Richtlinie zum Datenschutz und zur EDV-Nutzung

P12_RL01_00

Zweck und Geltungsbereich:

Diese Richtlinie gilt für alle Mitarbeiter der Schönek Gruppe und all ihren Partnern. Die geltenden gesetzlichen Anforderungen sind in dieser Richtlinie berücksichtigt, werden einmal im Jahr auf ihre Gültigkeit überprüft, bei Änderungen angepasst und Mitarbeitern und externen Partnern (falls ein Projekt dies erfordert) zur Verfügung gestellt. Kundenspezifische Anforderungen zum Thema Datenschutz gelten ergänzend zu dieser Richtlinie, es sei denn, zwischen dem Kunden und der Firma Schönek wird eine andere Regelung vereinbart.
Die Erstellung dieser Richtlinie ist Teil der Implementierung des Informationsmanagementsystems nach VDA, wie im Managementreview des Geschäftsjahres 2021 festgelegt.

Verantwortlichkeit:

IT-Beauftragte(r)

0	Neuerstellung
Revision	Beschreibung

Erstellt:	20.07.2022, Thiesbürger, Björn
Geprüft	21.07.2022, Kinateder, Manuela
Freigegeben:	21.07.2022, Freitag, Andreas

Richtlinie zum Datenschutz und zur EDV-Nutzung

P12_RL01_00

Die Schönek Gruppe stellt den Mitarbeitern verschiedene Kommunikations- und EDV-Systeme zur Erfüllung ihrer Aufgaben zur Verfügung. Nachfolgende Richtlinien sind damit verpflichtend:

1. Die für die Zwecke des Unternehmens zur Verfügung gestellten Geräte, EDV- / Kommunikationsmittel, Programme und Daten sind vor Zerstörung, Verfälschung und Diebstahl zu schützen, insbesondere auch bei dessen mobilen Einsatz.

2. Hard- und Software sind ausschließlich vom bestimmten Mitarbeiter für betriebliche Aufgaben, d.h. für die jeweils angeordneten oder genehmigten Zwecke zu benutzen. Private Hard- und Software darf nicht installiert werden. Generell sind Veränderung an Hard- und Software nur durch autorisierte Personen wie dem EDV-Beauftragten durchzuführen; sowie auch in diesem Fall durch beauftragte Mitarbeiter eines Dienstleisters, beispielhaft aufgeführt der MS Solutions Informationssysteme GmbH und der Herrmann Datensysteme GmbH.

3. Die Installation und Nutzung von nicht lizensierter Software ist gemäß dem Urheberrechtsgesetz nicht erlaubt und somit strafbar. Das schließt Kopien installierter Software solange dies nicht der Datensicherung dient mit ein.

4. Die Nutzung von öffentlichen Apps (Applikationen) auf mobilen Geräten, wie beispielsweise WhatsApp, Facebook etc. bedingt besonderer Sorgfalt. Die Übermittlung von geheimen und oder datengeschützten Informationen ist mit derartigen Apps strengstens untersagt.

5. Passwörter sind personalisiert und stets geheim. Eine Nutzung von identischen Passwörtern, die sowohl privat als auch betrieblich genutzt werden, ist verboten. Sie dürfen auch nicht innerhalb der Organisation z.B. zu Vertretungszwecken oder an Vorgesetzte weitergegeben oder öffentlich notiert werden. Damit dürfen auch nur Kundenportale und Kundenzugänge genutzt werden, für dessen Aufgabenstellung der Mitarbeiter berechtigt wurde. Ggfls. sind Berechtigungen beim Systemadministrator zu beantragen.

6. Passwörter sollten gemäß üblicher Sicherheitsanforderungen mindestens aus sechs Zeichen mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen, nicht numerisch oder alphabetisch nachfolgend sein und keinen Bezug zum Kontonamen oder Namen des Benutzers haben.

7. Die Nutzung des Internets ist nur hinsichtlich der Aufgabenerfüllung gestattet. Links sind entsprechend bewusst zu verwenden. Downloads sind hier vorab besonders auf sichere Herkunft und zwingend über den Virenschutz zu prüfen.

8. Die Berücksichtigung des Datengeheimnisses nach Maßgabe des §5 des Bundesdatenschutzgeheimnisses (BDSG) ist für jeden Arbeitnehmer verpflichtend. D.h. es ist jedem Arbeitnehmer untersagt, geschützte personen- und unternehmensbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben zugänglich zu machen oder sonst zu nutzen.

