

Weisungen für den Umgang mit Informatik-Mitteln und Daten im Eidg. Departement für Wirtschaft, Bildung und Forschung (WIM-WBF)

vom 1. Januar 2014 (Stand am 1. Januar 2014)

Das Eidgenössische Departement für Wirtschaft, Bildung und Forschung (WBF),

gestützt auf Art. 30 Bst. g der Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998¹ (RVOV), das Bundespersonalgesetz vom 24. März 2000² (BPG) und die Bundespersonalverordnung vom 3. Juli 2001³ (BPV)

beschliesst:

1 Allgemeine Bestimmungen

1.1 Zweck

Das WBF stellt seinen Mitarbeitenden für die Erfüllung ihrer Aufgaben IKT-Mittel zur Verfügung. Sie sind beim Einsatz dieser Mittel für die Einhaltung der nachfolgenden Weisungen persönlich verantwortlich. Diese gelten auch für die Massnahmen zum Schutz der bearbeiteten und übermittelten Daten.

1.2 Geltungsbereich

Die Weisungen gelten unabhängig vom Standort für alle Mitarbeitenden des WBF sowie für weitere Personen, soweit sie Zugang zu IKT-Mitteln des WBF haben. Die Weisungen sind Bestandteil des Vertragsverhältnisses. Der Informatiksicherheitsbeauftragte oder der Integrationsmanager der Verwaltungseinheit können zur Erläuterung der Weisungen beigezogen werden.

1.3 Begriffe

IKT-Mittel im Sinne dieser Weisung sind Mittel der Informations- und Kommunikationstechnologie, also Hardware (Computer, Datenträger, Smartphones, Tablets, usw.), Software, Netzwerke und IKT-Dienste.

Das *Bürokommunikationsnetz* ist das Computernetzwerk des Bundes, welches die Büroarbeitsplätze miteinander verbindet.

Das *Geschäftsverwaltungssystem* (GEVER) ist ein System zur ordnungsgemässen Aufbewahrung der geschäftsrelevanten Dokumente.

Zugangsdaten sind alle Angaben, welche den Zugang zu einem Benutzerkonto schützen. Dazu gehören Passwörter, persönliche Identifikationsnummern (PIN) oder Smartcards.

Als *Leistungserbringer* werden diejenigen Verwaltungseinheiten oder externen Firmen bezeichnet, welche Informatikleistungen anbieten oder betreiben.

Schützenswerte Daten sind Geschäftsgeheimnisse, Daten ab der Klassifikationsstufe VERTRAULICH gemäss ISchV⁴ sowie besonders schützenswerte Personendaten gemäss DSG⁵.

¹ SR 172.010.1

² SR 172.220.1

³ SR 172.220.111.3

⁴ SR 510.411

⁵ SR 235.1

2 Umgang mit IKT-Mitteln

2.1 Geschäftlicher Einsatz von geschäftlichen IKT-Mitteln

- 2.1.1 Zur Erfüllung der Aufgaben werden die vom Arbeitgeber zur Verfügung gestellten standardisierten IKT-Mittel eingesetzt.
- 2.1.2 Notebooks und PCs, die nicht permanent mit dem Bürokommunikationsnetz verbunden sind, müssen regelmässig an dieses angeschlossen werden.
- 2.1.3 Notebooks und PCs sind bei Nichtgebrauch am Ende des Arbeitstages herunterzufahren.
- 2.1.4 Das selbständige Installieren von Software auf PCs und Notebooks ist untersagt. Das Herunterladen und Installieren von betrieblicher Software erfolgt ausschliesslich durch die dazu autorisierten Stellen.
- 2.1.5 Das Modifizieren der Hard- und Software ist untersagt.

2.2 Privater Einsatz von geschäftlichen IKT-Mitteln

- 2.2.1 Die Benutzung der IKT-Mittel für private Zwecke ist unter Beachtung der nachfolgenden Regeln gestattet, solange
 - die beanspruchten Ressourcen (insbesondere Arbeitszeit, Netz- und Speicherkapazität, Verbrauchsmaterial) vernachlässigbar sind,
 - sie im Rahmen der Rechtsordnung erfolgt,
 - die Aufgabenerfüllung nicht beeinträchtigt wird,
 - die Sicherheit der IKT-Mittel und Daten gewährleistet bleibt
 - und die Interessen der Bundesverwaltung jederzeit gewahrt werden.
- 2.2.2 Ausdrücklich untersagt ist der Zugriff auf Internetseiten mit widerrechtlichem, herabwürdigendem oder pornographischem Inhalt sowie das Weiterleiten von entsprechenden Inhalten und Links.
- 2.2.3 Das selbständige Installieren von Software aller Art auf geschäftlichen PCs und Notebooks ist untersagt.

