COMMERZBANK

Verpflichtungserklärung auf den Datenschutz und die Informationssicherheit für Fremdpersonal

Name/Adresse:

Personalnummer ----------

Anwendungsbereich

Die vorliegende Verpflichtungserklärung gilt grundsätzlich[1] für Fremdpersonal, das entweder direkt oder über einen Dienstleister für die Bank tätig ist und dabei Kenntnis von personenbezogenen Daten, Kundendaten oder Betriebs- und Geschäftsgeheimnisse nehmen kann.[2]

Persönliche Angaben des/der Verpflichteten

Zuname (sowie Geburtsname):

Vorname:

Beschäftigt bei Firma: Schule:

Eingesetzt in Projekt/Team: Commerzbank AG, Kaiserstr. 31, 51643 Gummersbach

Hiermit verpflichte ich mich, personenbezogene Daten (z. B. Kundendaten, Mitarbeiterdaten), zu denen ich im Rahmen meiner Tätigkeit Zugang erhalte oder Kenntnis erlange, vertraulich zu behandeln und nur nach den Anweisungen der Bank zu verarbeiten (Datengeheimnis auf der Grundlage von Artikel 5 Absatz 1 f, Artikel 28 Absatz 3 b und Artikel 29 sowie Sicherheit der Verarbeitung gemäß Artikel 32 Absatz 4 EU-Datenschutzgrundverordnung, kurz DSGVO). Dazu bin ich auf folgende gesetzliche Bestimmungen des Datenschutzrechts hingewiesen worden:

Es ist untersagt, durch die DSGVO geschützte personenbezogene Daten unbefugt zu verarbeiten.

Vom Begriff der Verarbeitung sind erfasst das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen und die Verwendung personenbezogener Daten. Des Weiteren sind erfasst die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung personenbezogener Daten.

Diese Verpflichtung zur Wahrung des Datengeheimnisses besteht auch nach Beendigung der Tätigkeit bei der Verarbeitung personenbezogener Daten bzw. dem Ende des Arbeitsverhältnisses fort.

Zudem verpflichte ich mich, Betriebs- und Geschäftsgeheimnisse zu schützen, das Bankgeheimnis zu wahren und die internen Richtlinien und Anweisungen der Bank zum Datenschutz und zur Sicherheit der Datenverarbeitung einzuhalten. Hierzu gehört insbesondere die Einhaltung der Vorgaben zur **Informationssicherheit am Arbeitsplatz**. Eine Einsichtnahme wird durch den internen beauftragenden Bereich ermöglicht.

Die auf den Folgeseiten aufgeführten Hinweise zu den gesetzlichen Bestimmungen zum Datenschutz, zur Informationssicherheit und Compliance habe ich zur Kenntnis genommen.

Die ausgefüllte Verpflichtungserklärung ist durch den Verantwortlichen des internen beauftragenden Bereiches für 10 Jahre nach Löschung der Benutzeridentifikation aufzubewahren.

Unterschriften:

Ort, Datum

Unterschrift des/der Verpflichteten

Unterschrift des Arbeitgebers

[1] Prüfer, die im Auftrag von Aufsichtsbehörden tätig sind, müssen diese Verpflichtungserklärung nicht unterschreiben. Im Antrag für die Vergabe einer Personalnummer (Formular 833/08/20) ist durch die beantragende interne Stelle zu vermerken, dass es sich um einen behördlichen Prüfer handelt. Nach Gegenzeichnung durch den internen Antragsteller wird das Formular dort abgelegt.

[2] In Ausnahmefällen kann die Verpflichtungserklärung durch einen autorisierten Vertreter des Dienstleisters für dessen Mitarbeiter einmalig unterschrieben werden. Hierzu ist eine schriftliche Vereinbarung mit GS-OS Datenschutz erforderlich. Der Dienstleister hat intern sicherzustellen, dass dessen Mitarbeiter in gleicher Weise verpflichtet werden.

9230/51/00 – HD1124-01

Verpflichtungserklärung auf den Datenschutz und die Informationssicherheit für Fremdpersonal

Merkblatt zum Datenschutz für Mitarbeiter der Bank

Für die Verarbeitung von Daten natürlicher Personen (personenbezogene Daten) ist seit dem 25. Mai 2018 die „Verordnung Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten“ (EU-Datenschutzgrundverordnung, kurz DSGVO) maßgeblich. Vom Datenschutzrecht nicht geschützt sind Daten juristischer Personen (z. B. von Kapitalgesellschaften), es sei denn, die Daten beziehen sich auf eine einzelne natürliche Person (z. B. Gesellschafter, Vorstandsmitglieder oder Geschäftsführer).

Die personenbezogenen Daten dürfen nur in dem von den einzelnen Bestimmungen der DSGVO geregelten Rahmen verarbeitet, d. h. insbesondere erhoben, erfasst, organisiert, geordnet, gespeichert, angepasst, verändert, ausgelesen, abgefragt, verwendet, durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung offengelegt sowie abgeglichen, verknüpft, eingeschränkt, gelöscht oder vernichtet werden.

