Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Postsendungen bitte an die Postanschrift des TLfDI, Postfach 900455, 99107 Erfurt!

Thüringer Landesbeauftragter für den Datenschutz und
die Informationsfreiheit (TLfDI), PF 900455, 99107 Erfurt

AZ: [redacted]

(Aktenzeichen bei Antwort angeben)

[redacted]

Ihre Nachricht vom :
Ihr Zeichen :
Bearbeiter/in : [redacted]

Erfurt, den : 28. Januar 2021

Anfrage [redacted] zu pandemiebedingtes Homeoffice in kommunalen Verwaltungen

Sehr geehrte [redacted],

in Ihrer [redacted] bitten Sie den Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) Ihnen das Antwortschreiben an [redacted] zum Homeoffice insbesondere zu der Verarbeitung besonderer Kategorien personenbezogener Daten zukommen zu lassen.

Dieser Bitte kommt der TLfDI nach und hat Ihnen das Antwortschreiben an [redacted] im Wortlaut auf den nächsten Seiten zitiert.

Antwortschreiben:

„(…)

<u>Frage eins:</u>

Teilt der TLfDI die restriktive Ansicht, dass Daten der Schutzstufe 2 nicht mobil und nicht in Telearbeit verarbeitet werden dürfen?

Postanschrift: Postfach 900455, 99107 Erfurt
Dienstgebäude: Häßlerstraße 8, 99096 Erfurt
Telefon: 0361 57-3112900
Telefax: 0361 57-3112904
E-Mail*: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

*Die genannte E-Mail-Adresse dient nur für den Empfang einfacher Mitteilungen ohne Signatur/ Verschlüsselung und für mit PGP verschlüsselte Mitteilungen.

Antwort zur 1. Frage:

I. Sie beziehen sich zur Definition der sog. Schutzstufen auf den 1. Tätigkeitsbericht des TLfDI für den Berichtszeitraum vom 1. März 1994 bis 31. Dezember 1995, hier unter Punkt 15.3 (S. 106 f.).

Dieses sehr alte, von Ihnen zitierte Schutzstufenkonzept von 1994 sollte nicht mehr verwendet werden und findet seit In-Kraft-Treten der Datenschutz-Grundverordnung (DS-GVO) 2018 auch kaum noch Verwendung. Gängige Praxis ist seitdem die Anwendung des **Standard-Datenschutzmodells (SDM)**. Wenn man darauf basierend Schutzstufen in seinem Verantwortungsbereich festlegt, ist dies durchaus weiterhin möglich, weitere Maßnahmen sollten sich aber zukünftig am SDM orientieren.

Mit dem SDM stellt die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ein Werkzeug bereit, mit dem die risikoadäquate Auswahl und rechtliche Bewertung der von der DS-GVO geforderten technischen und organisatorischen Maßnahmen unterstützt wird. Sie können die aktuelle Fassung des SDM und deren derzeit sieben veröffentlichten Maßnahmen (Bausteine) aufrufen unter:

https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ .

Das SDM verwendet zur Systematisierung der datenschutzrechtlichen Anforderungen den Begriff „Gewährleistungsziele“, die bereits aus dem IT-Grundschutz bekannt sind. Datenschutzrechtliche Anforderungen zielen auf die rechtskonforme Verarbeitung, die durch **technische und organisatorische Maßnahmen (TOM)** gewährleistet werden muss. Durch Festlegung und Umsetzung der TOM wird das Risiko des Eintretens von Abweichungen bzgl. der rechtskonformen Verarbeitung gemindert. Gewährleistungsziele bündeln und strukturieren auch im Datenschutz die festgeschriebenen gesetzlichen Anforderungen. Mit ihrer Hilfe können miteinander verknüpfte sowie skalierbare Maßnahmen messbar gestaltet und standardisiert werden. Die beschriebene Methode lehnt sich an den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an und hat sich bereits bewährt.

Gewährleistungsziele des Datenschutzes gemäß SDM sind:

- Datenminimierung
- Verfügbarkeit,
- Integrität,
- Vertraulichkeit,
- Nichtverkettung,
- Transparenz,
- Intervenierbarkeit.

