MOORE STEPHENS

5-Minuten-Check Datenschutz

Die neue EU-Datenschutzgrundverordnung (DSGVO) muss zum 25. Mai 2018 in Ihrem Unternehmen umgesetzt sein. Wer sich nicht bald mit der völlig neuen Gesetzeslage auseinandersetzt, wird durch den zeitlichen Aufwand der Umsetzung in Bedrängnis geraten. Machen Sie unseren Datenschutz Quick-Check, um herauszufinden, wie gut Ihr Unternehmen für die DSGVO aufgestellt ist: Besteht akuter Handlungsbedarf? Ist Ihre Umsetzung praktikabel?

1. Haben Sie einen (internen oder externen) Datenschutzbeauftragten bestellt?

i Wenn kein Datenschutzbeauftragter bestellt ist, sind Sie verpflichtet, jedes Verfahren der automatisierten Verarbeitung personenbezogener Daten (z.B. eine elektronische Zeiterfassung oder elektronisch geführte Zeit- und Urlaubskonten Ihrer Mitarbeiter) dem Landesdatenschutzbeauftragten zu melden, soweit mehr als neun Mitarbeiter mit personenbezogenen Daten beschäftigt sind. Da praktisch jeder Mitarbeiter mit personenbezogenen Daten beschäftigt ist, aber sicherlich niemand laufend mit dem Landesdatenschutzbeauftragten kommunizieren mag, ist die Bestellung eines (internen oder externen) Datenschutzbeauftragten bei mehr als neun Mitarbeitern zu empfehlen. Aufgabe des Datenschutzbeauftragten ist es, in einer Organisation die Einhaltung des Datenschutzes sicherzustellen.

Punkte

(10) Ja, wir haben einen externen Datenschutzbeauftragten bestellt.

(5) Ja, wir haben einen internen Datenschutzbeauftragten bestellt.

(0) Nein, wir haben keinen Datenschutzbeauftragten.

2. Verfügen Sie über eine aktuelle, vollständige und nachvollziehbare Systemdokumentation Ihrer IT?

i Die Systemdokumentation umfasst Erklärungen, mit deren Hilfe im Vertretungsfall Mitarbeiter Ihr System bedienen/aufgetretene IT-Probleme beseitigen können. Sie benötigen diese auch für die Zwecke der GoBD.

Punkte

(10) Ja, eine aktuelle, vollständige und nachvollziehbare Systemdokumentation ist vorhanden.

(5) Ja, eine Systemdokumentation liegt vor, müsste jedoch hinsichtlich Aktualität, Vollständigkeit und/oder Nachvollziehbarkeit optimiert werden.

(0) Nein, es ist keine Systemdokumentation vorhanden.

3. Verfügen Sie über aktuelle Verfahrensübersichten/ Verfahrensverzeichnisse und werden diese permanent gepflegt?

i Die Verfahrensübersicht bzw. das Verfahrensverzeichnis dokumentiert den Umgang mit und die Speicherung von personenbezogenen Daten. Bitte beachten Sie, dass z.B. auch in Outlook oder in Ihrem normalen Schriftverkehr zahlreiche personenbezogene Daten enthalten sind. Geraten Sie aus irgendeinem Grunde in das Blickfeld der Datenschutzbehörden - z.B. weil ein übelwollender Mitarbeiter Sie anschwärzt - und Sie können trotz der gesetzlichen Verpflichtung noch nicht einmal ein rudimentäres Verfahrensverzeichnis vorlegen, droht Ihnen ein erhebliches Bußgeld. Auch die GoBD verlangen, dass Sie eine entsprechende Verfahrensdokumentation vorlegen können.

Punkte

(10) Ja, eine aktuelle und permanent gepflegte interne und externe Verfahrensübersicht bzw. ein Verfahrensverzeichnis liegen vor.

(5) Ja, eine Verfahrensübersicht bzw. ein Verfahrensverzeichnis liegt vor, müsste allerdings ergänzt und/oder aktualisiert werden.

(0) Nein, eine Verfahrensübersicht bzw. ein Verfahrensverzeichnis ist nicht vorhanden.

4. Haben Sie den Zweck und die Rechtsgrundlage für die Bearbeitung von personenbezogenen Daten definiert und dokumentiert?

i Der Zweck für die personenbezogene Datenverarbeitung muss so präzise wie möglich definiert sein; gegebenenfalls muss eine Abwägung zwischen den schutzwürdigen Interessen der betroffenen Personen und denen des Unternehmens dokumentiert werden.

Punkte

(8) Ja, Zweck und Rechtsgrundlage für unsere personenbezogene Datenverarbeitung sind präzise definiert und dokumentiert.

