Hinweise für Verantwortliche öffentlicher Stellen zur Verpflichtung zur Einhaltung des Datenschutzes

1. Warum eine Verpflichtung zur Einhaltung des Datenschutzes?

Eine dem Datengeheimnis nach § 6 Absatz 2 SächsDSG entsprechende Regelung ist in der ab dem 25. Mai 2018 geltenden Datenschutz-Grundverordnung (DSGVO) nicht enthalten. Es wird dennoch empfohlen, ab dem 25. Mai 2018 neue Mitarbeiter auf die Beachtung des Datenschutzes zu verpflichten und damit die „Verpflichtung auf das Datengeheimnis“ nach dem bisher geltenden § 6 Abs. 2 SächsDSG weiterzuführen. Nicht dem Anwendungsbereich der DSGVO unterfallende Stellen können ggf. auch gesetzlich verpflichtet sein, weiterhin die Verpflichtung auf das Datengeheimnis vorzunehmen. Die Verpflichtung auf die Einhaltung des Datenschutzes ist eine organisatorische Maßnahme des Verantwortlichen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung personenbezogener Daten gemäß der DSGVO erfolgt. Zunächst ist hier Artikel 5 DSGVO zu nennen. Dieser schreibt vor, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Des Weiteren legt Artikel 5 DSGVO dem Verantwortlichen die Pflicht auf, die Einhaltung dieser Vorgabe nachweisen zu können (sog. Rechenschaftspflicht). Danach erwächst hieraus die Empfehlung einer dokumentierten Verpflichtungserklärung. Auch Artikel 24 DSGVO spricht explizit vom Erfordernis technischer und organisatorischer Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung personenbezogener Daten gemäß der DSGVO – und damit selbstverständlich auch gemäß den Grundsätzen niedergeschrieben in Artikel 5 DSGVO – erfolgt.

Weitere gesetzliche Anknüpfungspunkte sind beispielsweise Artikel 29 DSGVO und Artikel 32 DSGVO. Diese stellen klar, dass dem Verantwortlichen und Auftragsverarbeiter unterstellte Mitarbeiter, personenbezogene Daten, nur nach dessen Weisung verarbeiten dürfen.

2. Wann und durch wen soll die Verpflichtung zur Einhaltung des Datenschutzes vorgenommen werden?

Wie bisher soll die Verpflichtung auf die Beachtung des Datenschutzes zu Beginn des Dienst- oder Arbeitsverhältnisses erfolgen. Sie wird durch den Leiter der öffentlichen Stelle, den Arbeitgeber oder jeweils einen Beauftragten vorgenommen. Sie schließt die wichtige vorhergehende Unterrichtung des Bediensteten über die Grundsätze für die Verarbeitung personenbezogener Daten nach Artikel 5 und Artikel 6 DSGVO sowie die sonstigen bei seiner Tätigkeit zu beachtenden Vorschriften über den Datenschutz formal ab. Sie sollte am ersten Arbeitstag erfolgen. Die Verpflichtungserklärung sollte auf einem separaten Blatt in die Personalakte eingefügt werden.

Die vorhergehende Unterrichtung sollte durch eine geeignete Person vorgenommen werden. Dies kann der Datenschutzbeauftragte nach Artikel 37 DSGVO sein, der damit seiner ihm nach der DSGVO auferlegten Unterrichtungspflicht gemäß Artikel 39 Abs. 1 lit a DSGVO nachkommen kann.

3. Was ist Inhalt der Verpflichtung zur Einhaltung des Datenschutzes?

Die Verpflichtung zur Einhaltung des Datenschutzes beinhaltet insbesondere das Verbot der Verarbeitung personenbezogener Daten ohne entsprechende Befugnis, die sich nach Artikel 5 i. V. m. Artikel 6 DSGVOG vor allem aus einer Rechtsgrundlage (u. a. Gesetz, Rechtsverordnung, Satzung) oder der Einwilligung der betroffenen Person ergeben kann. In der Unterrichtung sollten außerdem die wichtigsten Grundsätze der Verarbeitung personenbezogener Daten eingehend erörtert werden. Wünschenswert ist die Darlegung der für den konkreten Bediensteten oder Mitarbeiter geltenden spezifischen Rechtsgrundlagen der Datenverarbeitung (z. B. Artikel 9 DSGVO oder im Sozialbereich § 35 SGB I, §§ 68 ff. SGB X etc.). Sonstige zu beachtende Vorschriften sind insbesondere die über technisch-organisatorische Maßnahmen zur Gewährleistung des Datenschutzes.

