**Synopse**

**Weisung zu Nutzung und Abgabe von Informatikmitteln (RRB Nr. 2018/1864 vom 27. November 2018)**

| | |
|---|---|
| | **Weisung zu Nutzung und Abgabe von Informatikmitteln (RRB Nr. 2018/1864)** |
| | *Der Regierungsrat des Kantons Solothurn*<br><br>gestützt auf § 54 des Gesetzes über das Staatspersonal (StPG) vom 27. September 1992<br><br>*beschliesst:* |
| **2. Geltungsbereich**<br><br>Mit Ausnahme der Solothurner Spitäler AG, der Fachhochschule Nordwestschweiz, der kantonalen Anstalten, der Polizei Kanton Solothurn und des pädagogischen Bereichs der kantonalen Schulen gilt die Weisung für alle Mitarbeitenden der kantonalen Verwaltung, im folgenden auch Benutzer genannt.<br><br>Die Weisung gilt für alle Informatikmittel gem. Ziff. 3, Bst. a). | 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.<br><br>Für die Mitarbeitenden der Polizei Kanton Solothurn (Polizei) gilt die Weisung, soweit sie keine abweichenden Bestimmungen enthält.<br><br>Die Weisung gilt für alle Informatikmittel gem. Ziff. 3, Bst. a). |
| **3. Begriffe**<br><br>Im Sinne dieser Weisung gelten als:<br><br>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 2001.<br><br>b) Daten: Sach- und Personendaten. Der Begriff «Personendaten» richtet sich nach dem InfoDG. | |

| | |
|---|---|
| c) Leistungserbringer: Amt für Informatik und Organisation (AIO) oder weitere von der kantonalen Verwaltung beauftragte Dienstleister. | c) Leistungserbringer: 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 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, Smartphones, Druckersysteme und Telefonie-Services). | 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 Informatikmittel und Daten zu beschaffen. |

| | |
|---|---|
| | n) Makro-/Sicherheitswarnung: Warnmeldung, dass beim Weiterfahren ein automatisiertes Hilfsprogramm ausgelöst oder eine andere Sicherheitsmassnahme übersteuert wird. |
| **11. Verlust und Diebstahl**<br><br>Der Verlust oder Diebstahl eines Informatikmittels muss umgehend dem zuständigen Leistungserbringer gemeldet werden. Weitergehende Regelungen finden sich in den Richtlinien des AIO. | <br><br>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. |
| **13. Nutzung von E-Mail**<br><br>Die Benutzer sind für den Inhalt ihrer elektronischen Mitteilungen verantwortlich, welche von ihrem geschäftlichen E-Mail-Konto übermittelt werden.<br><br>Geschäftliche E-Mails müssen über das geschäftliche E-Mail-Konto versendet werden.<br><br>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 Verwaltung.<br><br>Besonders schützenswerte Personendaten oder besonders vertrauliche Informationen dürfen nicht mit dem Mailsystem an Personen ausserhalb des kantonalen Netzwerkes versendet werden, sofern keine Verschlüsselung erfolgt. | <br><br><br><br><br><br>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 Verwaltung. Für die Mitarbeitenden der Polizei gilt die vom Polizeikommando erlassene Weisung. |

| | |
|---|---|
| **16. Datenzugriff bei unvorhergesehener Abwesenheit**<br><br>Muss bei der unvorhergesehenen Abwesenheit 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.<br><br>Auf privat gekennzeichnete oder auf offensichtlich privat erkennbare Ordner, E-Mails oder Dateien darf nicht zugegriffen werden.<br><br>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.<br><br>Der Leistungserbringer erstattet dem oder der Beauftragten für Information und Datenschutz jährlich summarisch Bericht über die erfolgten Zugriffe. | **16. Datenzugriff bei unvorhergesehener Abwesenheit, bei Beendigung des Anstellungsverhältnisses oder bei Freistellung**<br><br>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. |
| **17. Beendigung des Anstellungsverhältnisses**<br><br>Bei Beendigung des Anstellungsverhältnisses können die Benutzer ihre privaten Daten mitnehmen. Nach Beendigung des Anstellungsverhältnisses wird das Benutzerkonto deaktiviert und der persönliche E-Mail-Account sowie das persönliche Benutzerlaufwerk, inklusive der Daten, gelöscht. | **17. Beendigung des Anstellungsverhältnisses oder Freistellung**<br><br>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 dafür 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. |

