-Zugang bewilligen, wenn geschäftliche Gründe es erfordern.

Es besteht kein Rechtsanspruch auf Zugang zum Internet.

15. Private Nutzung

Die private Nutzung der vom Kanton zur Verfügung gestellten Informatikmittel ist erlaubt.

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

16. Datenzugriff bei unvorhergesehener Abwesenheit, bei Beendigung des Anstellungsverhältnisses oder bei Freistellung

Muss bei unvorhergesehener Abwesenheit, bei Beendigung des Anstellungsverhältnisses oder bei Freistellung eines Benutzers, ohne dass seine Zustimmung eingeholt werden kann, auf dringend benötigte geschäftliche Daten zugegriffen werden können, die nicht in der GEVER-Software oder im Amtslaufwerk gespeichert sind, so muss die vorgesetzte Person beim Departementssekretär oder der Departementssekretärin, beim Staatsschreiber oder der Staatsschreiberin, beim Gerichtsverwalter oder der Gerichtsverwalterin, bzw. deren Stellvertretungen, einen begründeten Antrag auf Datenzugriff stellen. Der Zugriff erfolgt in Anwesenheit einer vorgesetzten Person und der Departementssekretärin oder des Departementssekretärs, resp. der Staatsschreiberin oder des Staatsschreibers, resp. der Gerichtsverwalterin oder des Gerichtsverwalters, bzw. deren Stellvertretungen.¹⁰

Auf privat gekennzeichnete oder auf offensichtlich privat erkennbare Ordner, E-Mails oder Dateien darf nicht zugegriffen werden.

Der Zugriff muss zeitlich befristet sein. Der Leistungserbringer muss das Konto des abwesenden Benutzers nach erfolgtem Zugriff wieder sperren. Der Vorgang mit Beschreibung der Zugriffe wird durch die vorgesetzte Person protokolliert und der abwesenden Person nach deren Rückkehr ausgehändigt.

Der Leistungserbringer erstattet dem oder der Beauftragten für Information und Datenschutz jährlich summarisch Bericht über die erfolgten Zugriffe.

17. Beendigung des Anstellungsverhältnisses oder Freistellung

Bei Beendigung des Anstellungsverhältnisses oder bei Freistellung können die Benutzer ihre privaten Daten mitnehmen. Soweit es bei einer Freistellung oder fristlosen Auflösung des Anstellungsverhältnisses aus Sicherheitsgründen erforderlich ist, wird der da-

⁸ RRB Nr. 2017/1744 vom 23. Oktober 2017

⁹ Absatz geändert mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

¹⁰ Absatz und Titel geändert mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

für notwendige Zugriff auf die Netzwerke und Systeme vom Leistungserbringer begleitet und dokumentiert. Nach Beendigung des Anstellungsverhältnisses wird das Benutzerkonto deaktiviert und der persönliche E-Mail-Account sowie das persönliche Benutzerlaufwerk, inklusive der Daten, gelöscht.¹¹

Mobile Informatikmittel

18. Vom Kanton zur Verfügung gestellte Mobiltelefone und Smartphones

Mitarbeitende können bei regelmässigem Arbeiten ausserhalb des Büroarbeitsplatzes die Abgabe eines Mobiltelefons beantragen, um ihre Erreichbarkeit zu gewährleisten.

Mitarbeitende können ein Smartphone beantragen, wenn sie darüber hinaus einen ausgewiesenen beruflichen Bedarf geltend machen für den Zugriff auf das Geschäftsmailsystem.

Zusätzliche Voraussetzungen zu Abgabe und weitergehende Regelungen zu Beschaffung, Support, Schaden, Kosten, etc. finden sich in den Richtlinien des AIO.

Ergänzend gelten für die Mitarbeitenden der Polizei die Richtlinien des Polizeikommandos.¹²

19. Mobile Datenträger

Die Regelungen zu den mobilen Datenträgern finden sich in den Richtlinien des AIO.

Ergänzend gelten für die Mitarbeitenden der Polizei die Richtlinien des Polizeikommandos.¹³

20. Privat beschaffte Mobiltelefone und Smartphones

Mitarbeitende können beantragen, ihr privat beschafftes Mobiltelefon oder Smartphone an ihrem Arbeitsplatz einsetzen zu dürfen. Der schriftliche Antrag ist mit der Einwilligung der oder des Vorgesetzten einer Amtsstelle an den Leistungserbringer zu richten.

