Eigene Datenschutz-Policy

Beispiel:

Schulung und Sensibilisierung: Alle Beschäftigten sollten über die Datenschutzrichtlinien des eigenen Unternehmens informiert sein und diese auch verstehen. Das beinhaltet jegliche Vorschriften zur Datenspeicherung und -weitergabe: Wer etwas nicht versteht, sollte direkt nachfragen!

Sichere Passwörter: Alle Beschäftigten müssen sichere Passwörter verwenden, die eine Kombination aus Buchstaben, Zahlen und Sonderzeichen enthalten. Passwörter sollten regelmäßig geändert werden. Die eigenen Zugangsdaten sollten niemals mit anderen Personen geteilt werden.

Ausloggen aus Konten: Alle Beschäftigten sollten sich immer aus ihren Konten ausloggen und ihren Computer sperren, bevor sie ihn verlassen, auch wenn es nur für eine kurze Zeit ist.

Keine Speicherung persönlicher Informationen: Man sollte keine persönlichen Informationen auf Arbeitscomputern speichern, es sei denn, dies ist für die Arbeit absolut notwendig.

Sichere Internetnutzung: Alle Mitarbeiterinnen und Mitarbeiter sollten beim Surfen im Internet Vorsicht walten lassen und keine verdächtigen Links anklicken oder unsichere Websites besuchen - sie hüten sich auch vor Phishing-Versuchen und Spam-Mails.

Datenminimierung: Gesammelt werden nur die Daten, die für berufliche Aufgaben unbedingt erforderlich sind.

Verantwortungsvolle Kommunikation: Alle sind vorsichtig beim Versenden von E-Mails, insbesondere wenn diese sensible Informationen enthalten. Vor Versand sollte abgewägt werden, ob E-Mails wirklich notwendig sind oder ob eine sicherere Kommunikationsmethode wie ein internes Unternehmensportal (Intranet) verwendet werden kann.

Datensicherheit am Arbeitsplatz: Alle stellen sicher, dass sie ihren Arbeitsplatz im Betrieb oder während des mobilen Arbeitens physisch absichern. Das bedeutet, dass niemand Informationen vom Bildschirm ablesen kann. Maßnahmen sind z. B. das Sperren des Computers, sobald man den Arbeitsplatz verlässt und die sichere Aufbewahrung sensibler Dokumente z. B. im abschließbaren Schrank. Niemals sollten solche offen liegen gelassen werden!

Löschung von Daten: Daten, die nicht mehr benötigt werden, müssen gemäß den Vorschriften des Unternehmens nach Ablauf einer festgelegten Frist gelöscht werden.

Nutzung von Unternehmensanwendungen: Alle Beschäftigten nutzen nur vom Unternehmen genehmigte Anwendungen und Dienste, um sicherzustellen, dass sie den Datenschutzstandards entsprechen.

Sicherer Remote-Zugriff: Wer von außerhalb des Unternehmensnetzwerks arbeitet, verwendet sichere VPN-Verbindungen und andere Sicherheitsmaßnahmen, um den Zugriff auf berufliche Ressourcen zu schützen.