Betriebsvereinbarung über Awareness-Schulung und Phishing-Simulation

Muster, Stand 01.11.2026 · zwischen der _____ (Arbeitgeber) und dem Betriebsrat der _____

Wozu dieses Muster: Phishing-Simulationen können unter § 87 Abs. 1 Nr. 6 BetrVG fallen. Diese Vereinbarung regelt Zweck, Ablauf und Grenzen so, dass niemand überwacht oder bloßgestellt wird. Sie ist auf die Verarbeitung bei secureIT zugeschnitten; Anpassungen sind ausdrücklich erwünscht. Sie ersetzt keine Rechtsberatung.

§ 1 Gegenstand und Zweck

(1) Der Arbeitgeber führt mit dem Anbieter secureIT UG (haftungsbeschränkt) eine Awareness-Schulung zu IT-Sicherheit und Phishing sowie anschließend simulierte Phishing-E-Mails („Simulation") durch.

(2) Zweck ist ausschließlich die Schulung der Beschäftigten, die Stärkung der Sicherheitskultur und der Nachweis der Schulung gegenüber Versicherern, Auftraggebern und Aufsichtsbehörden. Eine Verhaltens- oder Leistungskontrolle einzelner Beschäftigter findet nicht statt.

§ 2 Geltungsbereich

Diese Vereinbarung gilt für alle Beschäftigten des Betriebs _____, die an der Schulung teilnehmen. Auszubildende und Aushilfen sind eingeschlossen, soweit sie ein dienstliches E-Mail-Postfach nutzen.

§ 3 Ablauf

1. **Information vorab:** Die Beschäftigten werden vor Beginn mit dem Infoblatt über Zweck, Ablauf und Datenverarbeitung informiert.
2. **Schulung zuerst:** Jede Person erhält Zugang zum Online-Kurs. Erst nach Abschluss der Schulung beginnt die Simulation.
3. **Angekündigte Simulation:** Die Beschäftigten wissen, dass innerhalb der Laufzeit simulierte Phishing-Mails eintreffen. Der genaue Zeitpunkt wird nicht genannt. Läufe ohne vorherige Schulung oder Ankündigung, die die Plattform für bereits geschulte Teams anbietet, sind von dieser Vereinbarung nicht umfasst und bedürfen einer Ergänzung.
4. **Lernmoment statt Sanktion:** Wer auf eine Simulation klickt, sieht sofort eine Erklärungsseite. Es folgt keine Meldung an Vorgesetzte und kein Eintrag in die Personalakte.
5. **Laufzeit:** Ein Durchlauf dauert höchstens _____ Wochen. Wiederholungen finden höchstens einmal je zwölf Monate statt, sofern nicht anders vereinbart.

§ 4 Auswertung ohne Personenbezug

(1) Zur Simulation erhält der Arbeitgeber ausschließlich den Teamreport: zusammengefasste Angaben ohne Namen (gesendet, geöffnet, geklickt, Daten eingegeben, technische Merkmale wie Betriebssystem und Browser) und die Beteiligung (Schulung aufgerufen, abgeschlossen, Phishing-Training absolviert). Ein Durchlauf umfasst mindestens drei Personen; die Betriebsparteien können eine höhere Mindestzahl festlegen. Für eine einzelne Person gibt es keinen Teamreport.

(2) Für den Schulungsnachweis und die Steuerung des Durchlaufs sieht der Arbeitgeber namentlich, wer die Schulung begonnen und abgeschlossen hat und wie viele Simulationsmails an die Person versandt wurden, nicht aber, wer geöffnet, geklickt oder etwas eingegeben hat.

(3) Es gibt keine Liste, welche Person geklickt hat. Der Anbieter stellt eine solche Liste dem Arbeitgeber nicht zur Verfügung.

(4) Jede Person sieht nur ihr eigenes Ergebnis. Das Teilnahmezertifikat bestätigt die Teilnahme an der Schulung, nicht das Klickverhalten.

(5) Ergebnisse der Simulation werden nicht für arbeitsrechtliche Maßnahmen, Beurteilungen, Zielvereinbarungen oder Vergütungsentscheidungen verwendet.

§ 5 Datenverarbeitung und Löschung

(1) Verarbeitet werden: Name, dienstliche E-Mail-Adresse, Gruppenzuordnung, Lernfortschritt und Schulungsabschluss mit Datum, Ergebnis des Wissenstests sowie Ereignisse der Simulation (Versand, Öffnung, Klick, Eingabe auf der Übungsseite) mit den dabei anfallenden technischen Daten (IP-Adresse, E-Mail-Programm, Browser). Eingegebene Passwörter werden nicht gespeichert.

(2) Die Verarbeitung erfolgt auf Servern in Deutschland im Auftrag des Arbeitgebers (Art. 28 DSGVO). Ein Auftragsverarbeitungsvertrag liegt vor. Ausnahme: Nur wenn der Arbeitgeber eine Simulationsvorlage mit Sprachnachricht auswählt, gehen Vorname und E-Mail-Adresse der Person zur Erzeugung der Stimme an den dort genannten Unterauftragsverarbeiter ElevenLabs in den USA.

(3) Personenbezogene Ereignisdaten der Simulation werden nach Abschluss des Durchlaufs archiviert, nicht weiter ausgewertet und spätestens nach Monaten gelöscht. Nachweisdaten (wer wann geschult wurde) werden für die Dauer der Nachweispflicht, höchstens drei Jahre, aufbewahrt.

§ 6 Rechte der Beschäftigten

(1) Die Teilnahme an der Schulung ist Arbeitszeit. (2) Jede Person kann ihr eigenes Ergebnis einsehen und Auskunft nach Art. 15 DSGVO verlangen. (3) Beschwerden über Ablauf oder Auswertung können an den Betriebsrat oder die Datenschutzbeauftragte / den Datenschutzbeauftragten gerichtet werden.

§ 7 Rechte des Betriebsrats

(1) Der Betriebsrat erhält den Teamreport zeitgleich mit dem Arbeitgeber. (2) Vor jedem weiteren Durchlauf wird der Betriebsrat informiert; wesentliche Änderungen am Verfahren bedürfen einer Ergänzung dieser Vereinbarung. (3) Der Betriebsrat kann die Simulation (nicht die Schulung) jederzeit aussetzen lassen, wenn ein Verstoß gegen § 4 vorliegt.

§ 8 Schlussbestimmungen

Diese Vereinbarung tritt mit Unterzeichnung in Kraft und kann mit einer Frist von drei Monaten zum Monatsende gekündigt werden; bis zum Abschluss einer neuen Vereinbarung wirkt sie nach. Sollte eine Bestimmung unwirksam sein, bleibt die Vereinbarung im Übrigen wirksam.

_____	_____
Ort, Datum · Arbeitgeber	Ort, Datum · Betriebsratsvorsitzende/r

Dieses Muster stellt secureIT UG (haftungsbeschränkt) kostenlos zur Verfügung. Es ist ein Formulierungsvorschlag, keine Rechtsberatung. Prüfen Sie es vor Unterzeichnung mit Ihrer Rechtsberatung oder Ihrem Datenschutzbeauftragten. Quelle: secureit.icu/fuer-betriebsraete