Betriebsvereinbarung Datenschutz und Sicherheit

Zwischen

der Hauptgeschäftsführung des Bundesverbands Öffentlicher Banken Deutschlands e.V. (VÖB), Berlin
(nachfolgend „VÖB“ oder „Arbeitgeber“ genannt)

und dem

Betriebsrat des Bundesverbandes Öffentlicher Banken Deutschlands e.V. (VÖB), Berlin
(nachfolgend Betriebsrat genannt)

wird die folgende Betriebsvereinbarung abgeschlossen:

Präambel

Die Betriebsparteien sind sich einig, dass das Recht auf informationelle Selbstbestimmung einen überragenden Stellenwert hat. Gerade im Verhältnis zwischen Arbeitgeber und Arbeitnehmer müssen personenbezogene Daten der Beschäftigten besonders geschützt werden, um ein Gleichgewicht zwischen den Parteien des Arbeitsverhältnisses herzustellen. Dazu dient diese Betriebsvereinbarung.

In 2016 ist die EU-Datenschutzgrundverordnung (DSGVO) in Kraft getreten, sie muss ab 25. Mai 2018 angewendet werden. Daher wurde auch das Bundesdatenschutzgesetz (BDSG) novelliert.

Die vorliegende Betriebsvereinbarung soll als eine im § 26 Absatz 1 BDSG beschriebene Kollektivvereinbarung wirken und damit auch eine Rechtsvorschrift mit Erlaubnischarakter i.S.d. der Artikel 5 und 6 DSGVO sein. Die Betriebsparteien sind sich darüber einig, dass durch diese Betriebsvereinbarung der Schutz der Beschäftigtendaten nicht gemindert, sondern im Gegenteil verbessert werden soll. Vor diesem Hintergrund verständigen sich die Betriebsparteien auf folgende Vereinbarung:

A Allgemeiner Teil

§ 1 Geltungsbereich

Diese Betriebsvereinbarung gilt für die Verarbeitung sämtlicher personenbezogener Daten der Beschäftigten, die bei der Begründung, Durchführung, Beendigung des Beschäftigungsverhältnisses und der Beachtung der nachvertraglichen Pflichten anfallen.

B Lenkungsausschuss

§ 2 Errichtung und Tätigkeit eines Lenkungsausschusses „Datenschutz“

(1) Die Betriebsparteien richten einen regelmäßig tagenden Lenkungsausschuss „Datenschutz“ (fortan Lenkungsausschuss) ein. Er ist insbesondere für eine Risikobewertung hinsichtlich der Einhaltung des Beschäftigtendatenschutzes und für eine regelmäßige Berichterstattung verantwortlich.

(2) Beide Betriebsparteien entsenden jeweils einen Bevollmächtigten in den Lenkungsausschuss, wobei die Benennung weder an Form noch Frist gebunden ist. Ferner gehört der betriebliche Datenschutzbeauftragte dem Lenkungsausschuss an.

(3) Der Lenkungsausschuss wird lediglich tätig, soweit ihm diese Betriebsvereinbarung dieses Recht zuschreibt. Für seine Entscheidungsfindung gelten folgende Verfahrensregeln:

   a. Der Lenkungsausschuss ist nur beschlussfähig, wenn alle Ausschussangehörigen oder bevollmächtigten Vertreter anwesend sind.

   b. Alle Entscheidungen bedürfen der Einstimmigkeit, wobei der betriebliche Datenschutzbeauftragte kein Stimmrecht hat.

   c. Dem Lenkungsausschuss steht der betriebliche Datenschutzbeauftragte vor (Ausschussvorsitzende).

   d. Der Ausschussvorsitzende lädt zu den Ausschusssitzungen in Schrift- und/oder Textform, mit einer Ladungsfrist von mindestens drei Werktagen. Bei Einstimmigkeit kann von diesen Form- und Fristvorschriften abgewichen werden.

   e. Die Sitzungen werden durch den Ausschussvorsitzenden geleitet.

(4) Weitere Verfahrensvorschriften gibt es nicht. Gleichwohl besteht die Möglichkeit, dass sich der Lenkungsausschuss eine Geschäftsordnung gibt, die aber nicht von den o.g. Verfahrensregeln abweichen, sondern diese nur ergänzen darf.

