

Externe Personen

Nutzungsbedingungen und Datenschutzhinweis für
bestimmte IT-Ressourcen der Deutschen Bundesbank

Stand: 06/2021

Inhalt

1	Einleitung.....	3
2	Nutzungsbedingungen.....	3
2.1	Umfang	3
2.2	Bundesbank PC-Arbeitsplatz.....	4
2.3	Telekommunikationsanlagen bei der Deutschen Bundesbank.....	6
2.4	Tablets und Smartphones bei der Deutschen Bundesbank	7
2.5	Nutzung des Internets über einen Internetzugang der Bundesbank.....	9
2.6	Teilnahme am E-Mail-Verkehr über die Infrastruktur der Bundesbank.....	9
2.7	Teilnahme an Chat, Video- und Webkonferenzen über die Infrastruktur der Bundesbank	9
3	Änderungen der Nutzungsbedingungen	10
4	Datenschutzhinweis	10
4.1	Zweck und Umfang der Datenverarbeitung	10
4.2	Rechtsgrundlagen der Datenverarbeitung	12
4.3	Aufbewahrungs- und Löschfristen	13
4.4	Betroffenenrechte.....	13
4.5	Datenschutzbeauftragte	13

1 Einleitung

Im Rahmen von Vertrags- bzw. Kooperationsverhältnissen ermöglicht die Deutsche Bundesbank (nachfolgend auch „Bundesbank“ oder „Bank“) externen, nicht zum Kreis ihrer Beschäftigten gehörenden Personen, ihre elektronischen Informations- und Kommunikationssysteme zu nutzen. Die Bundesbank erlaubt diesen Personen aufgrund ihrer Eigenschaft als

- Auftragnehmer
- Beschäftigte eines auftragnehmenden Unternehmens,
- Beschäftigte eines externen Partners (z. B. einer Behörde wie der Bundespolizei),
- Beschäftigte einer anderen Zentralbank oder
- sonstige betroffene Person (z. B. Praktikant)

(nachfolgend zusammenfassend als „externe Personen“ bezeichnet) ihre elektronischen Informations- und Kommunikationssysteme zu nutzen. Elektronische Informations- und Kommunikationssysteme sind IT-Arbeitsplätze (Desktop-PCs bzw. mobilen PC-Arbeitsplätze, Tablet, Access Portal¹), Telekommunikationssysteme (Telefon, Smartphone, Mobiltelefon, Fax) Anwendungen für Chat, Audiotelefonie, Videotelefonie und Webkonferenzen sowie Dokumentenmanagementsysteme, E-Mail, Intranet- und Internet-Zugang (nachfolgend zusammenfassend als „IT-Ressourcen“ bezeichnet).

Die nachstehenden Bestimmungen regeln verbindlich den Umgang mit den IT-Ressourcen und enthalten die hierfür gültigen benutzerbezogenen Bestimmungen.

Dieses Dokument fasst die Nutzungsbedingungen für alle IT-Ressourcen zusammen, die die Deutsche Bundesbank auch externen Personen zur Verfügung stellt. Die jeweils zu beachtenden Bedingungen bestimmen sich nach dem individuell bereitgestellten Umfang an IT-Ressourcen.

2 Nutzungsbedingungen

2.1 Umfang

Die Bundesbank erlaubt externen Personen die Nutzung ihrer IT-Ressourcen nur zur Erfüllung der vereinbarten Pflichten und unter Einhaltung der hier aufgeführten Nutzungsbedingungen.

Die private Nutzung der IT-Ressourcen ist nicht gestattet.

Unbeschadet weiterer vertraglicher Regelungen ist generell jede Nutzung der IT-Ressourcen durch die externe Person unzulässig, die geeignet ist, den Interessen der Deutschen Bundesbank oder deren Ansehen in der Öffentlichkeit zu schaden, die Sicherheit des Netzwerks der Bundesbank zu beeinträchtigen, oder die gegen geltende Rechtsvorschriften verstößt. Dies gilt vor allem für das Abrufen, Erstellen, Speichern, Ausdrucken oder Verbreiten von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen. Ferner für das Abrufen, Erstellen, Speichern, Ausdrucken oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden, pornografischen oder sonstigen sittenwidrigen Äußerungen oder Abbildungen, die Nutzung von interaktiven Spielen, die Teilnahme an Versteigerungen, Verlosungen, Wetten und Glücksspielen sowie den Zugriff auf Seiten mit Hacker-Instrumenten,

¹ Außer Access Portal für Partner

Malware und anderen zu Angriffen auf die System- und Netzsicherheit der Bank geeigneten Softwareinstrumenten.