| | |
|---|---|
| **18. Vom Kanton zur Verfügung gestellte Mobiltelefone und Smartphones**<br><br>Mitarbeitende können bei regelmässigem Arbeiten ausserhalb des Büroarbeitsplatzes die Abgabe eines Mobiltelefons beantragen, um ihre Erreichbarkeit zu gewährleisten.<br><br>Mitarbeitende können ein Smartphone beantragen, wenn sie darüber hinaus einen ausgewiesenen beruflichen Bedarf geltend machen für den Zugriff auf das Geschäftsmailsystem.<br><br>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. |
| **19. Mobile Datenträger**<br><br>Die Regelungen zu den mobilen Datenträgern finden sich in den Richtlinien des AIO. | Ergänzend gelten für die Mitarbeitenden der Polizei die Richtlinien des Polizeikommandos. |
| **20. Privat beschaffte Mobiltelefone und Smartphones**<br><br>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.<br><br>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. |

| | |
|---|---|
| **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, urheberrechtsverletzendem, 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, | b) über das Netzwerk der kantonalen Verwaltung auf Daten mit widerrechtlichem, urheberrechtsverletzendem, 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, |
| 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. |

| | |
|---|---|
| **22. Sanktionen bei Missbrauch**<br><br>Die missbräuchliche Nutzung stellt eine Verletzung der Dienstpflichten dar, welche nach dem Gesetz über das Staatspersonal vom 27. September 1992 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 1966 sanktioniert werden kann.<br><br>Strafanzeige erfolgt im Rahmen von § 20 des Einführungsgesetzes zur Schweizerischen Strafprozessordnung und zur Schweizerischen Jugendstrafprozessordnung (EG STPO) vom 10. März 2010.<br><br>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. |
| **Schutz, Überwachung und Kontrollen** | **Schutz, Überwachung und Kontrollen durch den Leistungserbringer** |
| **24. Protokollierung**<br><br>Protokolldaten dürfen zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsgemässen Betriebs einer Datenverarbeitungsanlage aufgezeichnet werden.<br><br>Protokolldaten dürfen nicht für eine präventive Verhaltens- oder Leistungsbewertung der Benutzer verwendet werden. | Vorbehalten bleibt Ziffer 26. |

| | |
|---|---|
| **25. Anonyme Auswertung von Protokolldaten**<br><br>Das Amt für Informatik und Organisation 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. | 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. |
| **26. Personenbezogene Auswertung von Protokolldaten**<br><br>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<br><br>a) bei einer ernsthaften und konkreten Gefährdung der Sicherheit und Verfügbarkeit der Informatikmittel und der Daten der kantonalen Verwaltung, sowie<br><br>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<br><br>- User-ID oder E-Mail Adresse und Passwort auf einer Webseite eingeben; oder<br>- einen Download von Schadsoftware nach einer aktiven Bestätigung durchführen; oder<br>- die einer E-Mail als Anhang beigefügte Datei öffnen und die Makro- bzw. eine Sicherheitswarnung übersteuern.<br><br>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. |

| | |
|---|---|
| Grundsätzlich werden die Betroffenen im Voraus über die personenbezogene Prüfung informiert. Auf die Vorankündigung kann verzichtet werden, wenn<br><br>a) die Datensicherheit, insbesondere die Verfügbarkeit des Systems, nicht mehr garantiert werden kann oder wenn<br><br>b) Anhaltspunkte für ein strafbares Verhalten vorliegen.<br><br>Die betroffenen Personen sind in diesen Fällen nachträglich über die durchgeführte Auswertung zu informieren.<br><br>Wird aufgrund der personenbezogenen Auswertung eine missbräuchliche Nutzung festgestellt, wird die zuständige Dienststelle informiert. Strafanzeige erfolgt im Rahmen von § 20 EG StPO.<br><br>Der Leistungserbringer erstattet dem oder der Beauftragten für Information und Datenschutz jährlich Bericht über Art, Umfang und Ergebnis von durchgeführten personenbezogenen Auswertungen. | |
| | Die Änderungen treten am 1. September 2022 in Kraft. |
| | Solothurn, 16. August 2022<br><br>Im Namen des Regierungsrates<br><br><br>Dr. Remo Ankli<br>Landammann<br><br><br>Andreas Eng<br>Staatsschreiber |