Bei der praktischen Umsetzung des SDM wird für jede zu betrachtenden Komponente der gesamten Systemstruktur - Daten, Systeme, Dienste sowie Prozesse – bzgl. der Gewährleistungsziele mit Referenzmaßnahmen verglichen. Daraus resultierend werden dann einzelne, konkrete TOM benannt und dokumentiert. Beachtet werden sollte, dass bestimmte Einzelmaßnahmen zur Erreichung mehrerer Gewährleistungsziele beitragen können. Dies ist im Einzelfall ebenfalls zu dokumentieren mit dem Ziel, Datenschutzanforderungen sinnvoll zu strukturieren und in der Folge systematisch in der Organisation umzusetzen.
Entsprechend DS-GVO sind die TOM nicht nur einmalig zu implementieren, sondern vielmehr sollte ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM vorgesehen sein (Art. 32 Abs. 2 DS-GVO). Die aktuelle Angemessenheit der TOM orientiert sich dabei am Stand der Technik (vgl. hierzu Abschnitt D im SDM).
Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden (Art. 32 Abs. 2 DS-GVO).
Weitere Hilfestellung zur Risikobetrachtung enthält Kapitel D3.2 des SDM in der jeweiligen Version.

Insbesondere wird in Kapitel D3.4 beschrieben, wie ausgehend vom ermittelten Risiko eines Verarbeitungsvorgangs der Schutzbedarf für eine von der Verarbeitung betroffenen Person bestimmt werden kann.
Die DS-GVO verlangt vom Verantwortlichen zudem die Beurteilung von Eintrittswahrscheinlichkeit als auch für die Schwere möglicher Schäden anhand objektiver Kriterien (siehe ErwGr. 76 DS-GVO). Vor Durchführung der Risikobewertung sind also die objektiven Kriterien zur Ermittlung der Eintrittswahrscheinlichkeit sowie der Schwere möglicher Schäden vom Verantwortlichen festzulegen.

Hinweise zur Durchführung einer Datenschutz-Folgenabschätzung (DS-FA) hat der TLfDI in der Handreichung zur Datenschutz-Folgenabschätzung (DS-FA) nicht-öffentlicher Bereich (abrufbar unter: https://tlfdi.de/mam/tlfdi/datenschutz/handreichung_ds-fa.pdf) zusammengestellt. Diese können analog verwendet werden.

Anzumerken ist: Nach aktueller Publikation des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom 17.03.2020 „Tipps für sicheres mobiles Arbeiten“ ist ebenfalls nicht die Rede von einem grundsätzlichen Verbot, sondern es wird die Forderung nach ausreichenden Sicherheitsmaßnahmen aufgemacht:

„*Wenn Mitarbeiter dienstliche Unterlagen oder Informationen mit erhöhtem Schutzbedarf bearbeiten müssen, sollte überlegt werden, von einem Arbeitsplatz außerhalb der Institution ganz abzusehen. Anderenfalls sollte der Telearbeitsplatz durch erweiterte, hochwertige technische Sicherungsmaßnahmen geschützt werden*“
(*https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/HomeOffice/homeoffice_node.html*).

II. Rechtlich betrachtet gilt zudem Folgendes: Die gültigen Datenschutzbestimmungen (DS-GVO, BDSG, ThürDSG) halten keine eindeutigen Regelungen zum „mobilen Arbeiten“ oder „Telearbeit“ durch Beschäftigte einer/eines Verantwortlichen bei Daten der Schutzstufe 2 parat. Auch hat der Gesetzgeber ein grundsätz-

liches „Verbot“ von Telearbeitet/mobilem Arbeiten bezüglich solcher Daten nicht in die genannten Regelungswerke aufgenommen, es vielmehr der verantwortlichen (hier der öffentlichen) Stelle auferlegt, unter Schaffung eines ausreichenden Sicherheitskonzeptes und Ergreifung geeigneter TOMs die technische Gewähr für die Datensicherheit zu treffen. Maßgebliche Bestimmung ist Art. 32 DS-GVO, die es Verantwortlichen (und Auftragsverarbeitern) auferlegt, entsprechend des konkret festgestellten Schutzbedarfs im Einzelfall „geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Wenn die Datensicherheit im konkreten Verarbeitungsvorgang durch Ergreifung geeigneter und ausreichender TOMs gewährleistet ist, dann – aber auch nur dann – dürfen personenbezogene Daten mit einem besonders hohen Schutzbedarf auch mobil bzw. in Telearbeitet verarbeitet werden.