Weitergehende Regelungen zur Nutzung der privat beschafften Mobiltelefone und Smartphones finden sich in den Richtlinien des AIO.

Mitarbeitenden der Polizei ist die Benutzung privat beschaffter Mobiltelefone und Smartphones zu dienstlichen Zwecken grundsätzlich untersagt.¹⁴

Missbrauch

21. Missbräuchliche Nutzung

Die Informatikmittel sind ausschliesslich im Rahmen dieser Weisung und der geltenden Rechtsordnung zu benutzen.

Den Benutzern ist es insbesondere untersagt,

- a) die Informatikmittel zur Begehung oder zur Unterstützung widerrechtlicher oder strafbarer Handlungen zu nutzen,
- b) über das Netzwerk der kantonalen Verwaltung auf Daten mit widerrechtlichem, ur-

¹¹ Absatz und Titel geändert mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

¹² Absatz eingefügt mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

¹³ Absatz eingefügt mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

¹⁴ Absatz eingefügt mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

heberrechtsverletzendem, rassistischem, beleidigendem, pornografischem oder herabwürdigendem Inhalt zuzugreifen oder solche zu verbreiten, soweit diese Handlungen nicht im Rahmen eines geschäftlichen Auftrags und im Einverständnis der oder des Vorgesetzten einer Amtsstelle erfolgen; für die Mitarbeitenden der Polizei wird der geschäftliche Auftrag und das Einverständnis vermutet,¹⁵

- c) auf die System- und Netzwerksicherheitsumgebung der kantonalen Verwaltung zuzugreifen oder zu versuchen, die Sicherheitsvorkehrungen zu manipulieren oder zu entfernen,
- d) ohne Zustimmung der oder des Vorgesetzten einer Amtsstelle Programme auf den Arbeitsstationen oder auf den zentralen Rechnern der kantonalen Verwaltung zu installieren oder zu speichern sowie an bestehenden Programmen Änderungen vorzunehmen,
- e) über das Netzwerk der kantonalen Verwaltung Informatikmittel zu privaten Zwecken kommerziell zu nutzen.

Die vorsätzliche oder grobfahrlässige Missachtung von Sicherheitsvorgaben stellt eine missbräuchliche Nutzung dar.¹⁶

22. Sanktionen bei Missbrauch

Die missbräuchliche Nutzung stellt eine Verletzung der Dienstpflichten dar, welche nach dem Gesetz über das Staatspersonal (StPG) vom 27. September 1992¹⁷ und dem Gesetz über die Haftung des Staates, der Gemeinden, der öffentlich-rechtlichen Körperschaften und Anstalten und die Verantwortlichkeit der Behörden, Beamten und öffentlichen Angestellten und Arbeiter vom 26. Juni 1966¹⁸ sanktioniert werden kann.

Strafanzeige erfolgt im Rahmen von § 20 des Einführungsgesetzes zur Schweizerischen Strafprozessordnung und zur Schweizerischen Jugendstrafprozessordnung (EG STPO) vom 10. März 2010¹⁹.

Bei wiederholten Verstössen gegen die Nutzungsvorschriften kann der Leistungserbringer in Absprache mit der vorgesetzten Stelle dem betroffenen Benutzer das Informatikmittel oder die Zugriffsberechtigung auf das Informatikmittel entziehen.

Sind Mitarbeitende der Polizei betroffen, obliegt diese Entscheidung dem Kommandanten.²⁰

Schutz, Überwachung und Kontrollen durch den Leistungserbringer²¹

23. Technische Schutzmassnahmen

Die vom Kanton zur Verfügung gestellten Informatikmittel werden durch geeignete technische Vorkehrungen geschützt, um die Sicherheit von Daten und Anwendungen zu garantieren oder den Betrieb vor Systemüberlastungen zu schützen.

24. Protokollierung

Protokolldaten dürfen zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsgemässen Betriebs einer Datenverarbeitungsanlage aufgezeichnet werden.

Protokolldaten dürfen nicht für eine präventive Verhaltens- oder Leistungsbewertung

¹⁵ Buchstabe geändert mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

¹⁶ Absatz eingefügt mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

¹⁷ BGS 126.1

¹⁸ BGS 124.21

¹⁹ BGS 321.3

²⁰ Absatz eingefügt mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

²¹ Titel geändert mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

der Benutzer verwendet werden.