Auch über die sich aus einer Verletzung ergebenden dienst-, arbeits-, ordnungswidrigkeiten- oder strafrechtlichen Konsequenzen sollte aufgeklärt werden. Eine unbefugte, nicht durch den Verantwortlichen veranlasste, Verarbeitung von personenbezogenen Daten durch Mitarbeiter stellt eine nicht von Art. 6 DSGVO umfasste Verarbeitung dar. Ein derartiger Verstoß fällt unter den Bußgeldtatbestand des Artikel 83 DSGVO sowie des § 22 SächsDSDG.

4. Wer sollte auf die Beachtung des Datenschutzes verpflichtet werden?

Es sollten sämtliche einem Verantwortlichen unterstellten Bediensteten, die Zugang zu personenbezogenen Daten haben, verpflichtet werden. Der Begriff „Zugang“ ist weit auszulegen. Auf die konkrete Tätigkeit des Bediensteten oder Mitarbeiters kommt es nicht an. Zugang kann auch derjenige haben, zu dessen Aufgaben die Verarbeitung personenbezogener Daten nicht gehört. Unter den Begriff fallen mithin neben den regulären Voll- und Teilzeitbediensteten des Verantwortlichen auch deren Auszubildende, Praktikanten, Gutachter, externe Datenschutzbeauftragte und freie Mitarbeiter. Rechtsgrundlage der Tätigkeit „für eine öffentliche Stelle“ in diesem Sinne kann ein Minister- oder Beamtenverhältnis, aber auch ein Dienst-, Arbeits-, Auftrags- oder Werkvertrag sein.

5. Verpflichtung im Fall der Auftragsverarbeitung?

Auftragsverarbeitungsverträge (z.B. Wartungs-, Aktenvernichtungsunternehmen) nach Artikel 28, 29 DSGVO sollten vorsehen, dass der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Einhaltung des Datenschutzes verpflichtet haben (Artikel 28 Absatz 3 lit. b DSGVO). Die Verpflichtung selbst kann durch den Auftragsverarbeiter vorgenommen werden. Aus den Anforderungen an die Auswahl des Auftragsverarbeiters ergibt sich allerdings, dass der Verantwortliche den Auftragsverarbeiter überwachen muss. Er muss sich wie bisher Gewissheit darüber verschaffen, dass der Auftragsverarbeiter alle technischen und organisatorischen Maßnahmen einhält, die zum Schutz der betroffenen personenbezogenen Daten getroffen wurden. Er kann sich vor diesem Hintergrund auch die Verpflichtungserklärungen zur Kontrolle vorlegen lassen.

Auszug aus der Datenschutz-Grundverordnung:

Artikel 4 Begriffsbestimmungen

„Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;
2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

   …

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;“

   …

Artikel 5 Grundsätze für die Verarbeitung personenbezogener Daten:

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Artikel 83 Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;

f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und

k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;

c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

…

Auszug aus dem Sächsischen Datenschutzdurchführungsgesetz

§ 22 Ordnungswidrigkeiten und Strafvorschrift

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften dieses Gesetzes oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten Daten, die nicht offenkundig sind, verarbeitet oder die Übermittlung durch unrichtige Angaben erschleicht.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfundzwanzigtausend Euro geahndet werden.

(3) Der Sächsische Datenschutzbeauftragte ist Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), das zuletzt durch Artikel 11 Absatz 33 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist, in der jeweils geltenden Fassung.

(4) Wer eine der in Absatz 1 bezeichneten Handlungen gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.