2.2 Bundesbank PC-Arbeitsplatz

2.2.1 Allgemeines

Soweit der externen Person die Nutzung eines PC-Arbeitsplatzes, eines Standalone-PC-Arbeitsplatzes bzw. eines mobilen PC-Arbeitsplatzes eingeräumt wird, handelt es sich nach Art und Ausstattung einschließlich Software um solche, die von der Bank üblicherweise ihrem eigenen Personal zur Verfügung gestellt werden. Die externe Person hat keinen Anspruch auf einen bestimmten Rechner bzw. bestimmte Rechnereigenschaften. Dies gilt auch für die vorhandene Software. Externe Personen dürfen die Ausstattung nicht verändern und die vorhandene Software nicht entfernen. Nach Beendigung der Tätigkeit ist bereitgestelltes Equipment ohne Aufforderung an die Lokalen IT-Services (LITS) zurückzugeben.

2.2.2 Zugang mit Bundesbank-Ausweis und PIN

Der Zugang zu den IT-Arbeitsplätzen der Bundesbank (PC-Arbeitsplatz, Standalone-PC-Arbeitsplatz und mobiler PC-Arbeitsplatz) sowie zur Anmeldung an ausgesuchten Anwendungen des ESZB ist auf Basis des Bundesbank-Ausweises und einer zugehörigen PIN möglich (2-Faktor-Authentifizierung).

Der Bundesbank-Ausweis ist immer mit sich zu führen oder an einem sicheren Ort geschützt vor dem Zugriff von Dritten aufzubewahren. Nicht zulässig sind insbesondere

- die Weitergabe an Dritte
- die Hinterlegung als Pfand bei Dritten oder
- das Verlassen des Arbeitsplatzes, ohne den Bundesbank-Ausweis aus dem Computer zu entfernen.

Lediglich eine Übergabe der Karte an das für die Initialisierung der Karte oder die Kontrolle der Karte zuständige Personal ist zulässig.

Ein Verlust oder Vergessen der Karte ist umgehend an die Sperrhotline 069 9566-11100 zu melden, damit die Karte nicht weiter für den Zugang und Anmeldung genutzt werden kann. Sie erhalten dann in Folge einen Ersatzausweis.

Für die PIN gelten adäquate Regelungen wie für Kennwörter

- 6-stellig, numerisch
- Sperrung nach 3 Fehlversuchen
- Die PIN kann jederzeit durch den Inhaber des Benutzerkontos verändert werden.
- Die Verwendung von sog. Trivial-PINs (z. B. 111111, 123456) sollte vermieden werden.

Die PIN ist geheim zu halten und darf nicht an andere Personen (auch Administratoren oder Beschäftigte des Help Desk) weitergegeben werden. Eine Unterstützung bei auftretenden Problemen der PC-Nutzung ist auch ohne Kenntnis der PIN möglich.

In folgenden Situationen sollte die PIN gewechselt werden:

- wenn eine andere Person Kenntnis von individuell vergebenen PIN bekommen hat oder Zugang zu der Karte hatte oder

- wenn der Verdacht besteht, dass eine andere Person Kenntnis von der PIN bekommen hat oder Zugang zu der Karte hatte.

Soweit beim Verlassen des Arbeitsplatzes keine Abmeldung vom System erfolgt, ist der IT-Arbeitsplatz in geeigneter Weise vor unbefugtem Zugriff auf Daten und Anwendungen zu sperren. Dies geschieht normalerweise durch Ziehen des Bundesbank-Ausweises, welches zu einem Sperren des Systems führt. Die Entsperrung erfolgt durch erneutes Stecken des Bundesbank-Ausweises und PIN-Eingabe.

2.2.3 Zugang zu speziellen Anwendungen & Access-Portal

Die Anmeldung mit Benutzerkennung und Kennwort wird für spezielle Anwendungsfälle, u. a. den Zugriff über das Access Portal (<https://ap.bundesbank.de>), benötigt. Für den Zugang über Access-Portal wird zusätzlich als zweiter Faktor ein RSA-Token benötigt. Hierbei ist

- Access-Portal nur von bekannten Geräten an sicheren Orten zu nutzen und
- Die Citrix Workspace App, der Virenschanner sowie das Betriebssystem des Gerätes immer aktuell zu halten.