(4) Unsere Zweckdefinition für die personenbezogene Datenverarbeitung und/oder unsere Rechtsgrundlage entsprechen möglicherweise nicht den datenschutzrechtlichen Anforderungen.

(0) Nein, Zweck und/oder Rechtsgrundlage für unsere personenbezogene Datenverarbeitung sind nicht definiert bzw. dokumentiert.

5. Jedermann hat das Recht, bei Ihnen abzufragen, welche personenbezogenen Daten über ihn bei Ihnen gespeichert wurden. Was könnten Sie, wenn ein solches Auskunftsverlangen gestellt würde, ohne großen Aufwand kurzfristig zur Verfügung stellen?

i Viele Unternehmen übersehen, wie weit die Auskunftsrechte gehen. Bereits nach geltender Rechtslage müssen nicht nur die gespeicherten Stammdaten aus Kommunikations-, Zahlungs-, CRM- und ERP-Programmen mitgeteilt werden, sondern auch Daten über die betreffende Person aus allen elektronisch durchsuchbaren Dateien (dies sind letztlich u.a. alle mit Word-, Excel- und sonstigen Office-Anwendungen erstellten sowie alle PDF-Dateien). Fast jedes Dokument enthält aber in Form der postalischen Anschrift etc. personenbezogene Daten. Ab dem kommenden Jahr tritt eine signifikante Verschärfung ein, da Sie dann auch mitteilen müssen, welche Daten über die betreffende Person Sie (nur) in Papierform in laufenden und archivierten Akten gespeichert haben (gilt bereits jetzt - aber handhabbar - für Personalakten). Entsprechende Auskunftsverlangen werden in der Praxis überwiegend von Personen gestellt, die Streit mit Ihnen haben/vorbereiten oder in Zusammenhang mit Presserecherchen.

Punkte

(10) Wir können ohne großen Aufwand nicht nur Stammdaten, sondern auch die personenbezogenen Daten aus allen elektronischen und Papierakten, laufenden Akten wie archivierten Akten, zur Verfügung stellen.

(7) Wir können ohne großen Aufwand die Stammdaten und die personenbezogenen Daten des Anfragenden aus diversen, aber nicht allen elektronischen Daten herausfiltern. Die entsprechenden Daten in unseren Papierakten zu finden, ist kaum möglich.

(0) Wir können mit vertretbarem Aufwand nur die Stammdaten und gegebenenfalls die Outlook-Kontaktdaten zur Verfügung stellen.

6. Haben Sie Dritten, z.B. Dienstleistern, Zugriff auf personenbezogene Daten eröffnet? Falls ja: Liegen hierfür Verträge zur Auftragsdatenverarbeitung vor?

i Eine Auftragsdatenverarbeitung (ADV) liegt nicht erst vor, wenn Sie Daten „nach außen" an einen Dritten zur Verarbeitung geben (z.B. an ein Rechenzentrum), sondern bereits dann, wenn Sie Dritten im Rahmen eines Softwarepflegevertrags oder einem externen IT-Administrator den Zugriff auf Ihr Netz, z.B. durch Fernwartung, erlauben.

Punkte

(6) Ja, unsere Auftragsdatenverarbeitung ist flächendeckend gemäß § 11 BSDG vertraglich geregelt.

(3) Ja, es liegen für die meisten Externen, die Zugang zu unserem Netz haben, vertragliche Auftragsdatenverarbeitungs-Verträge vor, die den Anforderungen des § 11 BSDG entsprechen.

(0) Nein, es sind keine vertraglichen Regelungen zur Auftragsdatenverarbeitung vorhanden.

7. Haben Sie eine aktuelle Sicherheitsrichtlinie und wird deren Einhaltung überwacht?

i Die Sicherheitsrichtlinie definiert den erstrebten nicht unbedingt perfekten Sicherheitszustand der EDV. Wer personenbezogene Daten erhebt, speichert oder verarbeitet, muss durch technische und organisatorische Maßnahmen sicherstellen, dass Dritte darauf nicht Zugriff nehmen. Ein dokumentiertes Sicherheitskonzept verlangen auch die GoBD.

Punkte

(10) Ja, eine aktuelle, verbindliche, betriebsübergreifende Sicherheitsrichtlinie liegt vor. Ihre Einhaltung wird rhythmisch überwacht.

(5) Ja, wir haben eine Sicherheitsrichtlinie, die gegebenenfalls ergänzt und aktualisiert werden müsste.

(0) Nein, eine Sicherheitsrichtlinie ist nicht vorhanden.

