

Vereinbarung über die Nutzung des Internetzugangs und des E-Mail-Dienstes sowie den Einsatz der Kommunikationsplattform Skype for Business im BMBF

Teil 1: Nutzung des Internetzugangs und des E-Mail-Dienstes

§ 1 Gegenstand; Begriffsbestimmung; Geltungsbereich

- (1) Diese Vereinbarung regelt die Nutzung des Internetzugangs und des E-Mail-Dienstes im Bundesministerium für Bildung und Forschung (BMBF).
- (2) Mit E-Mail-Dienst wird die E-Mail-spezifische Funktionalität von Outlook beim Empfangen, Bearbeiten, Versenden und Ablegen von elektronischer Post (E-Mail) über das Exchange-System im BMBF bezeichnet.
- (3) Die Nutzung von webbasierten E-Mail-Systemen im Internet unterliegt den Regelungen bezüglich der Nutzung des Internetzugangs in dieser Vereinbarung.

§ 2 Dienstliche und private Nutzung von Internetzugang und E-Mail-Dienst

- (1) Den Beschäftigten stehen Internetzugang und E-Mail-Dienst als Arbeitsmittel im Rahmen der Aufgabenerfüllung grundsätzlich zur Verfügung und dienen insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse.
- (2) Die private Nutzung des Internetzugangs in geringfügigem Umfang ist zulässig, soweit die dienstliche Aufgabenerfüllung sowie die Verfügbarkeit des IKT-Systems für dienstliche Zwecke nicht beeinträchtigt werden.
- (3) Das Abrufen von kostenpflichtigen Informationen und die Nutzung kostenpflichtiger Dienste für den Privatgebrauch sind nicht zulässig. Im Rahmen der privaten Nutzung des Internetzugangs dürfen keine kommerziellen Zwecke verfolgt werden.
- (4) Protokollierung und Kontrolle gemäß § 7 DV-IKT erstrecken sich auch auf den Bereich der privaten Nutzung des Internetzugangs.
- (5) Durch die private Nutzung des Internetzugangs erklären die Beschäftigten ihre Einwilligung in die Protokollierung und Kontrolle gemäß § 7 DV-IKT für den Bereich der privaten Nutzung.
- (6) Der Versand privater Mails ist nicht zulässig. Aus dienstlichem Anlass erstellte private E-Mails gelten als dienstliche E-Mails und dürfen über das dienstliche E-Mail-Postfach versendet werden. Eingehende private Mails sind zu löschen, anderenfalls werden die Daten im Rahmen

der üblichen Datensicherung gespeichert. Aus Sicherheitsgründen kann die Internetnutzung beschränkt oder gesperrt werden. Der Personalrat und die Beschäftigten werden zeitnah informiert.

- (7) Einzelheiten zum internen und behördenübergreifenden Einsatz des dienstlichen E-Mail-Dienstes sind in EGO-BMBF 7.5 festgelegt.
- (8) Hinweise und Regelungen für die dienstliche und private Nutzung von sozialen Netzwerken im Internet (Social Media) sind in der Hausanordnung Nr. 3/2012 festgelegt.
- (9) Nicht zulässig ist jede Nutzung des Internet- und des E-Mail-Dienstes, die geeignet ist, den Interessen der Dienststelle oder deren Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Behördennetzes zu beeinträchtigen oder die gegen geltende Rechtsvorschriften verstößt. Dies gilt vor allem für das Abrufen oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen sowie das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, Gewalt verherrlichenden oder pornografischen Äußerungen oder Abbildungen.
- (10) Ferngesteuerte Zugriffe oder Steuerungen von Rechnersystemen über sogenannte Remote-Anwendungen bzw. Terminal-Emulationen sind grundsätzlich nicht zugelassen. Sollte hierfür dienstlicher Bedarf bestehen, ist dies beim IT-Referat unter Angabe der Gründe zu beantragen.

