Leitlinie zum Schutz personenbezogener Daten und zur Informationssicherheit

Fassung vom 13.05.2020

Inhaltsverzeichnis

Präambel

Bei den Dienstleistungen der a.s.k. Datenschutz e.K. ist davon auszugehen, dass personenbezogene Daten erhoben und verarbeitet werden müssen sowie zur Sicherstellung der notwendigen Verfügbarkeit, Vertraulichkeit und Integrität ein angemessenes Informationssicherheitsniveau gewährleistet sein muss.

Geltungsbereich

Diese Leitlinie gilt für alle Mitarbeiter und zu erbringenden Leistungen der a.s.k. Datenschutz e.K. Aufgrund der Unternehmensstruktur und dezentralen mobilen Arbeitsweise entfällt die Angabe eines räumlichen Geltungsbereichs.

Grundlagen

Gemäß Artikel 4 Ziffer 1 der EU-Datenschutz-Grundverordnung (EU-DSGVO) sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der besondere Schutz personenbezogener Daten ist bereits seit dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15.Dezember 1983 verfassungsrechtlich verankert: Aus dem allgemeinen Persönlichkeitsrecht ergibt sich ein Recht auf informationelle Selbstbestimmung. Der Datenschutz bezweckt somit den Schutz des Einzelnen vor Beeinträchtigungen in seinem Persönlichkeitsrecht durch den angemessenen Umgang mit seinen personenbezogenen Daten.

Der Umgang mit personenbezogenen Daten in Umsetzung völkerrechtlicher Verpflichtungen ist ab dem 25. Mai 2018 in der EU-DSGVO geregelt, die in den europäischen Staaten und damit auch für die a.s.k. Datenschutz e.K. gilt. Damit obliegt es ihr die technischen und organisatorischen Maßnahmen zu treffen die erforderlich sind, um die Ausführung der EU-DSGVO zu gewährleisten.

Der Schutz sensitiver betrieblicher Daten, Informationen und Systeme ist ebenfalls eine zwingende Anforderung, obwohl dieser Bereich gesetzlich weniger explizit als der Datenschutz geregelt ist. Diese Anforderung ergibt sich vielfach aus vertraglichen und rechtlichen Verpflichtungen, darüber hinaus aber auch aus Eigeninteresse.

Ziele

Mit dieser Leitlinie zum Datenschutz und zur Informationssicherheit gibt sich die a.s.k. Datenschutz e.K. den Rahmen für den Umgang mit personenbezogenen Daten und den sicheren Betrieb der informationstechnischen Infrastrukturen, die für die Erfüllung der Organisationsaufgaben benötigt werden.

Die allgemeingültigen Sicherheitsziele sind:

- Vertraulichkeit, Verfügbarkeit, Integrität aller Informationen der Organisation zu gewährleisten
- Schutz gegen Angriffe aus dem Internet, die das interne Netzwerk gefährden, zu verhindern
- Geschäftsprozesse und Arbeitsabläufe dokumentieren
- Sichere und vertrauenswürdige Datenverarbeitung
- Erhalt der in die Technik, Arbeitsprozesse und Wissen investierten Werte
- Minimierung der möglichen Ausfallzeit und Schäden durch Systemausfälle
- Etablierung eines starken Bewusstseins für Informationssicherheit innerhalb der Organisation

Selbstverpflichtung

Die Geschäftsführung und die Mitarbeiter der a.s.k. Datenschutz e.K. sind sich ihrer Verantwortung bei der Erbringung Ihrer Leistungen und im Umgang mit den dafür eingesetzten informationstechnischen Infrastrukturen bewusst. Die Umsetzung von Datenschutz und Informationssicherheit hat einen hohen Stellenwert. Es werden alle notwendigen geeigneten und angemessenen Maßnahmen getroffen, um negative materielle und immaterielle Folgen für Betroffene und die a.s.k. Datenschutz e.K. auszuschließen.

Prinzipien

Der Umgang mit personenbezogenen Daten ist in der EU-DSGVO als **Verbot mit Erlaubnisvorbehalt** geregelt. Damit ist das Verarbeiten von personenbezogenen Daten grundsätzlich verboten. Ausnahmen bestehen nur, wenn ein Gesetz dies erlaubt oder der Betroffene einwilligt. Hieraus leitet die a.s.k. Datenschutz vier Prinzipien zur Umsetzung des Datenschutzes ab. Diese sind:

1. Die a.s.k. Datenschutz e.K. strebt bei allen ihren Arbeitsvorgängen an, die Verarbeitung von personenbezogenen Daten zu vermeiden (Prinzip der **Datenvermeidung).**

2. Soweit bei Arbeitsvorgängen die Verarbeitung von personenbezogenen Daten nicht vermieden werden kann, wählt die a.s.k. Datenschutz e.K. im Rahmen des technisch und organisatorisch Vertretbaren jeweils den Arbeitsvorgang, bei dem so wenig personenbezogene Daten wie möglich verarbeitet werden müssen (Prinzip der **Erforderlichkeit).**

3. Eine Verwendung von personenbezogenen Daten für einen anderen als den vorab festgelegten oder einem diesem besonders nahen Zweck ist ausgeschlossen. Ausnahmen ergeben sich nur, wenn ein Gesetz dies erlaubt oder der Betroffene einwilligt (Prinzip der **Zweckbindung).**

4. Bei allen Arbeitsvorgängen werden die gesetzlichen Löschfristen beachtet. Werden personenbezogene Daten nicht mehr benötigt, werden sie auch ohne Ausschöpfung der Löschfristen gelöscht (Prinzip der **Datenminimierung**).

