Datenschutz

Praxisnahe Hilfe für die DSGVO

[03.05.2018] Speziell für kleinere Behörden hat das Sicherheitsinstitut VdS Richtlinien zur praxisgerechten Umsetzung der Datenschutz-Grundverordnung herausgebracht. Welche Hilfe diese konkret bieten, beschreibt Markus Edel, Leiter des Bereichs Cyber-Security bei VdS.

Herr Edel, in vielen Behörden herrscht Irritation angesichts der neuen Datenschutz-Grundverordnung (DSGVO), die zum 25. Mai dieses Jahres vollständig umgesetzt sein muss. Können Sie uns bezüglich dieser Verordnung ein wenig aufklären?

Die Datenschutz-Grundverordnung soll einen europaweit einheitlichen Standard schaffen. Die Auswirkungen des fast 300 Seiten starken Werks auf Organisation und IT gerade von kleineren Dienststellen sind tiefgreifend – auf die ab dem 25. Mai geltende Rechtslage sind viele Behörden und auch viele der betroffenen Unternehmen nicht vorbereitet. Das ist riskant, da zum Stichtag bei Zuwiderhandlung hohe Bußgelder von bis zu 20 Millionen Euro drohen.

Was genau kommt hier auf die Behörden zu?

Die wohl gravierendste Neuerung gegenüber der jetzigen Rechtslage ist die so genannte Rechenschaftspflicht. Sie fordert: Jede Behörde muss jederzeit klar nachweisen können, dass sämtliche Vorgaben der DSGVO eingehalten werden. Das können Institutionen nur auf eine Art leisten: Durch das Einrichten eines Datenschutz-Management-Systems. Das ist ein Führungssystem, kein technisches Hilfsmittel – kann allerdings durch ein solches abgebildet werden. Nötig wird ein Regelrahmenwerk mit klar definierten Leit- und Richtlinien, Prozessen, Rollen und Verantwortlichkeiten sowie Kontrollmechanismen, auch mit prüffähiger Dokumentation und klarer Kommunikation. In praxisgerechte Vorgaben übersetzt wird der umfassende DSGVO-Umsetzungsprozess durch die neuen und kompakten Richtlinien 10010 der VdS Schadenverhütung. Gerade kleinere Behörden sagen, dieser präzise Management-System-Ansatz mache die EU-Forderungen für sie überhaupt erst anwendbar.

Was zeichnet die Richtlinien aus?

VdS-Richtlinien setzen schon seit Jahrzehnten Sicherheitsstandards und sind vor allem für ihre Praxisnähe sowie die Konkretheit der Hilfestellungen bekannt. Die neue VdS-Publikation zeigt Behörden einen Weg auf, die rechtlichen, organisatorischen und technischen Anforderungen der DSGVO so strukturiert wie möglich umzusetzen – und das mit überschaubarem Aufwand. Die 10010-Richtlinien beschreiben ein auditier- und zertifizierfähiges Datenschutz-Management-System, präzise zugeschnitten speziell für die zahlreichen kleineren Dienststellen.

„Wir wollen deutlich machen: Datenschutz ist kein reines IT-Thema, sondern Chefsache.“
Wie genau funktioniert der Leitfaden?

Die Richtlinien VdS 10010 präzisieren alle notwendigen Ressourcen zur Erfüllung der Datenschutz-Grundverordnung auf nur 32 Seiten und geben klar definierte Rollen und Verantwortlichkeiten vor. Generell adressiert der Leitfaden die oberste Behördenleitung. Wir wollen deutlich machen, dass Datenschutz keinesfalls ein reines IT-Thema, sondern Chefsache ist. Konkret heißt das: Die zentrale

Verantwortung für die Umsetzung des geforderten DSGVO-Niveaus trägt die oberste Behördenleitung. Zentraler Ansprechpartner für alle Belange zum Thema ist der Datenschutzbeauftragte (DSB) der Behörde, an ihn wenden sich betroffene Personen, Behördenmitarbeiter und übergeordnete Aufsichtsstellen. Er überwacht die Einhaltung der EU-Vorschriften. Zu seiner Unterstützung sehen die VdS-Richtlinien 10010 einen Datenschutz-Manager (DSM) vor. Dieser initiiert, plant und steuert die Implementierung des Datenschutz-Management-Systems und setzt es um. Unterstützt wird er dabei von einem Datenschutz-Team: Ein Gremium, das neben dem Vertreter der Behördenleitung sowie dem Datenschutzbeauftragten und/oder dem Datenschutz-Manager auch aus dem IT-Verantwortlichen und Mitarbeitervertretern besteht. Sinnvoll kann außerdem die Teilnahme von Vertretern der Abteilungen Recht, Personal, Finanzen und weiterer operativer Einheiten sein.

