# Muster-Betriebsvereinbarung: Nutzung privater IT-Systeme

§ 2 Allgemeine Bestimmungen

(1) Diese Betriebsvereinbarung regelt den datenschutzkonformen Einsatz privater IT-Systeme zur Erledigung dienstlicher Aufgaben sowohl innerhalb wie auch außerhalb der Diensträume des >>UNTERNEHMENS<< (im folgenden Unternehmen).

Private Endgeräte (stationär oder mobil) dürfen genutzt werden, um personenbezogene Daten auf einem gesicherten Server des Unternehmens oder einer beauftragten Stelle i.S. des Artikels 28 der DSGVO zu verarbeiten. Die Speicherung personenbezogener Daten auf dem Festspeicher privater mobiler Endgeräte (Smartphones und Tablets) ist nicht zulässig. Das Speichern und Anzeigen personenbezogener Daten in Clouds oder über Applikationen von Fremdanbietern ist zulässig, wenn zuvor mit diesen vom Unternehmen ein Vertrag zur Auftragsverarbeitung i.S. von Artikel 28 Abs. 3 DSGVO geschlossen wurde. Für den Fall, dass im Rahmen einer Auftragsverarbeitung eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgt, sind die Artikel 44 bis 49 DSGVO einzuhalten.

(2) Wenn Beschäftigte auf privaten IT-Systemen Daten nach § 4 verarbeiten, ist das eine dienstliche Tätigkeit. „Verantwortlicher“ i.S. der DSGVO ist daher auch in diesen Fällen das Unternehmen. Die Geschäftsleitung bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften auch dann verantwortlich, wenn die Beschäftigten derartige Daten zu Hause verarbeiten.

**§ 3 Genehmigungsverfahren**

(1) Beschäftigte, die auf einem privaten IT-System personenbezogene Daten nach § 4 verarbeiten wollen, bedürfen dazu der schriftlichen Genehmigung der Geschäftsleitung.

In dem Antrag auf Genehmigung sind das IT-System, die Software und die Datenschutz- und Datensicherungsmaßnahmen nach § 5 Abs. 1 in Stichworten zu beschreiben. Die Genehmigung wird nur erteilt, wenn die oder der Beschäftigte die in § 6 vorgeschriebene Verpflichtungserklärung abgibt. Die Genehmigung ist auf dem Antrag zu vermerken und zur Personalakte zu nehmen.

Eine Kopie des genehmigten Antrags ist der oder dem Beschäftigten auszuhändigen, eine weitere Kopie der oder dem Datenschutzbeauftragten des Unternehmens.

(2) Die Genehmigung gilt für einen Zeitraum von maximal zwei Jahren; danach ist ggf. erneut eine Genehmigung zu beantragen. Bei wesentlichen Änderungen, wie z.B. Austausch des IT-Systems und/oder Wechsel des Betriebssystems, ist unverzüglich eine neue Genehmigung durch die oder den Beschäftigten zu beantragen.

(3) Der genehmigte Antrag und die Verpflichtungserklärung sind aufzubewahren. Der genehmigte Antrag ersetzt nicht das Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 Abs. 1 DSGVO. Die Sammlung der genehmigten Anträge ist für Überprüfungen durch die Datenschutzaufsichtsbehörde vorzuhalten.

**§ 4 Datenrahmen**

(1) Es dürfen nur personenbezogen Daten verarbeitet werden, die für die Aufgabenwahrnehmung durch die oder den Beschäftigten erforderlich sind.

(2) Folgender Datenrahmen darf nicht überschritten werden:

*Auflistung der maximal erlaubten Daten bzw. Datenarten und der betroffenen Personengruppen
Beispiel:
Daten zu Verträgen mit Kunden (Kunden = Unternehmen)
Namen, Adressdaten, E-Mail-Adresse und Telefonnummer von Ansprechpartnern beim Kunden
Kommunikation mit den Ansprechpartnern, Vertragskonditionen*

Von diesen Daten dürfen nur die Daten verarbeitet werden, die für die jeweilige Aufgabenerledigung tatsächlich erforderlich sind.