Daher ist ein Abweichen von der bisher restriktiven Haltung in Bezug auf Telearbeit / mobilem Arbeiten bei der Verarbeitung von besonderen Kategorien von personenbezogenen Daten durchaus insoweit vertretbar. Gerade der vom Gesetzgeber dabei an vielen Stellen im Gesetz zu berücksichtigende „Stand der Technik“ hat sich in den vergangenen Jahren weiterentwickelt, sodass technische Lösungen der Absicherung von Daten auch bei der Klassifizierung in höheren Schutzstufen dabei genutzt werden könnten und sollten.

Frage zwei:

Reichen die dargestellten organisatorischen Maßnahmen aus, um auch Daten der Schutzstufe 2 mobil zu verarbeiten?

Antwort zur 2. Frage:

Die dargestellten organisatorischen Maßnahmen sind das Genehmigungsverfahren (Workflow) und sollen die anzuwendende Sorgfaltspflicht für die durch den Dienstherrn übergebenen Geräte einschließlich der nachfolgenden Merkmale gewährleisten:

Meldung bei Verlust und Verdacht der Passwort-Kompromitierung,
regelmäßige Sperrung/Abschaltung bei Nichtnutzung,
Verhindern von Einsichtnahme Dritter.

Die reine Betrachtung der organisatorischen Maßnahmen würde zu dem Schluss führen, dass diese nicht ausreichen, da weder die Passwortkomplexität geregelt ist, noch die Verwahrung von Zugangswissen und Zugangsbesitz (Nutzername & Passwort, Token). Als technische Maßnahmen kommen allerdings hinzu: 2-Faktor-Authentifizierung (Zertifikat und Token werden als gemeinsamer „Besitzfaktor“ angesehen), Bit-Locker-Verschlüsselung, irgendwie vom Normalsystem getrennte Nutzerprofile.

Unter Bezug auf die unter der Antwort auf die 3. Frage aufgeworfene Fragestellungen kann (bei reiner Darstellung von Bildschirminhalten und das Verhindern von lokaler Datenspeicherung oder Druckfunktionen) ein hoher technischer Schutzgrad mit Dienstgeräten erfüllt werden, wenn ein regelmäßiges Update als organisatorische Maßnahme, automatische Prüfung der Passwortkomplexität, Virenschutz und eine ausreichende Systemhärtung (durch Beschränkung der Systemdienste, Konfigurierbarkeit, restriktive Gruppenrichtlinien, Einstellung der Firewall auf minimale Datenkanäle) zusätzlich umgesetzt werden. Dabei muss genau dokumentiert sein, was „Schutzstufe 2“ bedeutet (siehe Antwort zur vorherigen Frage) und woran diese beim Umgang mit personenbezogenen Daten gemessen wird (! Kriterien).

Frage drei:

Genügt die dargestellte technische Lösung den Anforderungen für Verarbeitung von Daten der Schutzstufe 2? Bzw., wenn Sie die dargestellte Lösung nicht kennen, welche technischen Maßnahmen sind durch [redacted] *zu prüfen und zu dokumentieren? Oder muss für jede der betroffenen Verfahren (der Schutzstufe 2) jeweils eine DS-FA durchgeführt werden, obwohl die technische Anwendung (mobiles Arbeiten) gleich ist?*

Antwort zur 3. Frage:

Die dargestellte technische Lösung ist nicht vollständig. So wird zwar der VPN-Tunnel in vielen Details beschrieben, die Nutzung dieses Tunnels allerdings nicht. Es bleibt unklar, inwieweit dann z. B. technische Verfahren wie RDP, Citrix, VMware Horizon oder andere Terminaldienste genutzt werden sollen. Weiterhin fehlt die Aussage, ob der Rechner auf ein lokales Nutzerprofil zurückgreift und im Profil auf dem Rechner z. B. dienstliche Daten dauerhaft auf dem mobilen Arbeitsplatzrechner gespeichert werden (sollen/dürfen).

Gerade im Diebstahl-Szenario unterscheidet sich dann die Risikobewertung, da nicht klar ist, wie komplex das Passwort für die Bitlocker-Verschlüsselung ist und ob die Passwortkomplexität automatisch geprüft werden kann. Gerade wenn tatsächlich der (aussagegemäß sehr seltene) Fall eintritt, dass Daten einer Stufe mit höherem Schutzbedarf verarbeitet werden müssen, muss der genutzte Rechner die gleiche Sicherheit gewährleisten, wie in der Behördenarbeit vor Ort.