(5) Der Lenkungsausschuss darf Konkretisierungen beschließen, sofern ihm dieses Recht in dieser Betriebsvereinbarung zugebilligt wird, die Betriebsvereinbarung dadurch nicht verändert wird und die Rechte des Betriebsrates gewahrt bleiben.

§ 3 Rechteerhalt der Betriebsparteien

Die Rechte der Betriebsparteien, insbesondere die des Betriebsverfassungsgesetzes, bleiben von der Errichtung und Tätigkeit des Lenkungsausschusses unberührt.

C Aufbewahrung von Daten

§ 4 Allgemeine Aufbewahrungsbefugnis

(1) Der VÖB kann sämtliche Beschäftigtendaten i.S.v. § 1 dieser Betriebsvereinbarung für den Zeitraum von zehn Jahren speichern. Diese Frist beginnt jeweils am 31. Dezember des Jahres, in dem das Beschäftigungsverhältnis endet.

(2) Gesetzliche Aufbewahrungspflichten, die eine längere als den in Absatz 1 genannten Aufbewahrungszeitraum vorschreiben, bleiben unberührt.

§ 5 Einschränkungen zur allgemeinen Aufbewahrungsbefugnis

(1) Abweichend von § 4 müssen die Daten anlassbezogen vor Ablauf der dort genannten Frist gelöscht werden, wenn der betroffene Beschäftigte dies verlangt und der Löschung keine Rechtsvorschriften bzw. ein nachweisbares berechtigtes Interesse des Arbeitgebers entgegenstehen.

(2) Unabhängig davon, ob der Betroffene dies verlangt oder nicht, darf der Arbeitgeber die Daten i.S.v. § 1 dieser Betriebsvereinbarung nur verwenden, solange die jeweils gesetzliche Aufbewahrungspflicht eine Speicherungspflicht vorsieht.

D Nutzung betrieblicher Mittel und mobiles Arbeiten

§ 6 Nutzung betrieblicher Geräte, Rechte des Arbeitgebers

(1) Betriebliche Geräte dürfen zur Erfüllung arbeitsvertraglich geschuldeter Leistungen und kurzzeitig zu privaten Zwecken genutzt werden, sofern dadurch die Betriebsabläufe nicht erheblich gestört werden.

(2) Der Arbeitgeber darf auf seine betrieblichen Geräte zugreifen und Daten auf jedwede Form auslesen, auch wenn diese der privaten Nutzung eines Beschäftigten zuzuord-

nen sind (Privatdaten). Der Betriebsrat ist über das Auffinden von Privatdaten zu informieren.

(3) Der Arbeitgeber darf diese Privatdaten nicht gezielt suchen und auch nicht verwenden. Abweichend von Satz 1 dürfen sie gesucht und verwendet werden, wenn dies der Aufdeckung einer Straftat oder einer schwerwiegenden Pflichtverletzung (Anlass zur gezielten Suche und Verwendung) dient. Dies gilt jedoch nur dann, wenn es nach Würdigung objektiver Anhaltspunkte überwiegend wahrscheinlich ist, dass der Beschäftige schwerwiegend gegen seine Pflichten verstoßen hat. Bei dieser Würdigung sind die Interessen des Beschäftigten und des Verbandes gegeneinander abzuwägen. Der Betriebsrat ist unverzüglich zu informieren.

§ 7 Nutzung betrieblicher E-Mail-Konten, betrieblicher Software und des betrieblichen Internetanschlusses

Für die Nutzung betrieblicher E-Mail-Konten, betrieblicher Software und des betrieblichen Internetanschlusses gilt § 6 entsprechend.

§ 8 Mobiles Arbeiten

(1) Die nachfolgenden Regelungen betreffen die Fragen des Datenschutzes und der Datensicherheit, wenn Beschäftigte mobil arbeiten (siehe Betriebsvereinbarung zum Mobilen Arbeiten in ihrer jeweils gültigen Fassung).

(2) Auch wenn Beschäftigte mobil arbeiten, bleiben alle vertraglichen Weisungsrechte des Arbeitgebers bestehen und alle betrieblichen Daten, Informationen und Unterlagen sind Eigentum des Arbeitgebers. Allen Beschäftigten ist es daher untersagt, betriebliche Daten, Informationen oder Unterlagen – insbesondere personenbezogene und sonstige vertrauliche Daten – an Unbefugte weiterzugeben, sie unbefugten Dritten zur Kenntnis gelangen zu lassen (etwa durch Einsichtnahme am Bildschirm oder auf Ausdrucken), sie auf eigenen Speichermedien abzuspeichern, unbefugt zu kopieren oder zu anderen als betrieblichen Zwecken zu verwenden.