Warum halten Sie den Einsatz eines solchen Datenschutz-Teams für sinnvoll?

Das Gremium ist wichtig, da seine Zusammensetzung die Berücksichtigung möglichst vieler Interessen innerhalb der Behörde sicherstellt. Unsere fast 25-jährige Erfahrung mit Management-Systemen belegt: Verstehen Mitarbeiter das Veränderungsziel und haben den Eindruck, dass sie aktiv mitwirken können, agieren sie meist proaktiv und stehen hinter den geplanten Veränderungen. Sie werden dann zu werbenden Multiplikatoren, was in der Belegschaft die Akzeptanz für den Datenschutz erhöht.

Welche Hilfestellungen umfasst der Leitfaden 10010 konkret und wie ist er aufgebaut?

Die Richtlinien zum Datenschutz regeln behördenindividuelle Grundsätze der Datenverarbeitung nach DSGVO: Rechtmäßigkeit, Zweckbindung, Richtigkeit, Treu und Glauben, Verhältnismäßigkeit, Transparenz, Datenminimierung, Vertraulichkeit, Verfügbarkeit und Integrität, Speicherbegrenzung, Nachweisbarkeit. Zudem präzisieren die Richtlinien 10010 Verfahren, um die von der DSGVO geforderten Prozesse sicherzustellen – unter anderem für die Wahrung von Betroffenenrechten, die Sensibilisierung von Mitarbeitern, das Erstellen und Pflegen des Verarbeitungsverzeichnisses, das Vertragsmanagement, die Durchführung der Risikoanalyse und der Datenschutz-Folgenabschätzung. Die VdS 10010 orientieren sich an unserem prämierten Informationssicherheits-Management-System VdS 3473. Ein Fokus liegt auf klarer und eindeutiger Sprache. So sind zwingend benötigte Anforderungen immer mit großgeschriebenem „MUSS“ gekennzeichnet. Mit großem „SOLLTE“ markierte Punkte stellen Empfehlungen dar, die für eine Zertifizierung nicht relevant sind. Sehr hilfreich dürfte zudem der kostenlose Quick-Check sein, mit dem Behörden nach 26 kompakten Fragen ihren individuellen Umsetzungsstatus bestimmen können und, wo nötig, erste Optimierungshilfen erhalten.

Welche weitere Hilfe kann VdS den Kommunen bieten?

Wird, insbesondere in kleineren Behörden, unterstützende Fachkunde auf dem Gebiet des Datenschutzes benötigt, so empfiehlt sich die Einbeziehung qualifizierter Dienstleister. Ein entsprechendes VdS-Anerkennungsverfahren für Datenschutz-Management-System-Berater haben wir vor Kurzem etabliert. Die ersten speziell von VdS ausgebildeten und zertifizierten Experten können die Behörden bei Bedarf bereits unterstützen.

Wie geht es für die Behörden nach dem 25. Mai weiter?

Wir werden in Kürze konkret sehen, welche Anforderungen die Aufsichtsbehörden an die Umsetzung der DSGVO stellen. In der Folge wird es dann wohl auch zu Präzisierungen in der Verordnung kommen. Natürlich werden unsere Experten die VdS-Hilfestellungen immer aktuell anpassen und auch die Überarbeitungen weiterhin kostenlos zur Verfügung stellen. Übrigens bieten wir für interessierte Behörden

auch die Zertifizierung ihres Datenschutzes nach VdS 10010 an.

()

Dieser Beitrag ist in der Ausgabe Mai 2018 von Kommune21 im Schwerpunkt Datenschutz erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Datenschutz, DSGVO