Bei der erstmaligen Anmeldung an bestimmten Anwendungen ist ein ggf. vorhandenes Initialkennwort verfahrensgemäß durch ein persönliches Kennwort zu ersetzen. Für den Aufbau von Kennwörtern gelten spezielle Sicherheitsrichtlinien, die produktbezogen in den jeweiligen Benutzeranleitungen der Anwendungen dokumentiert sind und den externen Personen zugänglich gemacht werden. Das Wissen über die Kennwörter darf keiner anderen Person weitergegeben werden. Dies gilt auch bei einem erweiterten Zugangsschutz für das Authentifizierungsmedium (z. B. Chipkarte, Token), das sich nur im Besitz der zugangsberechtigten Person bzw. Personen befinden darf.

2.2.4 Eingesetzte Software

Auf IT-Systemen im Arbeitsplatzumfeld darf ausschließlich von der Bank freigegebene Software verwendet werden. Deren Bereitstellung erfolgt in Verantwortung der zuständigen Stelle (im Regelfall Lokaler IT-Service (LITS)). Eigenmächtiges Installieren von Software auf bankeigenen Geräten sowie die Nutzung von nicht freigegebener/privater Software (auch sog. portable Versionen) auf bankeigenen Geräten (auch auf portablen Speichermedien) ist untersagt.

Unbefugte Systemmodifikationen, z. B. Deaktivierung von Schutzfunktionen, und die Einrichtung lokaler Administrationsrechte für im Netz der Bank betriebene PC-Arbeitsplätze sind unzulässig. Die Bank behält sich vor, einem etwaigen begründeten Begehren der externen Person Rechnung zu tragen, soweit ihre berechtigten Interessen, etwa Sicherheitsinteressen, diesem nicht entgegenstehen. Die externe Person hat hierauf aber keinen Anspruch.

Das Anfertigen von Kopien von bei der Bank eingesetzter Software ist untersagt.

2.2.5 Umgang mit Daten

Es ist nicht gestattet, Kopien von Datenbeständen der Bank anzufertigen.

Soweit der externen Person Zugang zu Datenbeständen (z. B. Konfigurationen, Datenbanken) der Bank eingeräumt ist, hat sie diese vor einem Zugriff bzw. vor einer Einsichtnahme durch Unbefugte zu schützen.

Daten dürfen nur nach ausdrücklicher Genehmigung durch die Bank vervielfältigt bzw. versendet werden.

Daten sind grundsätzlich in FAVIS, auf den bankweit zur Verfügung stehenden Netz- bzw. Gruppenlaufwerken oder in zentraler, geschützter Umgebung (z. B. Notes) zu speichern. Für zusätzlichen Speicherbedarf erhält jede Benutzerin bzw. jeder Benutzer zusätzlich einen individuellen Speicherort (persönliches Verzeichnis) in Form eines Netzlaufwerkes.

Die Nutzerin bzw. der Nutzer eines mobilen PC-Arbeitsplatzes (Notebook) ist dafür verantwortlich, dass durch dessen Einsatz kein Datenverlust für die Bundesbank eintritt. Daher gilt insbesondere:

- Das Notebook darf nie unbeaufsichtigt sein bzw. ist gegen Diebstahl zu schützen.
- Die persönlichen Zugangsinformationen sind geheim zu halten.
- Es ist darauf zu achten, dass Dritte die auf dem Bildschirm angezeigten Daten (v. a. PIN oder sonstige Passwörter) nicht mitlesen können.
- Das Notebook darf nicht in kritischen Staaten gem. Staatenliste des BMI genutzt werden.

Bei Nichtgebrauch ist der mobile Arbeitsplatz logisch von allen Datennetzen zu trennen, auszuschalten und sorgfältig aufzubewahren, um etwa Diebstähle zu vermeiden. Insbesondere sind Verschlussmöglichkeiten zu nutzen.

Zum Zeitpunkt der Beendigung des Überlassungszeitraums muss die externe Person eventuell von ihr gespeicherte Dateien sowie gesendete oder empfangene E-Mails löschen, soweit sie nicht vertragsgemäß der Bank zustehen und als aktenrelevantes Schriftgut in FAVIS oder einem anderen geeigneten revisionssicheren Expertensystem abzulegen sind. Unterlässt sie dies, ist die Bank ohne weiteres zur Löschung berechtigt. Das gleiche gilt, wenn von den Dateien oder E-Mails Gefahren für die IT-Ressourcen der Bank, insbesondere für das Netzwerk, ausgehen.

2.2.6 *Verlust, Störung etc.*

Ein Abhandenkommen oder die Beschädigung der überlassenen Hard- und Software ist dem UHD der Bank (User Help Desk – 069 9566-2323) unverzüglich anzuzeigen. Gleiches gilt für Auffälligkeiten (z. B. Verdacht auf Missbrauch von Kennwörtern) und bei vermuteten oder erkannten Sicherheitslücken. Die Arbeit am IT-Arbeitsplatz ist zu unterbrechen, bis von dieser Stelle weitere Anweisungen erfolgen.

