

Gesellschaft / Behörde _____

Name des Verantwortlichen _____

Straße _____

PLZ / Ort _____

Vertraulichkeitserklärung

1. Die oben genannte Gesellschaft / Behörde ist verpflichtet, über alle Informationen, die ihr im Zusammenhang mit ihrer Tätigkeit bei der Verkehrsbetriebe Peine-Salzgitter GmbH (VPS) bekannt werden, Stillschweigen zu bewahren, gleichgültig ob es sich dabei um VPS selbst oder deren Geschäftsverbindungen handelt.
2. Diese Vertraulichkeitsverpflichtung gilt nicht für Informationen, die
 - a. die oben genannte Gesellschaft / Behörde nachweislich von Dritten erhalten hat oder erhält,
 - b. allgemein bekannt sind,
 - c. deren Bekanntgabe VPS schriftlich zugestimmt hat.
3. Bei Einschaltung Dritter hat die oben genannte Gesellschaft / Behörde deren Verpflichtung zur Verschwiegenheit sicherzustellen.
4. Erhaltene Geschäfts- und Betriebsunterlagen dürfen nur im Rahmen der betrieblichen Erfordernisse und der urheberrechtlichen Bestimmungen vervielfältigt werden.
5. Die oben genannte Gesellschaft / Behörde hat die technischen und organisatorischen Maßnahmen gemäß § 9 BDSG zu berücksichtigen (siehe Anlage).

Verpflichtung auf das Datengeheimnis

Die oben genannte Gesellschaft / Behörde wird wie folgt auf das Datengeheimnis nach Maßgabe des § 5 BDSG verpflichtet und auf die Strafbarkeit von Verstößen hingewiesen:

1. Die oben genannte Gesellschaft / Behörde verpflichtet sich, unbeschadet sonstiger betrieblicher Geheimhaltungspflichten, das Datengeheimnis zu wahren.
2. Die oben genannte Gesellschaft / Behörde ist befugt, ihr anvertraute personenbezogene Daten nur im Rahmen der mit ihr geschlossenen Vereinbarung zu verarbeiten.
3. Verstöße können nach § 43 ff BDSG und anderer einschlägiger Rechtsvorschriften mit Geld- oder Freiheitsstrafe geahndet werden.

Diese Pflicht besteht auch nach Beendigung des Vertragsverhältnisses mit VPS.

Ort, Datum

Unterschrift des Verantwortlichen / (Klarschrift)

1 Kopie an bDSB (Abt. ZA - Herr Ludwig)

1. Zutrittskontrolle → Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insb. auch zur Legitimation der Berechtigten:

- | | |
|---|---|
| <input type="checkbox"/> Zutrittskontrolle (Ausweisleser, Magnetkarte, Chipkarte) | <input type="checkbox"/> Überwachungseinrichtungen (Alarmanlage, Video- /Fernsehmonitor) |
| → zu beachten: § 6c BDSG (Mobile personenbezogenen Speicher- und Verarbeitungsmedien) | → zu beachten: § 6b BDSG Beobachtung öffentlich zugängliche Räume mit optisch-elektronischen Einrichtungen) |
| <input type="checkbox"/> Schlüssel / Schlüsselvergabe | <input type="checkbox"/> Türsicherung (elektrische Türöffner usw.) |
| <input type="checkbox"/> Werkschutz, Pförtner | <input type="checkbox"/> Festlegung der zutrittsberechtigten Personen |
| <input type="checkbox"/> Protokollierung der Zutritte / Abgänge | <input type="checkbox"/> Einrichtung von Sicherheitszonen u -bereichen |

2. Zugangskontrolle → Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- | | |
|---|---|
| <input type="checkbox"/> Einrichtung eines Benutzerstammsatzes pro User | <input type="checkbox"/> Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßige Kennwortänderung) |
| <input type="checkbox"/> Absicherung der DV-Systeme und Netzwerke gegen Zugänge von außen | <input type="checkbox"/> Regelmäßige Kontrolle der Gültigkeit der Zugangsberechtigungen |
| <input type="checkbox"/> Protokollierung der Zugänge | <input type="checkbox"/> Automatische Sperrung (z.B. Kennwort oder Pausenschaltung) |
| <input type="checkbox"/> Verschlüsselung von Datenträgern | <input type="checkbox"/> Sicherung der Bildschirmarbeitsplätze bei Abwesenheit und laufendem System |

3. Zugriffskontrolle → Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- | | |
|---|---|
| <input type="checkbox"/> Berechtigungskonzepte (z.B. Profile, Rollen, Transaktionen) | <input type="checkbox"/> Festlegung der Zugriffsrechte (z.B. Lesen, Ändern, Löschen, Auswerten, Administrieren) |
| <input type="checkbox"/> Regelmäßige Kontrolle der Gültigkeit der zugewiesenen Berechtigungen | <input type="checkbox"/> Festlegung der personellen Zuständigkeiten |
| | <input type="checkbox"/> Protokollierung der Zugriffe |

4. Weitergabekontrolle → Der Schutz personenbezogener Daten bei Weitergabe ist zu gewährleisten.

- | | |
|---|---|
| <input type="checkbox"/> Verschlüsselung | <input type="checkbox"/> Festlegung der Übermittlungswege und Datenempfänger |
| <input type="checkbox"/> Elektronische Signatur | <input type="checkbox"/> Transportsicherung (z.B. verschlossener Versand, Kennwortschutz bei Dateübertragung) |
| <input type="checkbox"/> Tunnelverbindung | |
| <input type="checkbox"/> Protokollierung bei Weitergabe | |
| <input type="checkbox"/> Virtual Private Network (VPN) | |

5. Eingabekontrolle → Die Nachvollziehbarkeit der Datenverwaltung und -pflege ist zu gewährleisten.

- | |
|---|
| <input type="checkbox"/> Protokollierung der Eingabe |
| <input type="checkbox"/> Festlegung der Zuständigkeiten für Eingabe |

6. Auftragskontrolle → Die weisungsgemäße Auftragsdatenverarbeitung sowie die Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer sind zu gewährleisten.

- | | |
|--|---|
| <input type="checkbox"/> Festlegung der Kriterien zur Auswahl des Auftragnehmers | <input type="checkbox"/> Regelmäßige Kontrolle der Vertragsausführung |
| | <input type="checkbox"/> Eindeutige Vertragsgestaltung |

7. Verfügbarkeitskontrolle → Die Daten sind gegen Zerstörung oder Verlust zu schützen.

- | | |
|---|--|
| <input type="checkbox"/> Notfallplan (z.B. USV) | <input type="checkbox"/> Regelmäßige Datensicherung (Backup-Verfahren) |
| <input type="checkbox"/> Virenschutz | <input type="checkbox"/> Regelmäßige Durchführung einer Risiko- und Schwachstellenanalyse bezogen auf Hard- und Software |
| <input type="checkbox"/> Getrennte Aufbewahrung | |
| <input type="checkbox"/> Spiegeln von Festplatten | |

8. Trennungskontrolle → Daten, die zu verschiedenen Zwecken erhoben wurden, sind getrennt zu verarbeiten.

- | | |
|--|--|
| <input type="checkbox"/> Funktionstrennung / Produktion / Test | <input type="checkbox"/> Aufteilung in mehrere Mandanten |
|--|--|