Vorschlag für eine Adaptionsverfügung für Verarbeitungsverzeichnisse

1. Grunddaten der Fachanwendung

Bezeichnung des Verfahrens/ Kurzbezeichnung	
Zweckbestimmung (Aufgaben, zu deren Erfüllung die Daten verarbeitet werden)	
Verfahren in Betrieb seit	
Freigabe erteilt am	
Auflagen vorhanden: ja/nein **Auflagen umgesetzt: ja/nein**	
Verfahrensspezifisches Sicherheitskonzept vorhanden? Wenn ja, dann bitte benennen	

2. Überführung der bisher angewendeten Regelungen auf das Niveau der DS-GVO

Auf der Grundlage des bisherigen Freigabeverfahrens war jedes automatisierte Verfahren, mit dem personenbezogene Daten verarbeitet wurden, gemäß § 34 ThürDSG und den darin dokumentierten technisch organisatorischen Maßnahmen innerhalb des Verfahrensverzeichnisses nach §§ 9, 10 ThürDSG vor der produktiven Freischaltung einem Prüfverfahren zu unterwerfen. Dieses besteht im Wesentlichen aus dem Freigabeverfahren nach § 34 Abs. 2 ThürDSG, der Pflicht zum Führen eines Verfahrensverzeichnisses nach § 10 ThürDSG sowie der Sicherstellung des Datenschutzes durch geeignete technische und organisatorische Maßnahmen, § 9 ThürDSG. Zweck der datenschutzrechtlichen Freigabe ist die Vorabkontrolle der Zulässigkeit der automatisierten Verarbeitung personenbezogener Daten. Durch geeignete organisatorische Regelungen ist sicherzustellen, dass automatisierte Verfahren erst nach der vorherigen schriftlichen Freigabe zum Einsatz gelangen. Im Rahmen eines solchen Freigabeverfahrens wurde regelmäßig ein Verfahrensverzeichnis erstellt. Dieses wurde gegebenenfalls ergänzt durch IT Sicherheitskonzepte, Rechte-Rollenkonzepte und Dienstanweisungen.

Als Mindestvoraussetzung für die datenschutzrechtliche Dokumentation hat der für die automatisierte Verarbeitung unmittelbar verantwortliche Leiter der Organisationseinheit das Formblatt für den Eintrag in das Verfahrensverzeichnis nach § 10 ThürDSG zu erstellen (Hinweise des Thüringer Innenministeriums zum Thüringer Datenschutzgesetz - ThürDSG - vom 07. Februar 2003). Anträge auf Freigabe sind von der Organisationseinheit, die den Einsatz des automatisierten Verfahrens beabsichtigt, unter Einhaltung des Dienstweges dem

fachlich zuständigen Leiter der Dienststelle oder einem von ihm Beauftragten zur Entscheidung vorzulegen. Dem Antrag sind die Formblätter zum Verfahrensverzeichnis sowie ein Vermerk, der die Beteiligung der verantwortlichen Organisationseinheiten und hier insbesondere die Beteiligung des für die Behörde bestellten internen Beauftragten für den Datenschutz an der Vorbereitung der Entscheidung ausweist, beizufügen. Die Freigabeentscheidung ist der das Verfahren betreibenden Organisationseinheit zur Kenntnis zu geben, der Beauftragte für den Datenschutz erhält die Formblätter zur Aufnahme in das von ihm geführte Verfahrensverzeichnis.

2.1 Freigabeverfahren („Datenschutz-Folgenabschätzung"), Verfahrensverzeichnis, technische und organisatorische Maßnahmen in der Praxis der (öffentliche Stelle eintragen) bis zum 25. Mai 2018

Bei der (öffentliche Stelle eintragen) ist bereits vor der Geltung der der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung – DS-GVO) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) für die automatisierte Verarbeitung von Daten sowie die Verarbeitung personenbezogener Daten in Akten durch

- Hier die relevanten Grundlagen der Datenverarbeitung (z. B. Dienstanweisungen, Richtlinien, Konzepte, Dienstvereinbarungen, Beschreibungen, Sicherheitsanalysen, etc.) aufführen.

ein qualifiziertes datenschutzrechtliches und informationssicherheitstechnisches Freigabeverfahren etabliert worden.