2.3 Telekommunikationsanlagen bei der Deutschen Bundesbank

Die dienstlichen Telefon- und Telefaxanschlüsse dienen der Unterstützung und Erleichterung des internen und externen Fernsprechbetriebs bzw. Telefaxverkehrs bei der Erfüllung der dienstlichen Aufgaben.

Dies gilt sowohl für bankinterne Verbindungen als auch für Verbindungen in das deutsche Festnetz, bei denen der Bank keine zusätzlichen Kosten entstehen (Flatrate).

2.4 Tablets und Smartphones bei der Deutschen Bundesbank

2.4.1 Allgemeines

Bei iOS-Endgerätearten wird grundsätzlich zwischen zwei Bereichen unterschieden, welche technisch strikt getrennt sind und organisatorisch zum Teil unterschiedlich behandelt werden. Der sog. dienstliche Bereich umfasst alle verschlüsselten dienstlichen Anwendungen auf den iOS-Geräten. Diese Anwendungen sind nur nach vorheriger Autorisierung über den UEM Client nutzbar. Demgegenüber umfasst der sog. öffentliche Bereich des Endgerätes alle Anwendungen außerhalb der verschlüsselten dienstlichen Anwendungen auf den iOS-Geräten.

Die Inbesitznahme von mobilen Geräten der Bank ist schriftlich zu quittieren. Das Gerät darf – insbesondere beim Transport – nicht unbeaufsichtigt gelassen werden.

Für die Nutzung des dienstlichen Bereichs auf dem Endgerät gelten alle für den IT-Arbeitsplatz gültigen Nutzungsbedingungen.

2.4.2 Zugang

Bei der Einrichtung des Endgerätes wird eine der Nutzerin bzw. dem Nutzer persönlich zugewiesene Apple-ID verwendet. Diese Apple-ID ist für das Herunterladen von Anwendungen (Apps) sowie für die Aktualisierung (Update) der Apps und des Betriebssystems erforderlich. Das dazu gehörende Passwort ist vertraulich zu behandeln. Der Zentralbereich IT hat keinen Zugriff auf dieses Passwort und kann insoweit auch keinen Support (z. B. Passwortrücksetzung) leisten.

2.4.3 Umgang mit Daten

Bei der Benutzung mobiler Geräte ist seitens der externen Person sicherzustellen, dass eine Einsichtnahme in oder ein Zugriff auf vertrauliche Informationen bzw. Daten der Bank oder solchen vertraulichen Informationen bzw. Daten, für die die Bank verantwortlich ist oder die sie betreffen, durch Unbefugte ausgeschlossen ist.

Aus Datenschutzgründen ist ein sorgsamer Umgang mit personenbezogenen Daten bei der Internet-Nutzung als auch im externen E-Mail-Verkehr notwendig. Da Internetzugriffe nicht über die Sicherheitsinfrastruktur der Bank erfolgen, besteht das Erfordernis eines sorgsamen und gewissenhaften Handelns beim Arbeiten im Internet in besonderem Maße.

Bei diesen Geräten ist das Betriebssystemupdate durch die Nutzerinnen und Nutzer unverzüglich nach ihrer Bereitstellung durchzuführen, sofern keine anderweitigen Weisungen des Zentralbereichs IT vorliegen. Ferner ist sicherzustellen, dass die Geräte stets über einen aktivierten geschäftlichen Bereich verfügen.

Die Nutzerin bzw. der Nutzer eines Endgerätes ist dafür verantwortlich, dass durch dessen Einsatz kein Datenverlust für die Bundesbank eintritt. Daher gilt insbesondere:

- Das Endgerät darf nie unbeaufsichtigt sein bzw. ist gegen Diebstahl zu schützen.
- Zur Sicherung gegen unbefugte Benutzung ist die Codesperre zu aktivieren, wenn das Endgerät nicht genutzt wird.
- Die persönlichen Zugangskennungen (Passwörter) sind geheim zu halten.
- Es ist darauf zu achten, dass Dritte die auf dem Bildschirm angezeigten Daten (v. a. Passwörter) nicht mitlesen können.

- Daten und Anwendungen - auch im öffentlichen Bereich - dürfen nur aus vertrauenswürdigen Quellen heruntergeladen werden.

Die Verarbeitung und Speicherung von dienstlichen Daten ist ausschließlich im gesicherten Bereich des Endgerätes gestattet. Eine Übergabe an Anwendungen außerhalb des dienstlichen Bereichs ist verboten und wird systemseitig verhindert. Der öffentliche Bereich unterliegt nicht automatisch einer Datensicherung. Die dort gespeicherten Daten können bei einer Störung des Endgerätes ggf. verloren gehen.

