

Bedingungen für eine mögliche Nutzung bestimmter IT-Ressourcen der Deutschen Bundesbank über das Access-Portal für Partner

1 Einleitung

Im Rahmen von Vertrags- bzw. Kooperationsverhältnissen ermöglicht die Deutsche Bundesbank externen, nicht zum Kreis ihrer Beschäftigten gehörenden Personen, ihre elektronischen Informations- und Kommunikationssysteme von außen über das Access-Portal für Partner zu nutzen. Die Bundesbank erlaubt diesen Personen aufgrund ihrer Eigenschaft als Beschäftigte eines externen Partners oder Beschäftigte einer anderen Zentralbank (nachfolgend zusammenfassend als „externe Personen“ bezeichnet) ihre elektronischen Informations- und Kommunikationssysteme zu nutzen. Die hierunter fallenden elektronischen Informations- und Kommunikationssysteme sind IT-Arbeitsplätze, die ausschließlich über das Access-Portal für Partner¹ bereitgestellt werden sowie dazugehörige Systeme wie die Nutzung von E-Mail oder Dokumentenmanagementsysteme (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 Bundesbank über das Access-Portal für Partner 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 Mitarbeiter/Mitarbeiterinnen des Partners unzulässig, die geeignet ist, den Interessen der 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 gilt es 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

¹ Für die Nutzung von IT-Ressourcen innerhalb der Bundesbank Infrastruktur (z. B. Desktop-PC oder mobiler PC-Arbeitsplatz sowie Telekommunikations- oder Dokumentenmanagementsysteme) müssen die „Bedingungen für eine mögliche Nutzung bestimmter IT-Ressourcen der Bundesbank für externe Personen“ berücksichtigt (Vordruck-Nr. 11059-1) und eine andere Version der Einwilligungs- und Verpflichtungserklärung unterschrieben werden (Vordruck-Nr. 11059-2).

auf Seiten mit Hacker-Instrumenten, Malware und anderen zu Angriffen auf die System- und Netzsicherheit der Bundesbank geeigneten Softwareinstrumenten.

2.2 Zugriff auf Access-Portal

2.2.1 Zugang mit User-ID, Kennwort, RSA-Token und PIN

Der Zugang zum Access-Portal für Partner ist generell über 2-Faktor-Authentifizierung (Besitz eines RSA-Token und Wissen einer PIN) geschützt. Für die Anmeldung am Access-Portal für Partner wird ein RSA-Token von der Bundesbank ausgeliefert. Hierfür muss die externe Person eine PIN initialisieren.

Zur Identifizierung ist zusätzlich eine Benutzerkennung (Identifikationsmerkmal, hier User-ID) und ein Kennwort (Authentifikationsmerkmal) notwendig. Die externe Person erhält damit die folgenden Zugriffsberechtigungen:

- Zugang zum Access-Portal für Partner
- Zugriff auf Netz-Laufwerke, Datenbanken, Applikationen (abhängig von den Berechtigungen)

Authentifizierungsdaten bzw. RSA-Token dürfen nicht an Dritte weitergegeben werden.

Für den erstmaligen Zugang zum Access-Portal für Partner stellt die Bundesbank der externen Person ferner ein vertrauliches Startkennwort (Authentifikationsmerkmal) zur Verfügung. Bei der erstmaligen Anmeldung muss das Startkennwort durch ein neues persönliches Kennwort ersetzt werden, das anderen Personen nicht bekannt oder zugänglich gemacht werden darf. Für die Zurücksetzung des Kennwortes für die Benutzerkennung ist ein Self-Service implementiert.

Das Kennwort läuft regelmäßig ab und muss rechtzeitig geändert werden.

Soweit beim Verlassen des Arbeitsplatzes keine Abmeldung vom System erfolgt, ist das IT-Arbeitsplatzsystem in geeigneter Weise vor unbefugtem Zugriff auf Daten und Anwendungen zu sperren. Spätestens, wenn die Arbeit für den laufenden Tag beendet wird, ist die Verbindung zum Access-Portal für Partner ordnungsgemäß zu beenden.

2.2.2 Zugang zu speziellen Anwendungen

Bei der erstmaligen Anmeldung an bestimmten Anwendungen ist ein ggf. vorhandenes Startkennwort verfahrensgemäß durch ein persönliches Kennwort zu ersetzen. Für den Aufbau von Kennwörtern gelten spezielle Sicherheitsrichtlinien, die produktbezogen in den entsprechenden Benutzeranleitungen dokumentiert sind.

2.2.3 Voraussetzungen für die Nutzung

Die elektronischen Zugriffsberechtigungen einer externen Person werden erst eingerichtet, wenn eine unterschriebene Einwilligungs- und Verpflichtungserklärung der externen Person vorliegt.

2.3 Eingesetzte Software

Der technische Zugang für Partner wird von der Bundesbank über die universelle Plattform Access-Portal bereitgestellt. Die Anwendungen werden je nach Zugriffsberechtigung im Access-Portal angezeigt. Sie können gleichzeitig mit anderen Nutzern aufgerufen werden. Es wird lediglich die Anzeige der Anwendung als Datenstrom nach außen transportiert.

Eigenmächtiges Installieren von Software sowie die Nutzung von nicht freigegebener/privater Software (auch sog. portable Versionen) über das Access-Portal für Partner ist untersagt.

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

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

2.4 Umgang mit Daten

Es ist nicht gestattet, Kopien von Datenbeständen der Bundesbank anzufertigen, soweit dies nicht ausdrücklich zwischen der Bundesbank und dem Partner vereinbart wurde.

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

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

Zum Zeitpunkt der Beendigung des Überlassungszeitraums muss die externe Person eventuell von ihr gespeicherte Daten sowie gesendete oder empfangene E-Mails löschen, soweit sie nicht vertragsgemäß der Bundesbank zustehen. Unterlässt sie dies, ist die Bundesbank ohne weiteres zur Löschung berechtigt. Das gleiche gilt, wenn von den Dateien oder E-Mails Gefahren für die IT-Ressourcen der Bundesbank, insbesondere für das Netzwerk, ausgehen.

2.5 Verlust, Störung etc.

Ein Abhandenkommen oder die Beschädigung der überlassenen Hard- und Software ist dem UHD der Bundesbank (User Help Desk – Kurzwahl 32323) unverzüglich anzuzeigen. Gleiches gilt für Auffälligkeiten (z. B. Verdacht auf Missbrauch von Kennworten) und bei vermuteten oder erkannten Sicherheitslücken. Die Arbeit am IT-Arbeitsplatz ist zu unterbrechen, bis von dieser Stelle weitere Anweisungen erfolgen.

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

Die externe Person hat im E-Mail-Verkehr, welcher unter Nutzung des Access-Portal für Partner abgewickelt wird, deutlich zu machen, dass sie nicht für die Bundesbank, sondern für ihr Unternehmen auftritt und für dieses handelt.

Eingehende Nachrichten mit Dateianhängen oder verschlüsselt eingehende Nachrichten sind nur zu öffnen, wenn sie von bekannten und als vertrauenswürdigen eingestuften Stellen eingehen. Im Zweifel ist der User-Help-Desk der Bundesbank 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 Bundesbank.