9. Daten müssen gemäß Berechtigung und vorgegebenen Prozessen seitens der Systemadministratoren hinsichtlich Verwendung, Sicherung und Schutz an den vorgegebenen Speicherplätzen verschlüsselt gespeichert werden. Lokale Speicherungen unterliegen nicht der Datensicherung und sind nur zu Ausnahmezwecken temporär erlaubt.

10. Fremde Daten von beispielsweise einem USB-Stick oder einer CD-ROM dürfen nur über eine vorgeschaltete Virenprüfung im Netzwerk abgelegt werden. Ggfls. ist der Systemadministrator / Datenschutzbeauftragte einzubeziehen.

11. Mobile Endgeräte und mobile Datenträger dürfen nur verschlüsselt und PIN-/passwortgeschützt außerhalb des Unternehmens verwendet werden. Bei Verbindung mit dem Firmennetzwerk ist die Verschlüsselungspflicht über Gruppenrichtlinien administrativ voreingestellt. Bei der Nutzung mobiler Endgerät und Datenträger ist zwingend darauf zu achten, dass niemand oder nur befugte Personen anwesend sind und somit keine unbefugte Person geschützte Informationen einsehen kann.

12. Kundenvorgaben hinsichtlich der Versendung, Verwendung und Speicherung von Daten sind gemäß Kundenvorgaben und den Lieferantenvereinbarungen, der Projektvorgaben und verlinkten Datenschutzrichtlinien einzuhalten. Vorgaben und Prozesse sind einzuhalten. Sind diese Prozesse in der Schönek Gruppe nicht installiert, muss der Datenschutzbeauftragte sowie der Systemadministrator vom Mitarbeiter mit einbezogen werden.

13. Sollte der Arbeitnehmer den Arbeitsplatz oder das EDV- / Kommunikationsmittel während der Aufgabenerledigung verlassen, so muss das jeweilige Gerät vor nicht autorisierter Nutzung gesperrt werden (klassische Sperre: Windows-Taste + L) – Passwortsperre, PIN-Aktivierung, oder andere geeignete Werkzeuge sind verpflichtend.

14. Bei Reisetätigkeiten sind die mobilen Datenträger, Laptops grundsätzlich im Handgepäck zu transportieren.

15. Nicht mehr verwendete EDV- / Kommunikationsmittel müssen professionell gelöscht, überschrieben oder zerstört werden, dass eine Wiederverwendung der Daten und Geräte nicht mehr möglich ist. Erst dann dürfen sie auch entsorgt werden. Die Organisation erfolgt über den EDV-Verantwortlichen, sowie auch in diesem Fall durch beauftragte Mitarbeiter eines Dienstleisters, beispielhaft aufgeführt der MS Solutions Informationssysteme GmbH und der Herrmann Datensysteme GmbH.

16. Sollten bei der Nutzung der internen EDV, der mobilen Endgeräte oder der mobilen Datenträger irgendwelche Fehlermeldungen, abnormen Funktionen oder andere Unregelmäßigkeiten festgestellt werden, die ggfls. auf eine Manipulation hinweisen könnten, so ist sofort jegliche Tätigkeit zu stoppen, sofern möglich alle externen Verbindungen zu unterbrechen und unmittelbar der EDV-Verantwortliche einzuschalten.

17. Der Systemadministrator sperrt nach dem Ausscheiden eines Mitarbeiters das persönliche Benutzerkonto zur Sicherung vor unberechtigten Zugriffen von betriebsfremden Personen. Das Benutzerkonto wird nach einer Frist von 3 Monaten endgültig durch den Systemadministrator gelöscht.

18. Für den Fall eines Verstoßes gegen einer dieser genannten Richtlinien zum Datenschutz und der EDV-Nutzung sind entsprechende Sanktionen im Unternehmen obligatorisch.

19. Diese Richtlinie zum Datenschutz und der EDV-Nutzung bleibt bestehen, solange und soweit sie nicht durch eine spätere schriftliche Richtlinie aufgehoben oder verändert wird.

20. Prozessbeschreibungen und Arbeitsanweisungen, die sich auf diese Richtlinie beziehen gelten verpflichtend.

Nittenau im Juli 2022
Schönek Gruppe

i. V. 

_____

Geschäftsleitung