Der Download von Software (z. B. Apps) ist im Rahmen der durch den Zentralbereich IT getroffenen Regelungen ebenfalls gestattet; die Nutzerinnen und Nutzer haben dabei darauf zu achten, dass nur Software aus vertrauenswürdigen Quellen heruntergeladen wird, um das Risiko von Schadsoftware zu verringern.

2.4.4 Nutzung von Threema Work

Mit Threema Work bietet die Bundesbank die Möglichkeit, dienstliche Informationen über eine sichere Messenger-App auszutauschen. Die Threema Work App befindet sich dabei außerhalb des dienstlichen Bereichs.

Folgende Aspekte müssen bei der Verwendung der Threema Work App berücksichtigt werden:

- Für Threema Work darf nur eine ID angelegt werden.
- Threema Work darf nur auf einem Gerät genutzt werden.
- Die Code-Sperre ist zu aktivieren.
- Das Backup der Threema ID muss selbständig unter Nutzung von Threema Safe durchgeführt werden. In Threema Safe werden auch Einstellungen und Kontakte verschlüsselt gespeichert.
- Die Verwendung dienstlicher Daten in Threema Work ist gestattet, diese dürfen jedoch die Threema Work App nicht verlassen und in anderen Apps verarbeitet werden.

2.4.5 Verlust, Störung etc.

Auffälligkeiten beim Endgerät sind unverzüglich dem User Help Desk (UHD – 069 9566-2323) zu melden und das Endgerät - im Rahmen der IT-Sicherheitsvorfallsbearbeitung - den Lokalen IT-Services (LITS) auszuhändigen.

Ein Endgeräteverlust ist dem UHD unverzüglich zu melden.

2.4.6 Mobilität

Die Endgeräte sind für die mobile Nutzung mit einer SIM-Karte ausgestattet. Im Inland steht dabei eine Datenflatrate zur Verfügung, so dass unabhängig von der Nutzung für Datenverbindungen keine weiteren Kosten anfallen.

Innerhalb der Bundesbank können in einigen Besprechungsräumen sowie nahe gelegenen Büros WLAN-Hotspots der Bank genutzt werden. Bei der mobilen Datennutzung über Mobilfunk im Ausland können evtl. hohe Roamingkosten entstehen. Datenroaming ist daher zunächst deaktiviert und kann von der Nutzerin bzw. dem Nutzer für die - ausschließlich dienstliche - Nutzung im Ausland in den „Geräteeinstellungen“ aktiviert werden. Bluetooth ist ebenfalls zunächst deaktiviert und kann über die "Geräteeinstellungen" bei Bedarf aktiviert werden. Die Übertragung sicherheitsrelevanter Daten (z. B. Passwörter) über Bluetooth ist nicht erlaubt.

Bei Nichtgebrauch sind mobile Geräte sorgfältig aufzubewahren, um etwa Diebstähle zu vermeiden. Insbesondere sind Verschlussmöglichkeiten zu nutzen.

2.5 Nutzung des Internets über einen Internetzugang der Bundesbank

Die Nutzung des Internetzugangs ist ausschließlich zu Recherchezwecken und über die seitens der Bank zugelassenen Verbindungen gestattet. Bei der Nutzung der Infrastruktur der Bank bestehen Beschränkungen durch Contentfilterung und die Sperrung von nicht freigegebenen verschlüsselten Verbindungen. Diese werden von der externen Person akzeptiert.

2.6 Teilnahme am E-Mail-Verkehr über die Infrastruktur der Bundesbank

Die externe Person hat im E-Mail-Verkehr, welcher auf der Basis von Notes abgewickelt wird, deutlich zu machen, dass sie nicht für die Bank, sondern für ihr Unternehmen auftritt und für dieses handelt. Für den externen E-Mail-Verkehr stellt die Bundesbank entsprechende Funktionalitäten bereit, wobei mit anderen Nationalbanken eine separate Infrastruktur und mit beteiligten Behörden der Informationsverbund der Bundesverwaltungen (Netze des Bundes, NdB) genutzt wird.

Vertrauliche Informationen bzw. Daten der Bank oder solche vertraulichen Informationen bzw. Daten, für die die Bank verantwortlich ist oder die sie betreffen, dürfen nicht mittels externer E-Mail versandt werden. Sofern die Bank ausnahmsweise einer Übermittlung derartiger vertraulicher Inhalte per externer E-Mail zustimmt, sind dafür von der externen Person die von der Bank zur Verfügung gestellten Verschlüsselungslösungen in Anspruch zu nehmen. Innerhalb des Netzwerkes der Bank versandte E-Mails der externen Person mit vertraulichen Inhalten sind mit der von Notes angebotenen Verschlüsselungsfunktion zu verschlüsseln.

