Kundeninformation

Anspruch auf Aushändigung einer vollständigen und aktuellen Systemdokumentation

IT-Dienstleister sind durch gesetzlich formulierte Anforderungen verpflichtet, im Rahmen ihrer Leistungserbringung die IT-Systemdokumentation in einer für Dritte nachvollziehbaren Lesart und in zeitnaher Aktualität an die Auftraggeber auszuhändigen.

Der Auftraggeber (Verantwortlicher / Eigentümer des IT-Systems) ist nicht nur Eigentümer dieser Dokumentation, sondern auch gegenüber Dritten nachweispflichtig. Die IT-Dokumentation ist Bestandteil dieser Nachweis-Dokumente.

Gleichzeitg bildet die IT-Systemdokumentation die Basis für die vertrags- und qualitätsgerechte Leistungserbringung durch den Dienstleister am IT-System des Auftraggebers.

Bei der IT-Dokumentation sollte eine Separierung in einen „technischen" und einen „sensiblen" Teil erfolgen.

Der technische Teil beinhaltet die Beschreibung und den Netzplan der IT-Infrastruktur, einschließlich der Konfigurationsparameter.

Der sensible Teil enthält die jeweiligen Zugangsdaten zur Verwaltung der Mitarbeiterkonten sowie der Administration der Hard- und Softwarekomponenten. Dieser Teil ist durch den Auftraggeber sicher (z. B. in einem Safe) zu verwahren.

Die Anforderungen zur Aushändigung der Dokumentation an den Auftraggeber ergeben sich aus einschlägigen Gesetzen:

- aus der Verantwortung (Pflicht) eines Geschäftsführers gemäß **KonTraG, GmbHG**,**HGB** insbesondere zur Abwendung von Schäden für die Gesellschaft durch Pflege einer Verfahrensdokumentation, Ergreifung von Maßnahmen zur IT-Sicherheit und Schaffung einer besseren Transparenz
- aus den Anforderungen zum Schutz von Geschäftsgeheimnissen gemäß **GeschGehG**
- aus den Anforderungen der **EU-DSGVO**, insbesondere der Ergreifung von technischen und organisatorischen Maßnahmen zur Realisierung der Gewährleistungsziele
- flankierend aus den vom BSI empfohlenen Maßnahmen aus dem **ITSicherheitsgesetz** zur Erhöhung der Informationssicherheit

sowie auch der **GoBD** (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff)

Bezug nehmend auf die EU-DSGVO ergibt sich die Erfordernis zur Dokumentation (**Gewährleistungsziel „Transparenz"**) im Verantwortungsbereich des Verantwortlichen (Auftraggebers) aus dem Schutzauftrag gegenüber Betroffenen, deren personenbezogene Daten verarbeitet werden:

- **Art. 32** (Sicherheit der Verarbeitung), Ergreifen von technischen und organisatorischen Maßnahmen gegen unbefugte Zugriffe durch Dritte
- **Art. 5** (Grundsätze für die Verarbeitung personenbezogener Daten) sowie **Art. 24** (Verantwortung des für die Verarbeitung Verantwortlichen) zum Nachweis der Einhaltung
- **Art. 25** (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) zum Nachweis, dass die IT-Umgebung den aktuellen Schutzanforderungen entsprechen und die Zugriffsrechte die Vertraulichkeit der Daten gewährleisten.

Der Datenschutz betrachtet 7 Gewährleistungsziele, die durch die Ergreifung entsprechender technischer und organisatorischer Maßnahmen zu erreichen sind. Anbei beilspielhaft Inhalte, die eine aussagefähige Dokumentation erfordern.

Auszugsweise!: (aufgeführte Punkte unter den Gewährleistungszielen sind nicht vollständig!)

„Datenminimierung"

- Reduzierung des Umfangs der erfassten und verarbeiteten Daten sowie der Anzahl des am Verarbeitungsprozess beteiligten Personen (Kenntnisnahme)
- Implementierung von Sperr- und Löschroutinen
- Regeln zur Kontrolle der Einhaltung

„Verfügbarkeit"

- Anfertigung von Sicherheitskopien (Datensicherungskonzept)
- Schutz vor äußeren Einflüssen (Strom, Wasser, Brand, Diebstahl, Cyber-Angriffe usw.)
- Redundanz von Hard- und Software sowie Infrastruktur

„ Integrität"

- Einschränkung von Schreib- und Änderungsrechten
- Dokumentierte Zuweisung von Berechtigungen (Berechtigungskonzept)
- Aktualität der Daten

„ Vertraulichkeit"

- Berechtigungen nach Erforderlichkeitsprinzip
- Authentisierungsverfahren
- Festlegung und Kontrolle zugelassener Ressourcen (Kommunikationskanäle)
- Schutz vor äußeren Einflüssen

„ Nichtverkettung"

- Einschränkung von Verarbeitung-, Nutzungs- und Übermittlungsrechten
- Trennung mittels Rollenkonzepten
- Maßnahmen zum Verbot von „Backdoors"

„Transparenz"

- Dokumentation von Verfahren (mit Darstellung der Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen)
- Protokollierung von Zugriffen und Änderungen
- Dokumentation von Verträgen mit internen Mitarbeitern und externen Dienstleistern

„Intervenierbarkeit"

- Dokumentierte Bearbeitung von Störungen

In abgewandelter Form finden diese hier benannten Maßnahmen Anwendung bei der Umsetzung der Anforderungen in den oben beschriebenen Gesetzen bzw. Grundsätzen.

Haben Sie Rückfragen zu dieser Information? Wir stehen Ihnen gern zur Verfügung.

COMMPACT GmbH
Gesellschaft für Informationstechnologie
COMMPACT GmbH
Gesellschaft für Informationstechnologie
Adolph-Kolping-Str. 6
17034 Neubrandenburg
www.commpact.de
@-Mail: info@commpact.de
Tel.: 0395 56 86 0
Fax: 0395 56 86 150