So ist z. B. eine Datenerhebung, -speicherung oder -verwendung erlaubt, wenn und soweit die betroffene Person ihre Einwilligung erteilt hat oder soweit dies zur Erfüllung eines Vertrages mit der betroffenen Person oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist. Geschieht die Datenverarbeitung nicht mit Einwilligung der betroffenen Person oder im Rahmen eines Vertrages oder vorvertraglicher Maßnahmen, so ist regelmäßig zu prüfen, ob diese Datenverarbeitung zur Wahrung berechtigter Interessen der Bank oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Darüber hinaus ist die Verarbeitung personenbezogener Daten auch dann zulässig, sofern eine anwendbare Rechtsvorschrift dies vorschreibt oder erlaubt.

Ferner schreibt die DSGVO vor, dass personenbezogene Daten durch technische und organisatorische Maßnahmen gesichert werden.

Werden personenbezogene Daten (z. B. Kundendaten, Mitarbeiterdaten) im Auftrag und nach Anweisung der Bank unter Nutzung eines von der Bank bereit gestellten Fernzuganges (VPN-Token) durch Fremdpersonal verarbeitet (Auftragsverarbeitung gemäß Artikel 28 DSGVO), so wird dieses in seinem Verantwortungsbereich die folgenden Punkte einhalten:

- Es wird zugesagt, dass geeignete, dem Risiko angemessene technische und organisatorische Schutzmaßnahmen in den verwendeten Räumen, auf den benutzten Informationstechnologien und im Umgang mit dem überlassenen VPN-Token so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet.
- Zur Erfüllung des erteilten Auftrages werden keine weiteren Dienstleister ohne die schriftliche Genehmigung der Bank in Anspruch genommen. Nicht der Genehmigung unterliegen Dienstleistungen, die Nebenleistungen zur Unterstützung der Auftragsdurchführung darstellen, wie z. B. Telekommunikationsleistungen.
- Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, Kategorien betroffener Personen sowie Pflichten und Rechte der Bank werden dem Vertrag, in dem die Tätigkeit vereinbart wurde, sowie den Anweisungen der Bank entnommen.
- Personenbezogene Daten der Bank werden nur auf aufgrund der dokumentierten Anweisungen der Bank verarbeitet, sofern nicht eine darüber hinaus gehende anwendbare rechtliche Pflicht besteht; der Bank wird diese rechtliche Pflicht vor der Verarbeitung mitgeteilt. Insbesondere werden personenbezogene Daten nicht unbefugt verwendet oder an Dritte übermittelt.
- Die Bank wird informiert, falls die Auffassung besteht, dass eine Anweisung der Bank gegen die DSGVO oder eine andere Datenschutzbestimmung verstößt.
- Sofern eine betroffene Person gegenüber der Bank ihre Datenschutz-Rechte geltend macht, wird die Bank im Rahmen der Möglichkeiten dabei unterstützt, ihrer Pflicht zur Beantwortung gegenüber der betroffenen Person nachzukommen.
- Unter Berücksichtigung der Art der Verarbeitung und den zur Verfügung stehenden Informationen, wird die Bank im Rahmen der Möglichkeiten bei der Einhaltung folgender Pflichten unterstützt:
  - Treffen geeigneter, dem Risiko angemessener technischer und organisatorischer Schutzmaßnahmen,
  - Meldung einer Datenschutz-Verletzung an datenschutzbeauftragter@commerzbank.com sowie Bereitstellung von Informationen, damit ggf. eine Benachrichtigung betroffener Personen möglich wird,
  - Bereitstellung von Informationen, damit ggf. eine Datenschutz-Folgenabschätzung möglich wird.
- Sollte eine lokale Kopie der personenbezogenen Daten erstellt worden sein, so wird diese nach Abschluss der Verarbeitungsleistungen - nach Wahl der Bank - entweder gelöscht oder zurückgegeben.
- Nach Aufforderung werden der Bank erforderliche Informationen zum Nachweis und Überprüfung der Einhaltung der oben genannten Punkte zur Verfügung gestellt.

Die internen Richtlinien und Anweisungen der Bank zum Datenschutz und Sicherheit der Datenverarbeitung sind einzuhalten.

Die gesetzlichen Datenschutzvorschriften verbieten jeden Missbrauch von personenbezogenen Daten. Diejenigen Personen, die personenbezogene Daten in unzulässiger Weise Dritten offenbaren oder unbefugt personenbezogene Daten verarbeiten oder erschleichen, können nach den anzuwendenden Strafvorschriften mit einer Geldstrafe oder auch mit Gefängnis bestraft werden. Datenschutzverstöße können auch zu hohen Bußgeldern für die Bank führen.