Eingehende Nachrichten mit Dateianhängen oder verschlüsselt eingehende Nachrichten sind nur von bekannten und als vertrauenswürdigen eingestuften Stellen zu öffnen. Im Zweifel ist der User-Help-Desk der Bank einzuschalten, dessen Weisungen zu befolgen sind.

Sofern die externe Person eigenverantwortlich über die Öffnung entscheidet, trägt sie damit allein das verbundene Risiko einer Schädigung von IT-Ressourcen der Bank.

2.7 Teilnahme an Chat, Video- und Webkonferenzen über die Infrastruktur der Bundesbank

Die Berechtigung und die Software für Chat, Video- und Webkonferenzen am Arbeitsplatz stehen jeder externen Person standortunabhängig zur Verfügung. Für die Kommunikation über die entsprechende Software ist die Anmeldung durch die jeweiligen Gesprächspartner erforderlich. Grundsätzlich ist die Nutzung freiwillig. Rein interne Videokonferenzen am Arbeitsplatz sind auch für vertrauliche Inhalte freigegeben; dies gilt nicht, sobald eine Person per WebRTC teilnimmt.

Bei der Nutzung von Videotelefonie bzw. Webkonferenzen müssen die dafür geltenden datenschutzrechtlichen Anforderungen und das Recht am eigenen Bild in besonderem Maße auch durch die teilnehmenden externen Personen beachtet werden. Auch sie haben dabei Sorge zu tragen, dass Persönlichkeitsrechte Dritter nicht verletzt werden und Dritte während der Videokommunikation nicht ungewollt von der Bild- und Tonübertragung erfasst werden.

Bei der Nutzung von Anwendungen für Chat, Audio- und Videotelefonie sowie Webkonferenzen sind alle Teilnehmenden vorab darüber zu informieren, falls weitere, bisher nicht angekündigte Personen ebenfalls teilnehmen sollen.

Bei der Nutzung von Anwendungen für Audio- oder Videotelefonie sowie Webkonferenzen ist auch von externen Personen darauf zu achten, dass nur die vorgesehenen Teilnehmenden die Übertragungen einsehen bzw. mithören können (Vermeidung des sogenannten Shoulder-Surfings) und der Schutz der Vertraulichkeit gewährleistet wird.

3 Änderungen der Nutzungsbedingungen

Änderungen der vorliegenden Nutzungsbedingungen werden durch ein Schreiben der Bundesbank bekannt gegeben. Die Übermittlung kann auch auf elektronischem Wege erfolgen. Sie gelten, soweit im Einzelfall nicht anderes bestimmt wird, vier Wochen nach Absendung der Mitteilung als vereinbart, wenn nicht die externe Person innerhalb dieses Zeitraums der Bundesbank gegenüber ihre Ablehnung angezeigt hat. Auf diese Genehmigungswirkung wird die Bundesbank in ihrer Mitteilung die externe Person besonders hinweisen.

4 Datenschutzhinweis

4.1 Zweck und Umfang der Datenverarbeitung

Die Deutsche Bundesbank (Wilhelm-Epstein-Straße 14, 60431 Frankfurt am Main, Tel.: 069/9566-0, E-Mail: info@bundesbank.de) wird im Falle einer Nutzung ihrer IT-Ressourcen auf Grundlage der nachfolgend in 4.2 benannten Rechtsgrundlagen die nachstehenden Protokollierungen und Auswertungen stichprobenartig oder anlassbezogen bei Verdachtsfällen vornehmen und die Ergebnisse zum Zweck der Systemoptimierung und –pflege sowie der Überprüfung der Einhaltung der im Kapitel 2 aufgeführten Nutzungsbedingungen verwerten:

- a) Abgehende Gespräche bzw. Telefaxverbindungen:
 - Name der Telefonanschlusshaberin bzw. des Telefonanschlusshabers oder der Betriebsstelle (z. B. „Besprechungsraum“),
 - Rufnummer der anrufenden Nebenstelle,
 - Datum des Gesprächs und Gesprächsbeginn (Uhrzeit),
 - Dauer des Gesprächs,
 - Zielrufnummer (einschließlich Ortsnetzkennzahl),
 - Tarifeinheiten bzw. Gesprächskosten.
- b) Ankommende Telefonate bzw. Telefaxverbindungen:
 - Rufnummer der bzw. des Anrufenden, sofern die Rufnummer nicht unterdrückt ist,
 - Rufnummer der angerufenen Nebenstelle,
 - Datum des Gesprächs und Gesprächsbeginn (Uhrzeit),
 - Dauer des Gesprächs sowie
 - Nur bei anlassbezogener Nutzung der restriktiv im Bereich der Handelsräume (Handelsgespräche (IPC-Handelssystem), Handelsgespräche "Pensionsfonds" in Hauptverwaltungen, Callcenter Hauskundengeschäft) sowie für Drohanrufe in der Vermittlung der Zentrale, der Sicherheitszentrale (SiZe C35) oder bei der Bundespolizei bereitgestellten Aufzeichnungsfunktion: der Inhalt des Gesprächs.