Vorbehalten bleibt Ziffer 26.²²

25. **Anonyme Auswertung von Protokolldaten**

Der Leistungserbringer nimmt periodisch anonyme Auswertungen von Protokolldaten zur Gewährleistung der technischen Sicherheit, der Funktionsfähigkeit oder der Verfügbarkeit der Informatikmittel sowie zur Überwachung der Einhaltung der Nutzungsvorschriften vor. Zur anonymen Auswertung von Protokolldaten im Zusammenhang mit Awareness-Kampagnen überlässt die Polizei dem AIO die hierfür erforderlichen E-Mail-Accounts der Mitarbeitenden der Polizei.²³

26. **Personenbezogene Auswertung von Protokolldaten**

Bei begründetem Verdacht auf eine missbräuchliche Nutzung von Informatikmitteln, kann der oder die Vorgesetzte einer Amtsstelle, bzw. die Stellvertretung, die personenbezogene Auswertung von Protokolldaten anordnen.

Die personenbezogene Auswertung von Protokolldaten kann ebenfalls vorgenommen werden

- a) bei einer ernsthaften und konkreten Gefährdung der Sicherheit und Verfügbarkeit der Informatikmittel und der Daten der kantonalen Verwaltung, sowie
- b) im Rahmen von Awareness-Kampagnen vom Durchführer der Awareness-Kampagne zur gezielten Schulung und Sensibilisierung von Benutzern. Der Durchführer der Awareness-Kampagne erstellt vollständig anonymisierte Auswertungen. Er meldet dem Personalamt zusätzlich Namen und Fehlverhalten derjenigen Benutzer, die im Abstand von weniger als zwölf Monaten ein zweites oder weiteres Mal eine Phishing-Mail öffnen und auf einen Link, einen Button oder eine Beilage im E-Mail klicken, und zusätzlich
 - User-ID oder E-Mail Adresse und Passwort auf einer Webseite eingeben; oder
 - einen Download von Schadsoftware nach einer aktiven Bestätigung durchführen; oder
 - die einer E-Mail als Anhang beigefügte Datei öffnen und die Makro- bzw. eine Sicherheitswarnung übersteuern.

Das Personalamt bestimmt für diese Benutzer die geeigneten Schulungs- und Sensibilisierungsmassnahmen. Soweit es Schulung und Sensibilisierung erfordern, informiert das Personalamt beim dritten und jedem weiteren Mal, innerhalb von zwölf Monaten seit dem letzten Fehlverhalten, die vorgesetzte Person.²⁴

Grundsätzlich werden die Betroffenen im Voraus über die personenbezogene Prüfung informiert. Auf die Vorankündigung kann verzichtet werden, wenn

- a) die Datensicherheit, insbesondere die Verfügbarkeit des Systems, nicht mehr garantiert werden kann oder wenn
- b) Anhaltspunkte für ein strafbares Verhalten vorliegen.

Die betroffenen Personen sind in diesen Fällen nachträglich über die durchgeführte Auswertung zu informieren.

Wird aufgrund der personenbezogenen Auswertung eine missbräuchliche Nutzung festgestellt, wird die zuständige Dienststelle informiert. Strafanzeige erfolgt im Rahmen von § 20 EG stopp²⁵.

Der Leistungserbringer erstattet dem oder der Beauftragten für Information und Da-

²² Absatz eingefügt mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

²³ Absatz geändert mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

²⁴ Absatz eingefügt mit RRB Nr. 2022/1198 vom 16. August 2022, in Kraft ab 1. September 2022

²⁵ BGS 321.3

tenschutz jährlich Bericht über Art, Umfang und Ergebnis von durchgeführten personenbezogenen Auswertungen.

Schlussbestimmungen

27. Aufhebung bisheriger Weisungen

Mit Inkrafttreten dieser Weisung sind die Weisung über die Benutzung der Informationssysteme und -anwendungen in der kantonalen Verwaltung (RRB vom 1. Juli 2003; Nr. 2003/1296), die Weisung für den Einsatz mobiler Kommunikationsmittel (RRB vom 3. September 2012; Nr. 2012/1793) in der Version 1.40 sowie die Weisung für Beschaffung und Einsatz von iPad in der kantonalen Verwaltung (RRB vom 21. August 2012, Nr. 2012/1714) in der Version 1.0 aufgehoben.

28. Inkrafttreten

Diese Weisung tritt am 1. Januar 2019 in Kraft.