8. Verfügen Sie über allgemeine Richtlinien für die private Nutzung von Internet und E-Mail-Diensten und wird deren Einhaltung überwacht?

i Wenn in Ihrem Hause die private Nutzung der E-Mail-Accounts erlaubt ist, bedarf es relativ komplizierter Mechanismen, um bei Urlaub, Krankheit oder Verdacht rechtswidrigen Verhaltens auf die E-Mails des betreffenden Mitarbeiters zugreifen zu können, ohne gegen Datenschutz-Vorschriften zu verstoßen. Wenn Sie Pech haben, kündigen Sie einem Mitarbeiter, weil er sich per E-Mail mit einem Kollegen verabredet hat, sich krank zu melden, um dessen Haus zu renovieren, dringen mit der Kündigung aber nicht

durch, weil Sie auf diese E-Mail nicht hätten zugreifen dürfen. Stattdessen verhängt der Landesdatenschutzbeauftragte ein Bußgeld gegen Sie, weil Sie private E-Mails ausgelesen haben. Die GoBD verlangen solche Richtlinien nicht ausdrücklich; zum Teil setzen die GoBD aber die Existenz solcher Richtlinien voraus.

Punkte

(8) Ja, wir verfügen über detaillierte Richtlinien für die Nutzung von Internet und E-Mail-Diensten, die sauber zwischen dienstlicher und privater Sphäre trennen. Die Einhaltung dieser Richtlinie wird auch stichprobenartig überwacht.

(4) Ja, wir haben Regeln zur Nutzung von Internet- und E-Mail-Diensten, die allerdings noch nicht verbindlich definiert und dokumentiert sind/wir überwachen die Einhaltung dieser Richtlinie aber nicht.

(0) Nein, bei uns existiert keine Regelung zur Nutzung von Internet- und E-Mail-Diensten.

9. Verfolgen Sie das Prinzip der Datensparsamkeit und werden diese nach Ablauf der Aufbewahrungsfristen gelöscht?

i Sie dürfen personenbezogene Daten nur in dem Umfang erheben, speichern und verarbeiten, wie sie wirklich benötigt werden. Zu den verschiedenen Datenkategorien müssen Fristen festgelegt sein, nach deren Ablauf die Daten gelöscht werden. Die datenschutzrechtlichen Fristen sind erheblich kürzer als die steuerlichen Aufbewahrungsfristen.

Punkte

(6) Ja, wir leben das Prinzip der Datensparsamkeit und Aufbewahrungsfristen werden beachtet.

(3) Unsere personenbezogene Datenerfassung müsste gegebenenfalls optimiert bzw. Aufbewahrungsfristen definiert und kontrolliert werden.

(0) Nein, wir haben uns bislang noch nicht mit dem Prinzip der Datensparsamkeit und den Aufbewahrungsfristen befasst.

10. Verfügen Sie über ein detailliertes Datensicherungskonzept, das eine Datensicherung für mindestens ein Jahr vorsieht?

i Mit der regelmäßigen Durchführung einer Datensicherung wird der Erhalt des Datenbestands sichergestellt. Dies kann für Ihr Unternehmen lebenswichtig sein. Solche Maßnahmen verlangen auch die GoBD.

Punkte

(10) Ja, unser detailliertes Datensicherungskonzept ist für einen Zeitraum von mindestens einem Jahr ausgelegt.

(5) Unser Datensicherungskonzept ist zeitlich und/oder inhaltlich weiter zu definieren.

(0) Nein, wir verfügen über kein Datensicherungskonzept.

11. Blicken wir auf Ihre IT-Sicherheitsmaßnahmen: Sind diese aktuell? Kann man mit diesen den Netzwerkverkehr überwachen, filtern und protokollieren? Können die Daten zur Kontrolle archiviert werden?

i Bitte beachten Sie, dass IT-Sicherheitsprogramme immer auf dem aktuellen Stand sein müssen und regelmäßig aktualisiert werden müssen - in Ihrem eigenen Interesse, aus steuerlichen Gründen (GoBD) und aus datenschutzrechtlichen Gründen.

Punkte

(10) Ja, unsere IT-Sicherheitsprogramme erfüllen alle geforderten Anforderungen.

(5) Unsere IT-Sicherheitsmaßnahmen werden auf dem aktuellen Stand gehalten. Sie sind aber wahrscheinlich nicht lückenlos.

(0) Nein, unsere IT-Sicherheitsprogramme weisen bekanntermaßen Mängel auf.

12. Werden bei Ihnen vertrauliche Daten sowie gefährdete Systeme wie z.B. Notebooks oder private Geräte Ihrer Mitarbeiter (Smartphones, Tablets etc.) durch Verschlüsselung oder andere Maßnahmen geschützt?

i Sicherheitsmaßnahmen wie z.B. Verschlüsselung bieten Schutz vor Bedrohungen aus dem Internet sowie Diebstahl und sind schnell installiert.