§ 3 Filterung

- (1) Alle eingehenden E-Mails werden durch eine Firewall, einen Spam-Filter sowie Virens Scanner geprüft bzw. gefiltert.
- (2) Der Zugriff auf Internet-Seiten mit beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, Gewalt verherrlichenden oder pornografischen Inhalten kann mit Hilfe einer Filtersoftware automatisch blockiert werden. Die Filterung kann sich auch auf weitere Seiten beziehen, die keinerlei dienstlichen Bezug haben (z. B. Chats). Die zu blockierenden Kategorien werden zwischen Dienststelle und Personalrat abgestimmt.
- (3) Der Eingang von E-Mails mit beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, Gewalt verherrlichenden oder pornografischen Inhalten (Spam-Mails) kann mit Hilfe einer Filtersoftware automatisch abgewiesen werden. Wie mit den abgewiesenen E-Mails verfahren wird, wird zwischen Dienststelle und Personalrat abgestimmt.
- (4) Der Eingang von Schadsoftware, die Computerviren oder Computerwürmer enthält, kann automatisch abgewiesen werden.

§ 4 Protokollierung und Kontrolle beim Internetzugang

- (1) Die folgenden Verbindungsdaten für den Internetzugang werden elektronisch protokolliert:

- Datum / Uhrzeit;
 - IP-Adressen von Absender und Empfänger;
 - übertragene Datenmenge.
- (2) Die Protokolldateien nach Absatz 1 werden ausschließlich zu den folgenden Zwecken verwendet:
- Analyse und Korrektur technischer Fehler;
 - Gewährleistung der Systemsicherheit;
 - Optimierung des Netzes;
 - statistische Feststellung des Gesamtnutzungsvolumens;
 - Stichprobenkontrollen gemäß Absatz 4;
 - Auswertungen gemäß § 6 dieser Vereinbarung (Missbrauchskontrolle).
- (3) Die bei der Nutzung des Internetzugangs anfallenden personenbezogenen Daten werden nicht zur Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften.
- (4) Die Protokolldateien werden durch eine(n) von Dienststelle und Personalrat beauftragte/n Beschäftigte/n (Beauftragte/r für die Nutzung des Internetdienstes und des E-Mail-Dienstes) regelmäßig hinsichtlich der übertragenen Datenmenge sowie stichprobenweise hinsichtlich der aufgerufenen Websites (in Form der IP-Adresse), aber nicht personenbezogen gesichtet und ausgewertet.
- (5) Der Zugriff auf die Protokolldateien für die Zwecke gemäß Absatz 2 ist auf die mit der Systemadministration betrauten Personen und den/die gemäß Absatz 4 beauftragte(n) Beschäftigte(n) begrenzt. Diese haben eine entsprechende Verpflichtungserklärung zum Datenschutz zu unterschreiben. Darüber hinaus werden sie hinsichtlich der Einhaltung des Fernmeldegeheimnisses und des Datenschutzes auf die strafrechtlichen Konsequenzen bei Verstößen hingewiesen.
- (6) Die Protokolldateien, mit Ausnahme der Daten bezüglich des monatlichen Gesamtdatenvolumens, werden nach einer Woche automatisch gelöscht, im Falle von Maßnahmen nach § 6 Absatz 1 erhöht sich die Lösungsfrist auf zwei Wochen. Bei Verdacht auf missbräuchliche/unerlaubte Nutzung des Internetzugangs gemäß §§ 2 und 3 wird die Löschung der relevanten Daten bis zum Abschluss des unter § 6 Absatz 2 beschriebenen Verfahrens ausgesetzt.

§ 5 Protokollierung und Kontrolle beim E-Mail-Dienst

- (1) Die folgenden Daten der eingegangenen und abgesendeten E-Mails werden elektronisch protokolliert:
- Datum / Uhrzeit;
 - E-Mail-Adresse des Absenders und Empfängers;
 - übertragene Datenmenge.