c) Nutzung der Internetrecherche-Infrastruktur:

- Datum und Uhrzeit aller Zugriffe,
- Benutzerkennung,
- Netzwerkadresse des benutzten PC,
- URL, enthält die abgerufene Adresse sowie die weiteren, an diese Adresse übertragenen Daten, wie z. B. den Namen der aufgerufenen Datei und den Anmeldenamen bei Anmeldung an externe E-Mail-Konten,
- URL Kategorie, enthält die Einstufung der URL in eine Kategorie entsprechend den Definitionen von bei der Deutschen Bundesbank eingesetzten URL-Filters,
- übertragene Datenmenge,
- sonstige technische Daten, z. B. Fehlercodes
- Übersicht über das jeweilige Gesamtvolumen des ein- / ausgehenden Datenverkehrs.

d) Nutzung der E-Mail-Fazilitäten:

- Datum und Uhrzeit des Empfangs oder Versands der Nachricht,
- Absender und Empfänger der Nachricht,
- Betreffzeile,
- Namen von Dateianhängen,
- übertragene Datenmenge,
- evtl. sonstige technische Daten (z. B. Fehlercodes).

e) Nutzung des Dokumentenmanagementsystems (DMS) FAVIS

- Auswertung personenbezogener Informationen der externen Person: Name, Vorname, Anmeldeame, Benutzeranmeldung, BenutzerID, ID des persönlichen Arbeitsbereichs, eingerichtete Vertreter, zugewiesene mittelbare Rechte (über Gruppen und Rollen) und unmittelbare Rechte (direkt dem User zugeordnet)
- Aktionen bei Verwendung einer regulären Anwenderkennung in Bezug auf Objekte (z. B. Akte, Vorgänge, Dokumente inkl. Metadaten): Art des Zugriffs (Lesen, Herunterladen, Drucken, Bearbeiten), Erstellung, Änderung, Ent-/Reservierung, Löschung, Statusänderung (Entwurf, Genehmigung, zu den Akten Verfügung)
- Aktionen bei Verwendung einer regulären Anwenderkennung in Bezug auf Aufgaben (Workflows, Wiedervorlagen): Informationen aus selbst erstellten Aufgaben (Aufgabempfeänger und deren Aufgaben, beigefügte Dokumente, Kommentierungen); aktive und überfällige eigene Aufgaben (Aufgabe, beigefügte Dokumente, Kommentierungen)
- Aktionen bei Verwendung einer Anwenderkennung mit administrativen Rechten: Zusätzlich Auswertung von Änderungen am Benutzer- und Berechtigungsgefüge von FAVIS (Änderungen von Benutzergruppen, Vergabe von Berechtigungen an Objekten, Änderung von Records-Management Einstellungen, Einrichten/Löschen von Benutzern, direkte Zuweisung von Benutzerrechten) sowie die Erstellung und Ausführung von Auswertungen
- Personenbezogene Daten, die sich aus dem Inhalt der im DMS gespeicherten Dokumente ergeben
- Auswertungen weisen neben der Benutzer-ID und der ID des betroffenen Objekts zusätzlich Datum und Zeitpunkt der jeweiligen Aktion aus. Bei administrativen Eingriffen

kann in einigen Fällen auch die Veränderung selbst ausgewertet werden (alter Wert, neuer Wert)

- Auswertungen beinhalten auch alle Aktionen und Aufgaben die im Rahmen einer Vertretung wahrgenommen wurden
- Eine personenbezogene Auswertung der Tätigkeiten von Nutzern mit administrativen Rechten erfolgt regelmäßig und ohne Anlass. Administrative Tätigkeiten erfolgen stets mit einer gesonderten Benutzerkennung.

f) Nutzung des Intranets (nur sofern der Unterzeichner entsprechend freigeschaltet wurde)

