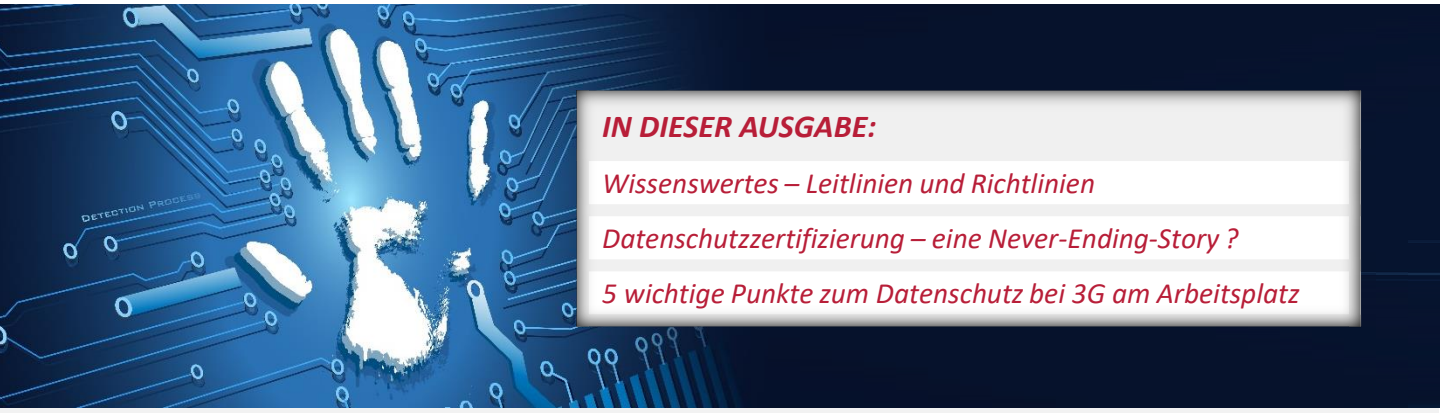

IN DIESER AUSGABE:

Wissenswertes – Leitlinien und Richtlinien

Datenschutzzertifizierung – eine Never-Ending-Story ?

5 wichtige Punkte zum Datenschutz bei 3G am Arbeitsplatz

Newsletter Februar 2022

Datenschutz

Liebe Leserinnen und Leser,

auch in diesem Jahr möchten wir Sie wieder zu relevanten und aktuellen Themen des Datenschutzes informieren. In unserer neuen Rubrik „Wissenswertes“ erläutern wir Ihnen einzelne Anforderungen der DS-GVO und hoffen, Ihnen so weitere Hilfestellungen für die Praxis zu geben.

Viel Spaß beim Lesen!

Ihre ANMATHO AG

Leitlinien und Richtlinien

Frei nach dem Motto „Tue Gutes und rede darüber“ werden die Unternehmen zu umfangreichen Dokumentationen verpflichtet. Die Dokumentationen sollen sicherstellen, dass sich das Unternehmen regelmäßig und im Detail mit seinen datenschutzrelevanten Themen beschäftigt und ein angemessenes und zweckdienliches Datenschutzniveau erreicht. Nicht unwesentlich ist dabei auch, dass die Aufsichtsbehörden bei Kontrollen oder bei der Aufklärung von Datenschutzvorkommnissen als Erstes genau diese Unterlagen einsehen wollen (Nachweispflicht).

Hinsichtlich der Dokumentationsvorgaben lassen sich zwei Richtungen unterscheiden.

1. Durch schriftliche Vorgaben der Unternehmensleitung (Vorgabedokumente) sollen die Datenschutz-Bedingungen des Unternehmens definiert und konkrete Vorgaben für das datenschutzkonforme Verhalten der einzelnen Beschäftigten im Umgang mit personenbezogenen Daten gemacht werden. Hierzu gehören vor allen Dingen Leitlinien, Richtlinien, Arbeitsanweisungen oder Verpflichtungserklärungen.
2. Die im Unternehmen festgestellten Risiken und daraus abgeleiteten Maßnahmen sind angemessen und konkret zu beschreiben (Systembeschreibungen). Hierzu gehören z.B. die Datenschutzfolgenabschätzungen und Verfahrensverzeichnisse für die einzelnen Verfahren aber auch schriftliche Festlegungen der Verantwortlichkeiten im Unternehmen, der vergebenen Zugriffsrechte, der Löschregelungen u.a.

Bleiben wir in dieser Ausgabe bei Punkt 1. - den Leitlinien und Richtlinien. Warum braucht man beides?

Die Erstellung von Leit- und Richtlinien ist das A und O, um das Datenschutzmanagement zu dokumentieren. Dabei geben Leitlinien, als „Herzstück“, die gesetzten Datenschutzziele der Unternehmensführung vor. Sie machen die Bedeutung des Datenschutzes für das Unternehmen deutlich und verpflichten die Belegschaft auf die Einhaltung der Datenschutzvorgaben. Die auf die Leitlinien aufbauenden Richtlinien setzen den Rahmen für die tatsächlichen Umsetzungsmaßnahmen.