- (2) Die Protokolldateien nach Absatz 1 werden ausschließlich zu den folgenden Zwecken verwendet:
 - Analyse und Korrektur technischer Fehler;
 - Gewährleistung der Systemsicherheit;
 - Optimierung des Netzes;
 - statistische Feststellung des Gesamtnutzungsvolumens;
 - Stichprobenkontrollen gemäß Absatz 4;
 - Auswertungen gemäß § 6 dieser Vereinbarung (Missbrauchskontrolle).
- (3) Die bei der Nutzung des E-Mail-Dienstes anfallenden personenbezogenen Daten werden nicht zur individuellen Leistungs- und Verhaltenskontrolle verwendet. Sie unterliegen der Zweckbindung dieser Vereinbarung und den einschlägigen datenschutzrechtlichen Vorschriften.
- (4) Die Protokolldateien werden durch eine/n von Dienststelle und Personalrat beauftragte/n Beschäftigte/n monatlich stichprobenweise bei 20 Beschäftigten mit dem Ziel überprüft, die missbräuchliche/unerlaubte Nutzung des E-Mail-Dienstes zu verhindern. Bei den Stichproben werden die gemäß Absatz 1 protokollierten Daten bestimmter nach dem Zufallsprinzip ausgewählter und nach außen abgesendeter E-Mails gespeichert und ausgedruckt. Die Ausdrucke und gespeicherten Daten werden spätestens nach drei Monaten vernichtet bzw. gelöscht. Bei Verdacht auf missbräuchliche/unerlaubte Nutzung des E-Mail-Dienstes gemäß §§ 2 und 3 wird die Vernichtung bzw. Löschung bis zum Abschluss des unter § 6 Absatz 2 beschriebenen Verfahrens ausgesetzt.
- (5) Der Zugriff auf die Protokolldateien für die Zwecke gemäß Absatz 2 ist auf die mit der Systemadministration betrauten Personen und den/die gemäß Absatz 4 beauftragte/n Beschäftigte/n begrenzt. Diese haben eine entsprechende Verpflichtungserklärung zum Datenschutz zu unterschreiben. Darüber hinaus werden sie hinsichtlich der Einhaltung des Fernmeldegeheimnisses und des Datenschutzes auf die strafrechtlichen Konsequenzen bei Verstößen hingewiesen.
- (6) Die Protokolldateien, mit Ausnahme der Daten bezüglich des monatlichen Gesamtdatenvolumens und der Stichprobendaten, werden nach einem Monat automatisch gelöscht. Bei Verdacht auf missbräuchliche/unerlaubte Nutzung des E-Mail-Dienstes gemäß §§ 2 und 3 wird die Löschung der relevanten Daten bis zum Abschluss des unter § 6 Absatz 2 beschriebenen Verfahrens ausgesetzt.

§ 6 Maßnahmen bei Verstößen; Missbrauchsregelung

- (1) Ist aufgrund der stichprobenhaften Kontrollen nach § 4 bzw. der Auswertung der übertragenen Datenmenge eine nicht mehr tolerierbare Häufung von offensichtlich privater Nutzung des Internetzugangs zu vermuten, so werden innerhalb einer Frist von 2 Wochen die Stichproben weiterhin nicht-personenbezogen durchgeführt. Ergeben diese Stichproben bzw. die Auswertung der übertragenen Datenmenge keine Änderung im Nutzungsverhalten, so können die Protokolle der folgenden 2 Wochen durch eine gemäß Absatz 2 eingesetzte

Untersuchungsgruppe personenbezogen ausgewertet werden. Hierbei wird wie im Falle einer missbräuchlichen Nutzung (vgl. Absatz 2) vorgegangen. Über die Verfahren nach Satz 1 und Satz 2 werden jeweils alle Beschäftigten vorab informiert.