2.3 Geschäftlichen Einsatz von privaten IKT-Mitteln

- 2.3.1 Die Verwendung privater IKT-Mittel richtet sich nach den übergeordneten Weisungen des Bundesrates über die Informatiksicherheit.¹
- 2.3.2 Sofern die Benutzung privater IKT-Mittel für geschäftliche Zwecke gestattet ist, sind die Sicherheit und die Interessen der Bundesverwaltung jederzeit zu gewährleisten.
- 2.3.3 Verboten sind insbesondere der Anschluss von Privatgeräten an das Bürokommunikationsnetz des Bundes, die Bearbeitung von schützenswerten Daten (3.1.4) und die Gefährdung der Sicherheit (analog 2.2.1), beispielsweise durch infizierte Datenträger.

¹ Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung, sowie die entsprechenden Anhänge des ISB.

3 Umgang mit Daten

3.1 Ablage und Bearbeitung

- 3.1.1 Die für die Aufgabenerfüllung notwendigen Daten sind unter Beachtung der Aktenführungs-
pflicht in den dafür vorgesehenen Dateiablagen so abzulegen, dass der Zugang durch befugte
Personen gewährleistet ist. Dazu gehört insbesondere das Geschäftsverwaltungssystem.
- 3.1.2 Bei der Speicherung dienstlicher Dateien ausserhalb von Geschäftsverwaltungssystemen und
Fachanwendungen sind angemessene Massnahmen zum Schutz der Daten und zur Sicherstel-
lung der Geschäftskontinuität zu treffen.
- 3.1.3 Die Übermittlung und Bearbeitung von schützenswerten Daten ist nur verschlüsselt gestattet.
- 3.1.4 Schützenswerte Daten dürfen nicht mit privaten IKT-Mitteln bearbeitet werden.
- 3.1.5 Die Veröffentlichung geschäftlicher Informationen (bspw. mittels Twitter, Blog) ist bewilli-
gungspflichtig.
- 3.1.6 Persönliche Dateiablagen inkl. Mailboxen werden beim Ausscheiden aus dem Dienst bzw.
nach Beendigung des Arbeitsverhältnisses gelöscht.
- 3.1.7 Das WBF lehnt jede Haftung im Zusammenhang mit privaten Daten ab.
- 3.1.8 Nicht erlaubt ist die Verwendung der geschäftlichen E-Mail Adresse, um sich Vorteile aus-
serhalb des geschäftlichen Umfelds zu verschaffen (beispielsweise durch Ausnützung der ge-
schäftlichen Position).
- 3.1.9 Die Postfachgrösse des E-Mail Programms ist begrenzt. Die für die Aufgabenerfüllung not-
wendigen, beziehungsweise geschäftsrelevanten Daten aus dem Mail-Verkehr sind fortlaufend
im Geschäftsverwaltungssystem abzulegen.

3.2 Besonderer Umgang mit Zugangsdaten

- 3.2.1 Persönliche Zugangsdaten dürfen niemandem weitergegeben werden.
- 3.2.2 Der Zugang auf Geschäftsdaten durch Stellvertreter ist ohne die Weitergabe der persönlichen
Zugangsdaten sicherzustellen.

4 Überwachung und Sanktionen

- 4.1 Bei der Verwendung der geschäftlichen IKT-Mittel werden sämtliche Aktivitäten aufgezeichnet und können im Rahmen der Rechtsordnung ausgewertet werden.
- 4.2 Bestehen Anhaltspunkte für einen Missbrauch, erstattet der jeweilige Leistungserbringer über den Informatiksicherheitsbeauftragten der Verwaltungseinheit der für Arbeitgeberentscheide zuständigen Stelle¹ Meldung. Erhält die Stelle auf anderem Weg Hinweise auf einen möglichen Missbrauch, geht sie analog vor.
- 4.3 Die für Arbeitgeberentscheide zuständige Stelle kann bei Bedarf in Übereinstimmung mit der Datenschutzgesetzgebung und unter Orientierung des oder der Betroffenen weitere benutzerspezifische Abklärungen veranlassen und Massnahmen treffen. Gegebenenfalls verfügt sie disziplinar- und arbeitsrechtliche Sanktionen oder erstattet bei der Bundesanwaltschaft Anzeige. Schadenersatzansprüche bleiben vorbehalten.
- 4.4 Eine missbräuchliche Benutzung hat disziplinar- und arbeitsrechtliche Konsequenzen. Das Vorgehen richtet sich nach dem Bundespersonalgesetz.

5 Inkrafttreten

Diese Weisungen treten am 1. Januar 2014 in Kraft und ersetzen die Weisungen vom 25. März 2004 (Stand: 1. November 2005).

EIDGENÖSSISCHES DEPARTEMENT FÜR
WIRTSCHAFT, BILDUNG UND FORSCHUNG WBF



i.A. Monika Rühl
Generalsekretärin

Geht an:

- VE WBF zum Vollzug

¹ Weisungen über das Personalwesen im WBF (WHR-WBF)