Bundesverband Lohnunternehmen BLU e.V.
Portlandstraße 24, 31515 Wunstorf
Tel. 05031 / 519 45 0, Fax. 05031 / 519 45 2827
http://www.lohnunternehmen.de
e-Mail: info@lohnunternehmen.de

Beschreibung der technischen und organisatorischen Maßnahmen (TOM)

Haftungsausschluss: Die nachstehende Mustervorlage ist nur nach sorgfältiger Prüfung und Anpassung auf Ihren konkreten Einzelfall und nach Ihren eigenen Anforderungen anzuwenden. Sie sollten sich auch in jedem Fall vor Verwendung des Musters an die Rechtsberatung des BLU e.V. wenden.

TOM	Bereich (Dieser Teil dient nur der Erklärung der jeweiligen TOM)	Umsetzung (Was sollte jeweils zur Einhaltung der TOM umgesetzt werden)	Konkretisierung der Maßnahme auf Ihren Betrieb
Zutrittskontrolle	nur befugte Personen dürfen Zutritt zu den Datenverarbeitungsanlagen haben.	Hier sind Personen zu nennen, die Zugang zum Server, Computersystemen usw. haben; Schließsystem, ID-Karte,Pförtner, Alarmanlage u.ä	Bsp. Zutritt hat nur Geschäftsführer
Zugangskontrolle	Unbefugte dürfen keine Möglichkeit haben, die Datenverarbeitungsanlagen zu nutzen. -> Hier sind die Vorkerhungen zur Sicherung z.B. Benutzernamen und Passwörter für berechtigte Personen der Buchhaltung usw.	Hier sind die Vorkehrungen zur Sicherung z.B. Schlösser, Türen usw. zu benennen, damit unbefugte nicht an die Systeme gelangen; Kennwörter, Datenträgerverschlüsselung, aut. Sperrung, usw.	Server und Ordner im Büroraum des Inhabers durch Türen mit Schlüssel gesichert. Schlüssel hat nur Betriebsinhaber...
Zugriffskontrolle	Personen, die zur Benutzung der Datenverarbeitungsanlagen berechtigt sind, dürfen nur auf solche Daten zugreifen können, die ihrer jeweiligen Zugriffsberechtigung unterliegen. Zusätzlich darf es nicht möglich sein, dass personenbezogene Daten nach dem Speichern unbefugt gelesen, kopiert, verändert oder entfernt werden können.	Hier sind entsprechend die Personen und deren Zugriffsrechte bzw. -beschränkungen anzugeben. Z.B. Personen aus Buchhaltung dürfen und können nur Kontodaten verändern u.ä., Beschränkungen durch Benutzerkennung und Passwörter; Berechtigungen, Zugriffsrechte, Passwörter, Sperrung ausscheidender Mitarbeiter	
Trennungskontrolle	Zu unterschiedlichen Zwecken erhobene Daten müssen grundsätzlich auch getrennt verarbeitet werden können.	Wer verarbeitet welche Daten in Ihrem Betrieb; Wer hat Zugriff auf Buchhaltungsdaten, Kundendaten, Administration usw.	
Pseudonymisierung	Daten sind nach Möglichkeit zu Pseudonymisieren	Auftragsnummer anstelle von Personenbezogenen Daten wie Name Adresse usw.; Rückschluss auf Personen nur mit zusätzlicher Info, Erschweren der Lesbarkeit von Datern durch Unbefugte	
Weitergabekontrolle	Personenbezogene Daten dürfen während der elektronischen Übertragung oder während eines Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Es muss nachvollziehbar und überprüfbar sein, an welche Stellen Daten übermittelt werden.	Wohin werden Daten weitergegeben. Wie ist das gesichert? Z.B. wer gibt die Daten zur Lohnabrechnung wie weiter. Wie erfolgt die Sicherung beim Steuerberater (verweis auf Auftragsdatenverarbeitungsvertrag) - ähnliches gilt bei Datenauftragsverarbeitung durch Datenerfassungssysteme in der Landwirtschaft; Verschlüsselung, VPN, SSL	

Bundesverband Lohnunternehmen BLU e.V.
Portlandstraße 24, 31515 Wunstorf
Tel. 05031 / 519 45 0, Fax. 05031 / 519 45 2827
http://www.lohnunternehmen.de
e-Mail: info@lohnunternehmen.de

Beschreibung der technischen und organisatorischen Maßnahmen (TOM)

Haftungsausschluss: Die nachstehende Mustervorlage ist nur nach sorgfältiger Prüfung und Anpassung auf Ihren konkreten Einzelfall und nach Ihren eigenen Anforderungen anzuwenden. Sie sollten sich auch in jedem Fall vor Verwendung des Musters an die Rechtsberatung des BLU e.V. wenden.

Eingabekontrolle	Es muss nachträglich überprüft werden, von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden.	Liegen Muster zur Verarbeitung der Daten vor und lässt sich die Verarbeitung nachverfolgen? Werden personenbezogene Daten im Auftrag von Dritten verarbeitet, darf dies nur den Anweisungen des Auftraggebers folgend geschehen; Protokollierung der Eingabe, Nachvollziehbarkeit	
Datensicherung	Die Daten müssen gegen zufällige Zerstörung oder Verlust geschützt sein.	regelmäßige Backups der Daten und sichere Aufbewahrung z.B. aufbewahren außerhalb des Unternehmens. Um gegen Datendiebstahl durch die eigenen Mitarbeitenden abgesichert zu sein, sollten sensible Daten verschlüsselt und bestimmte Räume oder Gebäude gegen unbefugten Zutritt gesichert sein; keine Feuchtigkeit zu hohe Hitze im Serverraum etc.	
Virenschutz- Firewall	Computer gegen Virenbefall sichern und regelmäßig aktualisieren. Dazu gehört auch eine vernünftige Firewall	Sie sollten vernünftige Programme vorhalten (nicht freeware); Internetzugang sichern und vertrauliche Daten verschlüsseln, um gegen Hackerangriffe gewappnet zu sein.	
Stetige Aktualisierung vom Betriebssystem und Software	Selbsterklärend		
Notfall- und Vertretungspläne	Systemadministration muss alle Systemeinstellungen und Passwörter dokumentieren und sicher hinterlegen. Für den Fall des Ausfalls eines Administrators/in sollte eine mit dem System vertraute Ersatzperson vorhanden sein.		

Die grauen Zeilen und Spalten sind in Ihrer TOM nicht aufzuführen,
sie dienen lediglich der Erklärung, was Sie zu tun haben