Betriebsvereinbarung

zur Datennutzung bei kritischen Vorfällen

Zwischen der Firma

- Arbeitgeber - [Name und Anschrift]

und

dem Betriebsrat der

- Betriebsrat - [Name der Firma]

Präambel

Das Unternehmen ist Teil eines sog. Cyber-Bündnisses zur gegenseitigen Unterstützung von Unternehmen nach kritischen Vorfällen bzw. Angriffen in den Phasen Detektion und Reaktion inklusive Wiederherstellung.

Das Vorliegen eines kritischen Vorfalls bzw. Angriffs und die damit verbundenen Detektions-, Reaktions- und Wiederherstellungsmaßnahmen können den Einsatz Dritter erfordern. Diese Dritte können im Rahmen der erforderlichen Tätigkeiten auch mit personenbezogenen oder personenbeziehbaren Daten der Beschäftigten in Kontakt kommen.

Mit dieser Betriebsvereinbarung regeln die Betriebsparteien unter welchen Voraussetzungen eine Datennutzung durch Dritte im Falle eines kritischen Vorfalls bzw. Angriffs zulässig ist und wie der Beschäftigtendatenschutz in einem solchen Fall sichergestellt wird.

§ 1 Erlaubnistatbestand und Anwendungsbereich

(1) Diese Betriebsvereinbarung ist ein Erlaubnistatbestand für die Verarbeitung personenbezogener Daten der Arbeitnehmer gemäß Art. 88 DSGVO iVm § 26 Abs. 4 BDSG.

(2) Diese Betriebsvereinbarung gilt für alle Arbeitnehmerinnen und Arbeitnehmer im Sinne des § 5 Abs. 1 BetrVG sowie für Leiharbeitnehmer des Betriebs.

Von dieser Vereinbarung sind ausgenommen:

- Leitende Angestellte im Sinne des § 5 Abs. 3 BetrVG
- Praktikantinnen und Praktikanten
- Auszubildende

Weitere Ausnahmen können zwischen dem Arbeitgeber und dem Betriebsrat vereinbart werden.

(3) Diese Betriebsvereinbarung gilt zeitlich für die Dauer eines kritischen Vorfalls bzw. Angriffs auf den Betrieb. Die sachliche Anwendbarkeit beginnt mit dem Bekanntwerden des kritischen Vorfalls bzw. Angriffs und endet mit der Beendigung des kritischen Vorfalls bzw. Angriffs oder im Falle negativer Auswirkungen auf den Betrieb infolge des kritischen Vorfalls bzw. Angriffs mit der vollständigen Beseitigung dieser negativen Auswirkungen.

(4) Die Betriebsvereinbarung gilt sachlich für die Verarbeitung von personenbezogenen und/oder personenbeziehbaren Daten unabhängig davon, in welchen Systemen diese Daten gespeichert sind und ob die Verarbeitung in standardisierter oder individueller Form erfolgt.

§ 2 Begriffsbestimmungen

(1) Personenbezogene und/oder personenbeziehbare Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person.

(2) Das Verarbeiten von Daten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener und/oder personenbeziehbarer Daten.

(3) Informations- und Techniksysteme (IT-Systeme) bezeichnen Hard- und Software einschließlich sämtlicher Peripheriegeräte, digitale Nebenstellenanlagen, Netze oder webbasierter Systeme.

(4) Im Übrigen gelten die Begriffsbestimmungen des Art. 4 DSGVO und des § 2 BDSG.

(5) Bei einem Vorfall handelt es sich um ein Ereignis, bei dem die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Geschäftsprozessen, IT-Diensten, IT-Systemen oder IT-Anwendungen beeinträchtigt werden und als Folge ein großer Schaden entstehen kann. Diese Vorfälle haben meist ihren Ursprung beispielsweise in einem provozierten Fehlverhalten, einer ausgenutzten Schwachstelle oder einer negativen Einwirkung von außen, hierzu zählen auch unbeabsichtigte und unkontrollierbare Einwirkungen durch Naturgewalten, wie z.B. Blitzschlag, Wasser, Feuer und Erdbeben.

(6) Ein Angriff ist jede interne oder externe Einwirkung auf ein oder mehrere andere IT-Systeme, mit der Absicht deren Cybersicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen.

Ein Angriff ist als negative Einwirkung von außen auf ein IT-System immer auch ein Vorfall.

(7) Kritisch ist ein Vorfall oder Angriff, wenn dieser erhebliche oder potentiell erhebliche Auswirkungen auf die Informationssicherheit hat und die Gefahr eine Krise birgt.

(8) Eine Krise ist eine vom Normalzustand abweichende Situation, die trotz vorbeugende Maß nahmen im Unternehmen in Folge eines Vorfalls jederzeit eintreten und mit der normalen Aufbau- und Ablauforganisation nicht bewältigt werden kann und zu einer Unterbrechung des Geschäftsbetriebs führt.

§ 3 Datenschutzregeln

(1) Die Betriebsparteien sind sich einig, dass bei jeglicher Datenverarbeitung im Zusammenhang mit dem Vorliegen eines kritischen Vorfalls bzw. Angriffs die Persönlichkeits- und Datenschutzrechte der Mitarbeiterinnen und Mitarbeiter bestmöglich zu wahren sind.

(2) Der Arbeitgeber ist befugt, im Falle eines kritischen Vorfalls bzw. Angriffs auch Dritten im Rahmen des Cyber-Bündnisses zur Bekämpfung des Vorfalls bzw. Angriffs Zugang zu per sonenbezogenen und/oder personenbeziehbaren Daten des Unternehmens zu gewähren, wenn dies für Detektions-, Reaktions- oder Wiederherstellungsmaßnahmen erforderlich ist.

(3) Der Arbeitgeber stellt sicher, dass diese Dritten bevor sie Zugriff auf Unternehmensdaten erhalten, hinreichend auf das Datengeheimnis und zur Vertraulichkeit verpflichtet wurden. Das Vorliegen entsprechender Verpflichtungen ist durch den Arbeitgeber zu dokumentie ren und dem Betriebsrat auf Verlangen vorzulegen.

(4) Der Arbeitgeber wird den Betriebsrat rechtzeitig, umfassend und unaufgefordert über die Folgen eines kritischen Vorfalls bzw. Angriffs auf die personenbezogenen und/oder personenbeziehbaren Daten der Beschäftigten informieren.

§ 4 Schlussbestimmungen

(1) Die Betriebsvereinbarung tritt mit ihrer Unterzeichnung in Kraft.

(2) Die Betriebsvereinbarung kann unter Einhaltung einer Kündigungsfrist von 3 Monaten zum Monatsende, frühestens jedoch zum gekündigt werden. Wenn diese Betriebsvereinbarung gekündigt wird, wirkt sie insgesamt nach, bis sie durch eine andere Regelung abgelöst wird.

(3) Sollten eine oder mehrere Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam oder undurchführbar sein, so bleibt die Wirksamkeit der übrigen Bestimmungen un-

berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt die Regelung, die dem von den Parteien mit der unwirksamen oder undurchführbaren Regelung Gewollten in rechtlich zulässiger Weise am nächsten kommt.