Das bedeutet, Daten dürfen nur mit erheblichem Aufwand (auch unter Einbeziehung von forensischen Mitteln) extrahierbar sein. Da beim mobilen Rechner die behördliche umgebende Infrastruktur fehlt, müsste das System gehärtet werden. Dies kann z. B. durch Beschränkung oder Abschaltung der Systemdienste, Verhinderung der Konfigurierbarkeit durch restriktive Gruppenrichtlinien und Nutzerverwaltung, Einstellung der Firewall auf minimale Datenkanäle, Festplattenverschlüsselung, Einsatz von Ubi-Keys usw. Der Grund ist hier, dass man vor Einwahl in den VPN-Tunnel in einem potenziell „feindlichen“, kompromittierbaren Netzwerk unterwegs ist, dass Schwachstellen des mobilen Rechners ausnutzen kann.

Für die Verarbeitung von personenbezogenen Daten mit einfachem Schutzbedarf sind dabei normale Sicherheitsmaßnahmen wie VPN-Tunnel, Firewall, Bitlocker, Virenscanner und regelmäßige Updates ausreichend, aber die Verarbeitung von personenbezogenen Daten mit höherem Schutzbedarf verlangt hier strengere

Maßnahmen. Dies hat eine erforderliche Härtung des Systems zur Folge. Der Grad der Härtung hängt davon ab, ob und in welchem Umfang dienstliche Daten auf dem mobilen Arbeitsplatzrechner vor Ort dauerhaft gespeichert werden (sollen/dürfen). Die kann nur der Verantwortliche nach einer zugeschnittenen Risikoabschätzung in den betreffenden Fachbereichen beurteilen, da hier Details zu den Daten und den Verfahren beachtet werden müssen. Der TLfDI sieht sich dazu außerstande.

Zur Frage, welche Verarbeitungsprozesse eine DS-FA benötigen, sei darauf hingewiesen, dass Art. 35 DS-GVO regelt wann eine DS-FA durchzuführen ist.
So regelt Art. 35 Abs. 1 DS-GVO:

„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.“

Dies muss also für jedes einzelne Verfahren geprüft werden, erst recht erneut, wenn dieses Verfahren für Telearbeit zugelassen wird.

Eine Liste nach Art. 35 Abs. 4 DS-GVO, wonach auf jeden Fall eine DS-FA durchzuführen ist, hat der TLfDI veröffentlicht, siehe
https://www.tlfdi.de/mam/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf .

Auf jeden Fall ist auch eine DS-FA durchzuführen, wenn es sich um eine umfangreiche Datenverarbeitung von Daten gemäß Art. 9 und Art. 10 DS-GVO handelt (Art. 35 Abs. 3 lit. b) DS-GVO).

Art. 32 Abs. 2 DS-GVO regelt:

„Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Bereits in den Ausführungen des TLfDI vom [redacted] teilte der TLfDI mit:

„Zur Dimension der Schadenshöhe kann der TLfDI keine Aussagen treffen, da nicht bekannt ist, welche Datenkategorien über E-Mail und Intranet‘ auf den betreffenden Privatrechnern zugänglich gemacht werden sollen. Anzumerken ist, dass es der Stadtverwaltung Erfurt obliegt, die maximale Schadenshöhe einzuordnen. Der TLfDI empfiehlt daher, das Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen‘ der unabhängigen Datenschutzbehörden des Bundes und der Länder“ (Datenschutzkonferenz – DSK) als Orientierung zu verwenden, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf).

Eine Handreichung zur DS-FA für den nicht-öffentlichen Dienst hat der TLfDI auf seiner Internetseite veröffentlicht: https://www.tlfdi.de/mam/tlfdi/datenschutz/handreichung_ds-fa.pdf . Diese ist zwar noch nicht dem öffentlichen Bereich angepasst, ist aber trotzdem empfehlenswert.

Abschließend möchte ich Sie noch darauf hinweisen, dass für jedes Fachamt eine Einzelfallprüfung erfolgen muss, aufgrund der verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten.

(…)“.

[redacted]

Für Rückfragen stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen
im Auftrag

[redacted]