**§ 5 Datenschutz- und Datensicherungsmaßnahmen**

(1) Durch geeignete organisatorische und technische Maßnahmen ist sicherzustellen, dass nur die oder der Beschäftigte selbst Zugang zu den in § 4 genannten Daten erhält:

* Werden die Daten auf internen Speichermedien (z.B. Festplatte) gespeichert, sind die Daten durch geeignete technische Maßnahmen gegen Zugriff zu sichern. Dafür ist mindestens eine Zugriffskontrolle durch das Betriebssystem auf Verzeichnis- oder Dateiebene einzurichten sowie eine Verschlüsselung der Verzeichnisse, in denen die Daten gespeichert sind, vorzunehmen. Online-Zugriffe auf die Daten sind durch den Stand der Technik entsprechende Vorkehrungen (z.B. Firewall) auszuschließen.
* Werden für die Speicherung der Daten externe Speichermedien verwendet, sind diese zu verschlüsseln und so aufzubewahren, dass sie Unbefugten nicht zugänglich sind.
* Es ist insbesondere darauf zu achten, dass aktuelle Updates und Patches auf der genutzten Hard- und Software (einschließlich Router, Endgeräte, Betriebssysteme, Applikationen und Programme) aufgespielt sind und ein hinreichender Schutz vor Schadprogrammen vorhanden ist.

(2) Es muss sichergestellt sein, dass die in § 4 genannten Daten jederzeit auch dann verfügbar sind, wenn das IT-System ausfällt oder der Datenträger oder -speicher beschädigt wird (Datensicherung).

(3) Die Daten nach § 4 dürfen auf den privaten Geräten nur so lange elektronisch gespeichert werden, wie die oder der Beschäftigte diese zur Aufgabenerfüllung auf dem privaten IT-System benötigt. Danach sind die elektronisch gespeicherten Daten zu löschen und es ist – soweit erforderlich – auf Daten, die auf Dienstgeräten gespeichert sind, zurückzugreifen.

(4) Die elektronische Übersendung oder Übertragung der Daten nach § 4 sowie der Transport der Daten mittels elektronischer Speichermedien sind nur zulässig, wenn die Daten verschlüsselt werden. Bei einer zulässigen Speicherung auf Speicherorten, die nur über das Internet erreichbar sind, ist ein verschlüsselter Transportweg einzuhalten.

(5) Weitergehende konkrete Vorgaben zur datenschutzkonformen Konfiguration der privaten IT-Systeme durch die IT-Abteilung bzw. die oder den Informationssicherheitsbeauftragte(n) müssen eingehalten werden.

**§ 6 Verpflichtungserklärung**

Mit dem Antrag auf Genehmigung der Verarbeitung personenbezogener Daten nach § 4 auf einem privaten IT-System ist der Geschäftsleitung folgende schriftliche Erklärung zu übergeben:

„Ich verpflichte mich, bei der Verarbeitung personenbezogener Daten des Unternehmens auf meinem privaten IT-System

* den Datenrahmen gemäß § 4 und die Datenschutz- und Datensicherungsmaßnahmen gemäß § 5 der Betriebsvereinbarung vom >>DATUM<< zur Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen (IT-Systemen) von Beschäftigten einzuhalten und
* dem Unternehmen einen Ausdruck oder ein verschlüsseltes elektronisches Speichermedium mit allen gespeicherten Daten zur Verfügung zu stellen, wenn das Unternehmen diese benötigt (z.B. wenn ein Antrag auf Auskunft nach Artikel 15 DSGVO gestellt worden ist).

Ich sichere zu, den Beschäftigten der zuständigen Datenschutzaufsichtsbehörde im Rahmen einer Prüfung auf Verlangen Zugang zu allen im Rahmen der o.g. Betriebsvereinbarung genutzten privaten IT-Systemen und Speichermedien zu gewähren, um ihr oder ihm die Wahrnehmung der gesetzlichen Kontrollaufgaben im dienstlichen Bereich zu ermöglichen.“

**§ 7 Rechtlicher Hinweis**

Die Einhaltung der Bestimmungen dieser BV kann von der Unternehmensleitung, der oder dem für das Unternehmen bestellten Datenschutzbeauftragten im privaten Bereich der Beschäftigten nicht kontrolliert werden. Darum ist von den Beschäftigten die Verpflichtungserklärung gemäß § 6 abzugeben.

Es wird ausdrücklich darauf hingewiesen, dass Verstöße gegen diese Bestimmungen eine Verletzung der arbeitsrechtlichen Pflichten darstellen, die arbeitsrechtlich verfolgt werden muss, wenn sie der Unternehmensleitung bekannt wird.