(3) Die Sicherheitsmaßnahmen aus der BV „Mobiles Arbeiten“ gelten auch für Geräte.

§ 9 Rechtsfolgen

Der Arbeitgeber hat die Beschäftigten über die rechtlichen Folgen bei Verstößen gegen Datenschutz und Datensicherheit zu belehren. Er muss nicht nur die arbeitsrechtlichen Folgen (Ermahnung, Abmahnung, fristgerechte oder fristlose Kündigung)aufzeigen, son-

dern auch darlegen, dass die Verstöße mit Geldbuße bedroht und/oder strafbar sein und Unterlassungs- und Schadensersatzansprüche nach sich ziehen können.

E Sicherheitsmaßnahmen der Verarbeitung

§ 10 Regelungsgegenstand

Der nachfolgende Abschnitt dient der Interpretation des Artikels 32 DSGVO „Sicherheit der Verarbeitung“ und der dort zu findenden, unbestimmten Rechtsbegriffe. Die Betriebsparteien verständigen sich auf diese Interpretationen, wobei Änderungen durch Behördenauffassungen und gerichtliche Entscheidungen unberührt bleiben.

§ 11 Analyse des Risikos

(1) Betriebsrat und Arbeitgeber verständigen sich darauf, dass mindestens bei den folgenden Bezugspunkten eine Risikobewertung zu erfolgen hat:

- eingesetzte Software,
- eingesetzte Hardware,
- Verarbeitungsprozesse,
- Auslagerung.

(2) Jeder Bezugspunkt i.S.v. Absatz 1, aber auch ggf. weitere Bezugspunkte, werden im Rahmen der Risikobewertung hinsichtlich folgender Aspekte evaluiert:

- Eintrittswahrscheinlichkeit (hiermit ist die objektive Wahrscheinlichkeit gemeint, dass einer der Bezugspunkte derart beeinträchtigt wird, dass personenbezogene Daten unrechtmäßig verarbeitet werden),
- Schadensschwere (hiermit sind alle materiellen und immateriellen Schäden zu berücksichtigen, die bei Betroffenen und beim Arbeitgeber eintreten, sofern personenbezogene Daten unrechtmäßig verarbeitet werden),
- betroffene Rechte und Freiheiten (hiermit sind die besonderen Rechte der Betroffenen zu berücksichtigen, insbesondere die Schutzrechte, die sich aus der Eigenart eines Beschäftigungsverhältnis ergeben, aber ggf. auch andere Grundrechte, wie die Unverletzlichkeit der Wohnung),
- Umfang der Verarbeitung (hier ist das Risiko v.a. an der Datenmenge und/oder der Sensibilität der Verarbeitungsart und des Verarbeitungszwecks zu messen).

(3) Die Betriebsparteien einigen sich auf folgende Klassifizierungskriterien:

- geringes Risiko - Hier ist keiner der drei nachfolgenden Risikofaktoren gegeben:
  1 Es sind der Öffentlichkeit oder den Betriebsparteien erfolgreiche Angriffe auf den jeweiligen Risikobereich bekannt geworden.
  2 Die verarbeiteten Daten sind sensibel, betreffen insbesondere Daten zu finanziellen Informationen einer Person, zur rassischen und ethnischen Herkunft, politischen Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.
  3 Es werden viele Daten verarbeitet.
- mittleres Risiko - Hier ist wenigstens einer der drei o.g. Risikofaktoren gegeben.
- hohes Risiko -Hier sind mindestens zwei der drei o.g. Risikofaktoren gegeben.

(4) Die Risikobewertung führt der Lenkungsausschuss durch. Der Lenkungsausschuss kann einen externen Berater hinzuziehen.

(5) Der Lenkungsausschuss verabschiedet im Zyklus von 24 Monaten eine neue Risikobewertung. Sofern innerhalb eines Zyklus Sicherheitsvorfälle oder wesentliche Veränderungen in den Risikobereichen auftreten, beschließt der Lenkungsausschuss zusätzlich eine anlassbezogene Risikobewertung.

(6) Die Risikobewertung wird dem Betriebsrat innerhalb von zwei Wochen nach Beschlussfassung zur Verfügung gestellt.