Ein angemessenes Maß an Sicherheit bei der Einführung der Verfahren gewährleisten dabei insbesondere die folgenden Maßnahmen (sofern sie nicht bereits unter dem ersten Spiegelstrich dargestellt worden sind):

- Abstellen auf die / Einfügen der Regelungen aus den relevanten Grundlagen der Datenverarbeitung (z. B. Dienstanweisungen, Richtlinien, Konzepte, Dienstvereinbarungen, Beschreibungen, Sicherheitsanalysen, etc.).

2.2 Erweiternde Regelungsinhalte der DS-GVO

Über die im bisherigen etablierten Freigabeprozess berücksichtigten Inhalte hinaus sieht die DS-GVO ergänzende bzw. anschauliche Prüfaspekte vor, die insbesondere im Rahmen der Wahl der technischen und organisatorischen Maßnahmen folgendermaßen einbezogen wurden:

2.2.1 Belastbarkeit der Systeme gem. Art. 32 Abs. 1 Buchstabe b) DS-GVO

Damit ist in der deutschen Literatur der Informatik regelmäßig die Widerstandsfähigkeit oder Ausfallsicherheit von Systemen und Diensten gemeint (vgl. dazu Jandt in: Kühling/Buchner, DS-GVO-Kommentar, Art. 32, Rz. 26) Unter dem Begriff der Resilienz (die englische Originalfassung der DS-GVO benutzt den Begriff der „resilience") wird allgemein die Fähigkeit eines Systems verstanden, mit Veränderungen, beispielsweise durch Risikoeintritte umgehen zu können.

Eine Planung der Belastbarkeit von Informationstechnik gehört zu den organisatorischen Planungsaufgaben für den Einsatz geeigneter Technik. Die_____(öffentliche Stelle einsetzen) richtet sich bei den umzusetzenden organisatorischen und technischen Konzepten nach den Empfehlungen des Grundschutzes des Bundesamtes für die Informationssicherheit (BSI). Hier werden insbesondere der Gefährdungskatalog „G 2.3 Fehlende, ungeeignete, inkompatible Betriebsmittel und die daraus resultierenden Maßnahmen“ beachtet und entsprechend umgesetzt.

2.2.2 Pseudonymisierung, Anonymisierung gem. Art. 25 Abs. 1 und Art. 32 Abs. 1 Buchstabe a) DS-GVO

Möglichkeiten zur Pseudonymisierung und Anonymisierung wurden auch bereits im bisherigen Prozess geprüft und wenn möglich insbesondere bei der Festlegung von Löschfristen bzw. bei Übermittlungen berücksichtigt.

2.2.3 Datenschutzrechtliche Voreinstellungen: Privacy by Design und Privacy by Default gem. Art. 25 Abs. 2 DS-GVO

Die Pflicht zur Einrichtung von datenschutzfreundlichen Voreinstellungen bedeutet grundsätzlich, dass ein Produkt oder Dienst für den Nutzer bereits ohne weiteres Zutun beim ersten Einschalten bzw. Aufruf die datenschutzfreundlichsten Einstellungen und Komponenten aufweisen soll (siehe dazu Hartung in: Kühling/Buchner, DS-GVO, Kommentar, Artikel 25, Rz. 24). Eventuell nicht vorhandene, datenschutz- bzw. IT-sicherheitstechnisch relevante Funktionen in den IT-Fachanwendungen wurden und werden nachträglich, ggf. im Wege von Auflagen, eingerichtet (z. B. lesende, schreibende Protokollierungen).

2.2.4 Datenminimierung gem. Art. 5 Abs. 1 Buchstabe c) und Art. 25 Abs. 1 DS-GVO

Das Grundprinzip der Datenvermeidung / -minimierung wurde auch bisher in dem datenschutzrechtlichen Freigabeverfahren, insbesondere bei der Prüfung von Zugriffs- und Rechtekonzepten sowie der Festlegung von Löschfristen berücksichtigt.