Es liegt in Ihrem eigenen als auch in unserem Interesse, dass Mängel in Angelegenheiten des Datenschutzes schnellstmöglich abgestellt werden. Sie sind verpflichtet, festgestellte Mängel möglichst umgehend entweder dem zuständigen Vorgesetzten, der Revisionsabteilung oder dem zuständigen Ansprechpartner für den Datenschutz mitzuteilen.

Durch die Datenschutzbestimmungen und insbesondere das Datengeheimnis wird nicht die allgemeine Verschwiegenheitspflicht berührt, die sich allgemein auf Betriebs- und Geschäftsgeheimnisse sowie das Bankgeheimnis und die Informationssicherheit begründet. Diese Verpflichtung gilt vielmehr neben der Pflicht zur Wahrung des Datengeheimnisses weiter.

9230/51/00 – HD1124-01

Verpflichtungserklärung auf den Datenschutz und die Informationssicherheit für Fremdpersonal

Hinweise zur Informationssicherheit

Alle bei der Ausübung der Tätigkeit zugänglich gewordenen Daten und Informationen der Bank sind entsprechend ihrer Klassifikation zu behandeln.

Der Zugriff auf und die Verwendung von Daten und Informationen sowie die Nutzung von Informationstechnologien der Bank ist nur insoweit gestattet, wie dies für die Erfüllung der vertraglichen Leistungen und übertragenen Aufgaben erforderlich ist.

Daten, Informationen und Informationstechnologien dürfen nicht an unbefugte dritte Personen weitergegeben oder diesen zur Kenntnis gebracht werden. Sie sind nach den Anweisungen der verantwortlichen Bankmitarbeiter zu benutzen.

Seitens der Bank bereitgestellte Arbeitsmittel dürfen nur im Rahmen und zu Zwecken der vertraglichen Leistungen und übertragenen Aufgaben verwendet werden. Dies gilt insbesondere für Arbeitsplatzrechner, E-Mail-Konten, Internetzugänge und Kleincomputer (z. B. Smartphone).

Die Schaffung oder Nutzung nicht zugewiesener Netzzugänge ist untersagt.

Die von der Bank bereit gestellten Fernzugänge (VPN-Token) für die Arbeit von zu Hause oder von unterwegs, dürfen mit geschützten privaten Rechnern in gesicherter Umgebung, d.h. abgeschirmt vor unberechtigten Dritten, genutzt werden.

Daten und Informationen dürfen nicht auf mitgebrachten Geräten oder Datenträgern (insbesondere auf privater Hardware oder Hardware des Dienstleisters) gespeichert oder in sonstiger Form vervielfältigt oder verwendet werden.

Daten, Informationen, Informationstechnologien, Kopien oder Auswertungen, dürfen nicht an Orte außerhalb der Datenverarbeitungssysteme der Bank geleitet oder an Orte außerhalb der Geschäftsräume der Bank verbracht werden. Geräte, Datenträger, Kopien oder Auswertungen sind in den Geschäftsräumen der Bank zu belassen soweit auf ihnen Daten oder Informationen der Bank gespeichert sind.

Nach Beendigung der jeweiligen Tätigkeit sind die von der Bank erhaltenen Daten und Informationen nicht rekonstruierbar zu löschen bzw. Datenträger zu vernichten oder der Bank unaufgefordert herauszugeben, soweit nicht eine gesetzliche Verpflichtung besteht, diese über die Vertragslaufzeit hinaus aufzubewahren.

Hinweise zu Compliance

Auf Aufforderung erfolgt eine Teilnahme an den Compliance-Pflichtschulungen der Bank. Bei der Verweigerung der Teilnahme kann die Bank einen Austausch des jeweiligen Mitarbeiters auf Kosten des Dienstleisters verlangen.

Folgen bei Zuwiderhandlungen

Sollte die Bank von Zuwiderhandlungen gegen diese Verpflichtungserklärung oder einer gesetzes- oder vertragswidrigen Nutzung von Daten, Informationen oder der Informationstechnologien der Bank Kenntnis erlangen, kann dies die aufgeführten Folgen nach sich ziehen:

- Sofortige vollumfängliche oder teilweise Entziehung der Zugangs- bzw. Zugriffsberechtigungen für Einrichtungen, Anwendungssysteme, IT-Infrastruktur, Daten und Informationen,
- Vertragskündigung,
- Nachforschungen, die Bußgelder oder Strafverfolgung gemäß den einschlägigen Bestimmungen zur Folge haben können,
- Geltendmachung von Schadensersatzansprüchen.

Mit einer Geld- oder Haftstrafe bestraft werden kann,

- wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,
  - einem Dritten übermittelt oder
  - auf andere Art und Weise zugänglich macht

  und hierbei gewerbsmäßig handelt, oder
- wer personenbezogene Daten, die nicht allgemein zugänglich sind,
  - ohne hierzu berechtigt zu sein, verarbeitet oder
  - durch unrichtige Angaben erschleicht

  und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

Version 2.1 DE

9230/51/00 – HD1124-01