(7) Der Lenkungsausschuss kann jederzeit die Absätze 1 bis 3 ergänzen sowie die Zeitraum des Prüfzyklus nach Absatz 5 verändern.

§ 12 Technische und organisatorische Maßnahmen

(1) Der Lenkungsausschuss muss anlassbezogen und mit jeder routinemäßigen Risikobewertung die durch den Arbeitgeber ergriffenen technischen und organisatorischen Maßnahmen zur Einhaltung des Beschäftigtendatenschutzes prüfen und ggf. den Arbeitgeber zu Anpassungen auffordern.

(2) Zu den technischen und organisatorischen Maßnahmen gehören: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Zweckkontrolle. Die Begriffsbestimmungen sind dem alten Bundesdatenschutzgesetz (§ 9 i.V.m. Anlage zum BDSG) zu entnehmen.

(3) Zusätzliche technische und organisatorische Maßnahmen sind: Pseudonymisierung/ Anonymisierung, Verschlüsselung, Maßnahmen zur Belastbarkeit der Systeme und Dienste und Wiederherstellbarkeit verloren gegangener Daten.

(4) Maßnahmen zur Pseudonymisierung oder Anonymisierung können wie folgt definiert werden:

- Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.
- Anonymisierung ist die Veränderung personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(5) Maßnahmen zur Belastbarkeit der Systeme und Dienste sind ausreichend ergriffen worden, wenn die Systeme und Dienste so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gewährleistet ist. Das schließt auch Maßnahmen ein, die ein System vor Angriffen von außen, etwa durch die gezielte Überlastung von Servern mittels sog DoS- oder DDoS-Attacken („[Distributed] Denial of Service"), schützen.

§ 13 Sicherheitsvorfälle

Der Lenkungsausschuss stellt den Beschäftigten ein Hinweisblatt zur Verfügung, in dem er über Sicherheitsvorfälle und die Meldekette informiert.

F Rechte der Beschäftigten und des Betriebsrats

§ 14 Datenschutzbericht

(1) Der Lenkungsausschuss beschließt einmal jährlich einen Datenschutzbericht. Dieser Bericht enthält zumindest folgende Informationen:

- Sicherheitsvorfälle i.S.v. § 12 der Betriebsvereinbarung sowie die hierauf getroffenen Gegenmaßnahmen,
- Veränderungen bei den technischen und organisatorischen Maßnahmen,
- Auslagerungsvorgänge,
- Missbrauchsfälle sowie die hierauf getroffenen Gegenmaßnahmen.

(2) Der Bericht muss so formuliert sein, dass keine Rückschlüsse auf einzelne Mitarbeiter gezogen werden können.

(3) Der Lenkungsausschuss stellt diesen Bericht den Beschäftigten zur Verfügung.

§ 15 Auslagerung

Im Fall einer Auslagerung nach Artikel 28 DSGVO treffen den Arbeitgeber die Auswahl- und Überwachungspflichten. Die Rechte des Betriebsrates nach Betriebsverfassungsgesetz sind zu wahren.

G Besondere Verarbeitungssituationen

§ 16 Eingabekontrolle

Die Betriebsparteien sind sich einig, dass der Arbeitgeber verpflichtet ist, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Hierfür darf der Arbeitgeber die anfallenden Daten verarbeiten. Sobald der Zweck der Verarbeitung entfällt, sind die hierbei erhobenen personenbezogenen Daten unverzüglich zu löschen.

H Schlussbestimmungen

§ 17 Inkrafttreten, Kündigung

Diese Betriebsvereinbarung tritt mit ihrer Unterzeichnung in Kraft. Die Betriebsvereinbarung kann mit einer Frist von drei Monaten ganz oder teilweise zum Ende eines Kalenderjahres gekündigt werden. Die Kündigung bedarf der Schriftform.

§ 18 Schlussbestimmungen

Sollte eine Vorschrift dieser Vereinbarung nicht mit dem geltenden Recht im Einklang stehen und deshalb unwirksam sein, behalten die anderen Regelungen dieser Vereinbarung ihre Gültigkeit. Die unwirksame Regelung ist rechtskonform so auszulegen, dass sie dem beiderseitigen Willen der Parteien entspricht.

Berlin, 25. Mai 2018

Hauptgeschäftsführerin

Betriebsratsvorsitzende