- (2) Bei Verdacht auf missbräuchliche/unerlaubte Nutzung des Internetzugangs oder des E-Mail-Dienstes gemäß § 2 dieser Vereinbarung durch einzelne Beschäftigte entscheidet AL Z unter Beteiligung des/der behördlichen Datenschutzbeauftragten, ob eine Überprüfung durch eine von ihm einzusetzende Untersuchungsgruppe durchgeführt wird. Dieser Untersuchungsgruppe gehören mindestens der/die nach § 4 Abs. 4 beauftragte Beschäftigte sowie ein/e Vertreter/in des Personalrats und der Dienststelle an. Sie veranlasst gegebenenfalls weitere Untersuchungsmaßnahmen (z. B. Offenlegung der IP-Adresse des benutzten PCs oder weitere Überprüfungen). Auf der Basis dieser Untersuchung erstellt sie einen Bericht, der dem/der Betroffenen ausgehändigt wird. Diese/r ist anschließend dazu zu hören.
- (3) Ein Verstoß gegen diese Vereinbarung kann neben den dienst- und arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben.
- (4) Die Dienststelle behält sich vor, bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs im Einzelfall nach Beteiligung des Personalrates zu untersagen.

Teil 2: Kommunikationsplattform Skype for Business

§ 7 Vorbemerkungen

- (1) Zur Verbesserung der Möglichkeiten der Zusammenarbeit bei geteilten Dienstsitzen und zur Unterstützung der mobilen Arbeit wird den Beschäftigten Skype for Business zur Verfügung gestellt.

§ 8 Ziel und Zweck von Skype for Business

- (1) Skype for Business ist eine Plattform für eine virtuelle Verbindung zwischen den Beschäftigten – zum Führen von Gesprächen als Echtzeitkommunikation, Audio- oder Videokonferenz, zum Freigeben von Desktop und Anwendungen und zur Zusammenarbeit in Echtzeit direkt am Computer.

§ 9 Nutzung

- (1) Skype for Business wird zur Verbesserung und Erweiterung der Möglichkeiten zur direkten Kommunikation und Zusammenarbeit auch auf Distanz eingesetzt.
- (2) Wer an der mobilen Arbeit teilnimmt, ist verpflichtet, Skype for Business zu nutzen. Bei Nutzung der Videofunktion sollte auf den Schutz der Privatsphäre geachtet werden.
- (3) Skype for Business wird nach einem Rechnerneustart automatisch gestartet.

§ 10 Funktionsweise

- (1) Voraussetzung für den Aufbau einer Echtzeit-Kommunikation zwischen zwei oder mehr Computern ist die Kommunikationsbereitschaft aller Teilnehmerinnen oder Teilnehmer. Diese Kommunikationsbereitschaft kann durch die von Skype for Business verwaltete Information „Präsenz“ (Verfügbarkeit) erkennbar sein. Sie zeigt an, ob Beschäftigte zur Kommunikation bereit sind.
- (2) Erleichternd für die Kontaktaufnahme kann die Verwaltung und Gruppierung von Daten zu möglichen Kommunikationspartnerinnen und -partnern in persönlichen Kontaktlisten im gegenseitigen Einverständnis sein (analog zu Outlook-Verteilerlisten).
- (3) Die Funktion „Präsenz“ bietet ferner bereits von Telefonlisten oder dem Who-Is-Who bekannte Informationen über die Kommunikationspartnerinnen und -partner (z. B. Kommunikations- und Organisationsdaten wie Telefonnummer und Raumnummer) und Informationen zu deren Kommunikationsbereitschaft in leicht erreichbarer Form an.
- (4) Diese Funktionalitäten sind standardmäßig deaktiviert und können individuell durch die Teilnehmenden selbst aktiviert werden.

§ 11 Status der Kommunikationsbereitschaft (Präsenz)

- (1) Die Funktion Kommunikationsbereitschaft (Präsenz) dient ausschließlich dem Ziel einer einfachen und schnellen direkten Kontaktaufnahme und unterliegt folgenden Vereinbarungen:
 - Die Teilnehmenden entscheiden selbst, ob und für wen ihr Präsenz-Status angezeigt wird.
 - Die Teilnehmenden entscheiden selbst, ob ihr Präsentstatus automatisch aktualisiert werden soll.
 - Der Präsenz-Status kann alternativ jederzeit manuell ausgewählt oder ganz abgeschaltet werden.
 - Ein manuell gesetzter Status bleibt unverändert, bis er erneut manuell geändert wird. Dies gilt auch nach Beenden und Neustart von Skype for Business oder einem Neustart des Rechners.
 - Beschäftigte sind nicht verpflichtet, sich in Skype for Business-Kontaktlisten aufnehmen zu lassen.
 - Es erfolgt keine Protokollierung des Status zur Kommunikationsbereitschaft.
 - Die Status-Zeitdaueranzeige mit der angezeigt wird, wie lange Kommunikationspartnerinnen und -partner "Abwesend" oder "Offline" sind, ist im BMBF grundsätzlich dauerhaft deaktiviert.