Eine wirksame Umsetzung des Datenschutzes ist nur mit einer wirkungsvollen Informationssicherheit zu erreichen. Zudem folgen für die a.s.k. Datenschutz e.K. auch aus grundsätzlichen Erwägungen Anforderungen an die Informationssicherheit. Darum formuliert die a.s.k. Datenschutz e.K. neben den vier Prinzipien zur Umsetzung des Datenschutzes auch drei Prinzipien zur Umsetzung der Informationssicherheit. Diese sind:

1. Die Vermeidung von Unterbrechungen und Inkonsistenzen der für die a.s.k. Datenschutz e.K. eingesetzten informationstechnischen Infrastrukturen spielt eine maßgebliche Rolle bei der Durchführung der Arbeitsvorgänge und Erbringung der

Dienstleistungen gegenüber Kunden. Deswegen werden die von der a.s.k. Datenschutz genutzten informationstechnischen Infrastrukturen so betrieben, dass Ausfälle einzelner Komponenten toleriert werden können (Prinzip der **Verfügbarkeit und Fehlerfreiheit).**

2. Technische und organisatorische Maßnahmen stellen sicher, dass die Auswirkungen von Unregelmäßigkeiten in Daten oder Fehlfunktionen in informationstechnischen Infrastrukturen vermieden werden, nicht unbemerkt bleiben und zeitlich begrenzt werden (Prinzip der **Integrität).**

3. Der Schutz sensibler Daten und informationstechnischer Infrastrukturen wird dadurch gewährleistet, dass diese ausschließlich Berechtigten zugänglich gemacht werden (Prinzip der **Vertraulichkeit).**

Die a.s.k. Datenschutz e.K. erbringt ausschließlich Dienste, deren Informationssicherheits- und Datenschutzniveau entsprechend dieser sieben Prinzipien umgesetzt werden kann. Bei der Umsetzung der Prinzipien berücksichtigt sie ein wirtschaftlich vertretbares Verhältnis im Vergleich zum Wert der betreffenden Informationen und IT-Systeme.

Umsetzung

Die Umsetzung der Prinzipien zum Datenschutz und zur Informationssicherheit in den Arbeitsabläufen der a.s.k. Datenschutz e.K. erfordert technische und organisatorische Maßnahmen. Diese werden in den Richtlinien zum Management der Informationssicherheit und zum Datenschutzmanagement, den dort verankerten Prozessbeschreibungen und anderen Vorgaben geregelt.

Durch die Etablierung eines Datenschutzmanagementsystems (DSMS) und eines Informationssicherheitsmanagementsystems (ISMS) werden kontinuierliche Revisionen dieser Regelungen und deren konsequente Einhaltung für das angestrebte Datenschutz- und Informationssicherheitsniveau sichergestellt. Abweichungen werden unmittelbar mit dem Ziel analysiert, den Datenschutz und die Informationssicherheit zu verbessern und auf dem aktuellen Stand der Technik zu halten.

Da die Mitarbeiter der a.s.k. Datenschutz e.K. allesamt als zertifizierte Informationssicherheitsbeauftragte und Datenschutzbeauftragte ausgebildet sind und im Bereich Datenschutz keine Pflicht zur Benennung eines Datenschutzbeauftragten für die a.s.k. Datenschutz e.K. besteht, wurde auf die Benennung eines Datenschutzbeauftragten und eines Beauftragten für Informationssicherheit bewußt verzichtet.

In die Zuständigkeit jedes Mitarbeiters fallen somit auch Maßnahmen, um den Datenschutz und die Informationssicherheit in dessen Bereich umzusetzen, aufrecht zu erhalten und bei Bedarf an neue rechtliche, technische und organisatorische Gegebenheiten anzupassen. Die hierfür erforderlichen technischen, organisatorischen und personellen Voraussetzungen werden von der Geschäftsführung im Rahmen der Verhältnismäßigkeit geschaffen. Diese

trägt auch die Gesamtverantwortung für die Themen Datenschutz und Informationssicherheit.

Verpflichtung zur kontinuierlichen Verbesserung

Die Sicherheitskonzeption wird von der Geschäftsleitung jährlich auf Aktualität und Wirksamkeit geprüft und bei Bedarf angepasst.

Verstöße und Sanktionen

Alle Mitarbeiter sind gehalten, im Sinne dieser Leitlinie die Themen Datenschutz und Informationssicherheit aktiv zu unterstützen und zu fördern. Fehler sind menschlich und können passieren. Eine Verletzung von Informationssicherheitsrichtlinien oder Dienstanweisungen kann jedoch bei schuldhaftem Verhalten für einen Beschäftigten arbeitsrechtliche Konsequenzen, bis hin zur Kündigung nach sich ziehen. Grob fahrlässige oder vorsätzliche Verstöße können im Falle finanzieller Schäden die Haftung und damit zu Regressforderungen führen. Auch strafrechtliche Konsequenzen sind in einem solchen Fall nicht ausgeschlossen.

Geltungsdauer

Diese Leitlinie tritt mit Unterzeichnung in Kraft. Sie gilt, bis sie außer Kraft gesetzt oder durch eine neuere Fassung ersetzt wird. Sie wird nach Unterzeichnung allen Mitarbeitern zur Kenntnis gebracht.

Simmelsdorf, den 13. Mai 2020

Titel des Dokuments				**Vertraulichkeitsstatus**	
Leitlinie Informationssicherheit und Datenschutz				Öffentlich	
Version	**Datum**	**Änderungen**	**Autor**	**Status**	**Freigabe**
1.0	13.05.2020	Erstellung des Dokuments	Sascha Kuhrau	Final	-