Punkte

(10) Ja, unsere IT-Systeme und sensible Daten sind durch Sicherheitsmaßnahmen geschützt, auch vor Malware auf privaten Geräten der Mitarbeiter.

(5) Unsere Sicherheitsmaßnahmen weisen noch Lücken auf, die sensiblen Daten und kritischen Systeme sind aber geschützt.

(0) Nein, wir verwenden keine Sicherheitsmaßnahmen.

13. Sind Ihre zentralen IT-Systeme in geschützten Räumen angesiedelt, zu denen nur berechtigte Personen Zutritt haben? Kann nachvollzogen werden, welche Person wann Zutritt hatte?

Ein festgelegtes Regelwerk stellt die Zutrittskontrolle sicher, um unbefugten Zutritt zu den zentralen IT-Systemen zu vermeiden. Haben Sie ein solches Regelwerk nicht, verstoßen Sie gegen Datenschutzrecht wie auch Ihre ureigensten Sicherheitsinteressen. Ein solches Regelwerk und seine Dokumentation verlangen die DSGVO als auch die GoBD.

Punkte

(10) Ja, unsere zentralen IT-Systeme sind in geschützten Räumen mit Zutrittskontrolle und -protokollierung gesichert.

(5) Die räumliche Ansiedlung unserer zentralen IT-Systeme bzw. der Zutritt zu diesen ist noch nicht einwandfrei gesichert.

(0) Unsere zentralen IT-Systeme befinden sich nicht in einem geschützten Raum bzw. es existiert keine Zutrittskontrolle.

14. Verfügen Sie über ein abgestuftes Berechtigungs- und Zugriffskonzept für Benutzer und Gruppen?

Das Berechtigungs- und Zugriffskonzept definiert die Zugriffsrechte einzelner Nutzer und können auf Dateien oder Ordner angewandt werden. Das ist ein Thema des Datenschutzes, noch stärker aber der GoBD.

Punkte

(10) Ja, wir haben ein Berechtigungs- und Zugriffskonzept/Unser Unternehmen ist so klein, dass ein gestuftes Berechtigungskonzept nicht realisierbar ist.

(5) Unser Berechtigungs- und Zugriffskonzept, insbesondere die Löschung oder unautorisierte Verschlüsselung von Daten, müsste ergänzt bzw. aktualisiert werden. Es bietet aber einen Basisschutz.

(0) Nein, ein Berechtigungs- und Zugriffskonzept ist nicht vorhanden.

Bitte zählen Sie Ihre Punkte zusammen!
Ihr Ergebnis:

Mehr als 100 Punkte

Sie sind für die DSGVO überdurchschnittlich gut vorbereitet! Möglicherweise übererfüllen Sie manche Anforderungen und Sie könnten mit einem Zurückschrauben des Niveaus den betrieblichen Alltag erleichtern/Kosten sparen.

Zwischen 70 und 100 Punkten

Es besteht kein Grund in Hektik zu verfallen. In den Bereichen, in denen Sie unterdurchschnittlich gepunktet haben, sollten Sie bei Gelegenheit das Niveau weiter hochziehen. Bereiche, in denen Sie null Punkte erzielt haben, sollten Sie allerdings bald nachziehen.

Weniger als 70 Punkte

Es besteht akuter Handlungsbedarf. Existentielle Unternehmensprozesse sind nicht vernünftig abgesichert oder Sie verstoßen massiv gegen das Datenschutzrecht.

Wenn Sie nicht der Unternehmensinhaber sind: Denken Sie daran, dass die Einhaltung angemessener IT-Sicherheitsstandards und datenschutzrechtlicher Vorschriften Ihre Pflicht als Geschäftsführer ist. Betreiben Sie Eigensicherung und setzen Sie sich nicht unnötig persönlicher Haftung aus. Zumindest ein durchschnittliches Niveau sollten Sie sich erstellen.

Unser Team unterstützt Sie gerne bei der praxistauglichen Umsetzung der DSGVO entsprechend Ihrer Unternehmensgröße!

Ihre Ansprechpartner:

Jochen König
Partner/Geschäftsführer
Rechtsanwalt, Wirtschaftsprüfer, Steuerberater
T 0203 29506-752
j.koenig @rhein-emscher.de

Carol Haßelmans
Partnerin/Geschäftsführerin
Wirtschaftsprüferin, Steuerberaterin, Certified Public Accountant, Fachberaterin für Internationales Steuerrecht
T 0203 29506-624
c.hasselmans@rhein-emscher.de

Paul Schendzielorz
IT Manager
B.Sc. Wirtschaftsinformatik
T 0203 29506-748
p.schendzielorz@rhein-emscher.de