§ 12 Übermittlung von Sofortnachrichten - Instant Messaging

- (1) Alle Teilnehmenden können über diese Funktion in Echtzeit in Textform kommunizieren. Es erfolgt keine Protokollierung.

§ 13 Audio- und Video-Kommunikation

- (1) Mittels der Audio- und Video-Kommunikation können Beschäftigte miteinander kommunizieren. Bei Bedarf und nach Möglichkeit kann ein Live-Bild über eine interne oder externe Webcam dazu übertragen und so eine PC-Videokonferenz durchgeführt werden.
- (2) Dazu wird ein Pool von Leih-Webcam-Geräten in Berlin und Bonn aufgebaut; eine Serienausstattung der Arbeitsplätze mit internen oder externen Webcams erfolgt nicht. Dauerleihen sind auf Wunsch der Arbeitseinheiten möglich.
- (3) Sofern Arbeitsplätze über eine Webcam verfügen, entscheiden Beschäftigte über aktives Starten der Bildübertragung selbst, ob sie an einer PC-Videokonferenz mit Bildübertragung teilnehmen wollen.
- (4) Bei Konferenzschaltungen oder einem Mitlesen bzw. Mithören über Bildschirm und Lautsprecher müssen alle Teilnehmerinnen und Teilnehmer zu Beginn des Gesprächs darüber informiert werden, wer noch an dem Gespräch teilnimmt.
- (5) Audio- und Videoinhalte werden nicht aufgezeichnet.

§ 14 Gemeinsame Nutzung von Desktopinhalten / Application Sharing

- (1) Im gegenseitigen Einverständnis können gemeinsam der gesamte Bildschirm oder einzelne freigegebene Anwendungen geteilt werden oder eine Fernsteuerung erfolgen. Alle Teilnehmenden entscheiden selbst, ob sie dies zulassen. Damit ist insbesondere in speziellen Fachverfahren eine vom IKT-Service nicht leistbare, unabhängige und standortübergreifende Unterstützung möglich.
- (2) Die Fernsteuerung kann jederzeit abgebrochen werden.

§ 15 Daten / Schnittstellen

- (1) Für die Nutzung von Skype for Business ist keine eigene Benutzerverwaltung erforderlich; Skype for Business benutzt wie Windows das Active Directory. Die Anmeldung kann automatisiert erfolgen, so dass seitens der Beschäftigten keine Doppeleingaben nötig werden.
- (2) Es bestehen keine Schnittstellen mit personenbezogenen Daten zu anderen DV-Verfahren.

§ 16 Auswertungen

- (1) Es werden keine personenbezogenen Auswertungen erstellt. Ggf. systembedingt erhobene Verbindungs-, Inhalts- und Nutzungsdaten werden unmittelbar nach der Nutzung gelöscht.

§ 17 Leistungs- und Verhaltensüberwachung

- (1) Eine Überwachung von Leistung und Verhalten von Beschäftigten ist unzulässig und findet mit Skype for Business nicht statt. Es werden keine personenbezogenen Auswertungen durchgeführt.

§ 18 Datenschutz / Informationssicherheit

- (1) Die Belange des Datenschutzes sind im Rahmen der gesetzlichen und internen Regelungen zu beachten. Die/der Datenschutzbeauftragte steht hierzu beratend zur Verfügung.
- (2) Die internen Regelungen zur Informationssicherheit sind zu beachten. Die/der Beauftragte für IT-Sicherheit steht beratend zur Verfügung.