Datenschutzzertifizierung – eine Never-Ending-Story ?

Seit Inkrafttreten der DS-GVO ist die Zertifizierung des Datenschutzes ein Thema. Aber bis heute, 4 Jahre später, gibt es noch keine akkreditierte Zertifizierungsstelle. Dies mag daran liegen, dass das Verfahren für eine Akkreditierung in Deutschland recht aufwändig ist. Zertifizierungsstellen können nur von der Deutschen Akkreditierungsstelle GmbH (DAkkS) zusammen mit den unabhängigen Datenschutzaufsichtsbehörden akkreditiert werden. Dabei muss jede Menge an Kriterien und Normen erfüllt werden. In diesem Jahr sollen nun aber die ersten Stellen den gesamten Prozess durchlaufen. Wir stellen Ihnen hier drei interessante Varianten der voraussichtlichen Zertifizierungsmöglichkeiten vor:

ISO 27701

Die ISO 27701 stellt eine Erweiterung der renommierten ISO 27001 um das Thema Datenschutz dar. Die Norm wurde im August 2019 veröffentlicht und wird nur zusammen mit der ISO 27001 zertifiziert werden. Informationssicherheit und Datenschutz werden so zusammen bewertet und Synergien genutzt. Bisher sieht es so aus, als würden die ersten Zertifizierungsstellen im ersten Halbjahr 2022 akkreditiert werden. Sollten Sie also bereits ISO 27001 zertifiziert sein, können Sie so mit wenig Aufwand den Datenschutz integrieren.

EuroPriSe – Zertifizierung der Auftragsdatenverarbeitung

EuroPriSe ist bekannt als ein privatwirtschaftliches Zertifikat für datenschutzkonforme IT-Produkte und IT-basierte Dienste. Der Fachpresse ist zu entnehmen, dass EuroPriSe bei der nordrhein-westfälischen Datenschutzaufsicht den Entwurf eines Kriterienkatalogs eingereicht hat, der sich auf die Auftragsdatenverarbeitung konzentriere. Die Behörde habe dazu wohl bereits grünes Licht gegeben, so dass in 2022 nun die weiteren Schritte im Akkreditierungsprozess anlaufen könnten.

Essener TÜV Informationstechnik GmbH (TÜViT) - Zertifizierung von informationsverarbeitenden Systemen

Nach Aussage der Essener TÜV Informationstechnik GmbH (TÜViT) wurde unter dem Arbeitstitel „Zertifizierung von informationsverarbeitenden Systemen gemäß Art. 42, 43 EU-DSGVO“, ein Zertifizierungsprogramm entwickelt, das Kriterien und Verfahren für eine Datenschutz-Zertifizierung nach Art. 42 DS-GVO enthält. Das Programm liege derzeit der DAkkS zur Fachprüfung vor. Wenn von Seiten der DakkS das „Go“ kommt, kann eine Genehmigung der Zertifizierungskriterien durch die zuständige Aufsichtsbehörde eingeholt werden. Damit könnte die TÜViT dann eine DS-GVO-Zertifizierung für die Datenverarbeitung durch informationsverarbeitende Services anbieten.

Nach unseren Einschätzungen wird die Zertifizierung der ISO 27701 als erstes die Ziellinie überqueren.

5 wichtige Punkte zum Datenschutz bei 3G am Arbeitsplatz

1. Zur Prüfung des Impfstatus bei „Geimpften“ und „Genesenen“ reicht eine einmalige Prüfung und der Eintrag in einer entsprechenden Prüfungsliste sollte sich auf Namen, Status und Gültigkeitsdauer sowie Prüfzeitpunkt beschränken.
2. Das Infektionsschutzgesetz (IfSG) stellt die notwendige Rechtsgrundlage für die Prüfung und Dokumentation des Impfstatus dar (Art. 6 Abs. 1c DS-GVO). Eine konkrete Einwilligung der Betroffenen ist nicht erforderlich.
3. Es dürfen keine Kopien von Nachweisen vom Arbeitgeber angefertigt und abgelegt werden.
4. Die Informationen zu und über den Impfstatus der Beschäftigten unterliegen als Gesundheitsdaten gemäß Art. 9 DS-GVO den Schutzvorschriften der DS-GVO: Der Kreis der zugriffsberechtigten Personen auf diese Daten ist daher unbedingt auf das notwendige Mindestmaß zu beschränken.
5. Die Bekanntgabe des Impfstatus eines Beschäftigten an andere Beschäftigte durch den Arbeitgeber ist aufgrund der Verschwiegenheitsverpflichtungen nicht erlaubt.

Wenn Sie Interesse an weiteren Informationen zu den vorgestellten Themen haben, wenden Sie sich gern an Ihren Daten-schutzbeauftragten der ANMATHO AG oder an info@anmatho.de.