- Datum und Uhrzeit aller Zugriffe,
- Benutzerkennung,
- Netzwerkadresse des benutzten PC,
- URL, enthält die abgerufene Adresse sowie die weiteren, an diese Adresse übertragenen Daten, wie z. B. den Namen der aufgerufenen Datei,
- übertragene Datenmenge,
- sonstige technische Daten, z. B. Fehlercodes
- Übersicht über das jeweilige Gesamtvolumen des ein- / ausgehenden Datenverkehrs.

g) Nutzung von Anwendungen für Chat, Audio- und Videotelefonie sowie Webkonferenzen:

- Datum und Uhrzeit aller Zugriffe,
- Benutzerkennung,
- Netzwerkadresse des benutzten PC,
- Netzwerkadresse der Gesprächspartnerin bzw. des Gesprächspartners,
- sonstige technische Daten, z. B. Fehlercodes,
- nur, sofern alle teilnehmenden Personen vor der Aufzeichnung informiert werden und einverstanden sind: Chatinhalte; eine Aufzeichnung und Protokollierung von Gesprächsinhalten erfolgt nicht.

h) Darüber hinaus speichert die Deutsche Bundesbank im IT-Arbeitsplatz und in den über den IT-Arbeitsplatz erreichbaren IT-Systemen personenbezogene Daten (z. B. UserID, Aktionen) und wertet diese im Rahmen der Wahrnehmung ihrer Aufgaben aus.

4.2 Rechtsgrundlagen der Datenverarbeitung

Die Verarbeitung der personenbezogenen Daten externer Personen erfolgt auf Grundlage der Bestimmungen von Artikel 6 Abs. 1 Buchst. e) DSGVO in Verbindung mit § 3 BDSG, d.h. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die der Deutschen Bundesbank übertragen wurde.

Soweit die externe Person in einer eigenständigen Vertragsbeziehung zur Deutschen Bundesbank steht, erfolgt die Verarbeitung Ihrer personenbezogenen Daten zudem auf der Grundlage der Bestimmungen von Artikel 6 Abs. 1 Buchst. b) DSGVO und ist zur Erfüllung des mit der Deutschen Bundesbank abgeschlossenen Vertrages erforderlich.

4.3 Aufbewahrungs- und Löschfristen

Die Daten aus 4.1 a) und b) werden spätestens nach 6 Monaten, jene nach 4.1. c und f) nach 2 Wochen und nach 4.1 d) nach 30 Tagen² gelöscht, sofern nicht im Einzelfall ein wichtiger Grund für eine längere Speicherung zum Zwecke der Verwendung (z. B. für Beweis Zwecke) vorliegt. Daten aus 4.1 c) und d) werden ohne Benutzerkennung in anonymisierter Form zu Zwecken der Gewährleistung der IT-Sicherheit ein Jahr gespeichert. DMS-Daten aus 4.1 e) werden nach Vorgaben des Fachbereichs, des Historischen Archivs, gesetzlicher Vorgaben und Richtlinien (z. B. Bundesarchivgesetz, Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien) aufbewahrt. Die Protokolldaten nach 4.1 g) werden im Rahmen der jeweils geltenden gesetzlichen Bestimmungen gespeichert und anschließend gelöscht.

4.4 Betroffenenrechte

Externe Personen haben gegenüber der Deutschen Bundesbank die folgenden Rechte hinsichtlich der sie betreffenden personenbezogenen Daten:

- Recht auf Auskunft (Art. 15 DSGVO),
- Recht auf Berichtigung (Art. 16 DSGVO),
- Recht auf Löschung (Art. 17 DSGVO),
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO),
- Recht auf Widerspruch gegen die Verarbeitung (Art. 21 DSGVO) und
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO).

Sie haben zudem nach Art. 77 DSGVO das Recht, sich bei der zuständigen Datenschutzaufsichtsbehörde über die Verarbeitung Ihrer personenbezogenen Daten zu beschweren. Die für die Deutsche Bundesbank zuständige Aufsichtsbehörde ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Graurheindorferstraße 153, 53117 Bonn, Tel.: 0228/ 997799-0, E-Mail: poststelle@bfdi.bunde.de).

4.5 Datenschutzbeauftragte

Die Datenschutzbeauftragte der Deutschen Bundesbank ist unter der E-Mail-Adresse datenschutz@bundesbank.de, telefonisch unter der Rufnummer 069/9566-2369 und postalisch unter der Anschrift Deutsche Bundesbank, Datenschutzbeauftragte, Postfach 10 06 02, 60006 Frankfurt am Main, zu erreichen.

² Protokollierungen des externen E-Mail-Verkehrs werden 30 Tage lang gespeichert, es dürfen aber nur die Protokollierungen von maximal den letzten zwei Wochen ausgewertet werden.