3. Überführungsergebnis

Die DS-GVO schreibt für alle öffentlichen Institutionen in den Mitgliedsstaaten die Durchführung einer sog. "Datenschutz-Folgenabschätzung" vor (Art. 35 ff. DS-GVO). Diese ist durchzuführen, wenn die Verarbeitung der personenbezogenen Daten mit besonders komplexen und neuartigen Verfahren vorgenommen wird. Explizit wird die Datenschutz-Folgenabschätzung verbindlich vorgeschrieben, wenn umfangreich besonders sensible Kategorien von Daten verarbeitet werden (z. B. Gesundheitsdaten nach Art. 9 DS-GVO). Die Datenschutz-Folgenabschätzung wird nicht bei jedem automatisiertem Verfahren erforderlich sein, während nach dem bisher geltenden ThürDSG das Freigabeverfahren häufiger zum Einsatz kam.

Darüber hinaus sieht die DS-GVO für alle Verarbeitungstätigkeiten ein Verzeichnis nach Art. 30 vor sowie die Pflicht des Verantwortlichen, bestimmte technische und organisatorische Maßnahmen zu treffen (Art. 24, 25, 32 der Verordnung (EU) 2016/679).

Vor dem Hintergrund der bisherigen gesetzlichen Verpflichtung der Freigabeverfahren durch die_____(öffentliche Stelle einfügen) unter regelmäßiger weiterer schriftlicher Erörterung datenschutzrechtlicher Fragestellungen und der Etablierung eines Prozesses zur Gewährleistung der Informationssicherheit am Maßstab der BSI-Methodik erscheint eine Adaptionsverfügung als gerechtfertigt, da die sich aus dem EU-Recht und ThürDSG künftig erge-

benden Anforderungen weitgehend nicht über den bisherigen Standard hinausgehen werden.

Im Rahmen eines solchen Freigabeverfahrens wurde regelmäßig ein Verfahrensverzeichnis vorgelegt. Dieses Dokument wurde bei einer Vielzahl der Verfahren durch das oben benannte Informationssicherheitskonzept (BSI-Methodik), ggf. durch ein Rechte-Rollenkonzept und Dienstanweisungen ergänzt, soweit die darin zu beschreibenden Angaben für eine Formulierung innerhalb des Verfahrensverzeichnisses zu umfangreich waren.

Es besteht Einvernehmen zwischen den beteiligten Akteuren und dem behördlichen Beauftragten für den Datenschutz, dass der nunmehr bereits seit Jahren praktizierte und unter 2.1. skizzierte Prüfprozess ein Höchstmaß an Qualität bezogen auf die datenschutzrechtlichen Regelungen und informationssicherheitstechnischen Erfordernisse nach dem Stand der Technik gewährleistet und in dieser Form den inhaltlichen Forderungen der DS-GVO nach Risikoabschätzung, Auswahl geeigneter technischer und organisatorischer Maßnahmen sowie der Dokumentation ergriffener Maßnahmen entspricht.

Festzuhalten ist somit, dass die unter Nummer 1 genannte Datenverarbeitung, die im Rahmen des durch den Datenschutzbeauftragten zu führenden Verfahrensverzeichnisses vorliegt und von diesem freigegebenen wurde, den Vorgaben der DS-GVO in großen Teilen entspricht.

Diese Einschätzung wurde von den Vertretern des Thüringer Ministeriums für Inneres und Kommunales, der kommunalen Spitzenverbände und des TLfDI in der gegründeten Arbeitsgruppe zur Umsetzung der DS-GVO auf kommunaler Ebene geteilt. Diese Adaptionsverfügung gilt, vorbehaltlich des Erfordernisses wesentlicher Änderungen für die jeweilige Fachanwendung, maximal zwei Jahre ab Anwendung der DS-GVO am 25. Mai 2018.

Die Verwendung dieser Adaptionsverfügung entbindet den Verantwortlichen nicht davon, bei relevanten Änderungen des Verfahrens das entsprechende Verzeichnis an die DS-GVO schon vor Ablauf der genannten Frist anzupassen. Die Verwendung der Adaptionsverfügung schließt ferner Kontrollen und weitere Maßnahmen des TLfDI nicht aus.

4. Schlusszeichnung

Ort, den

Verantwortliche Stelle oder bevollmächtigter Vertreter

5. Kopie an den bDSB zur Kenntnis