Der Landesbeauftragte für den **DATENSCHUTZ** und die **INFORMATIONSFREIHEIT** Rheinland-Pfalz

Empfehlungen des LfDI Rheinland-Pfalz an das Ministerium für Wissenschaft und Gesundheit für eine datenschutzkonforme Digitalisierung des Öffentlichen Gesundheitsdienstes in Rheinland-Pfalz

(Stand: 24.07.2024)

Ende 2023 und Anfang 2024 fand ausgehend von einem journalistischen Beitrag eine öffentliche Diskussion über den Stand von Datenschutz und Datensicherheit in rheinland-pfälzischen Gesundheitsämtern statt. Gegenstand waren vermutete konkrete datenschutzrechtliche Defizite sowohl bei dem landesweit zum Einsatz kommenden Softwareprodukt der Firma Mikroprojekt GmbH als auch bei den einzelnen Gesundheitsämtern. Dabei wurden auch Befürchtungen geäußert, dass die vermuteten IT-Sicherheitslücken Auswirkungen auf das laufende Landesprojekt zur Digitalisierung des Öffentlichen Gesundheitsdienstes in Rheinland-Pfalz haben könnten.

Der LfDI Rheinland-Pfalz, der von Anfang an das o.g. Digitalisierungsprojekt allgemein beratend begleitet hatte, ergriff seit Aufkommen der öffentlichen Diskussion diverse konkrete Maßnahmen zur Aufklärung der Vorwürfe. Hierzu gehörten neben Gesprächen mit dem Software-Hersteller und dem MWG auch örtliche Feststellungen zum Datenschutz in vier Gesundheitsämtern. Auf der Grundlage der in diesem Zusammenhang gewonnenen Erkenntnisse spricht der LfDI gegenüber dem MWG als projektkoordinierender Stelle folgende Empfehlungen für eine datenschutzkonforme Digitalisierung des Öffentlichen Gesundheitsdienstes in Rheinland-Pfalz aus:

- Die Digitalisierung des öffentlichen Gesundheitsdienstes in Rheinland-Pfalz setzt ein funktionierendes internes **Datenschutzmanagement** bei den Gesundheitsämtern bzw. den diese tragenden Kreisverwaltungen voraus.

- Bei Auswahl und Einsatz von IT-Anwendungen im Öffentlichen Gesundheitsdienst sind die Anforderungen an die **Datensicherheit** (Art. 24/Art. 32 DS-GVO) und die Grundsätze von **privacy by design** und **privacy by default** (Art. 25 DS-GVO) zwingend zu beachten. Software-Produkte müssen die Umsetzung dieser Anforderungen technisch unterstützen.

- Aufgrund der besonderen Schutzbedürftigkeit der im Öffentlichen Gesundheitsdienst verarbeiteten Gesundheitsdaten der Bürgerinnen und Bürger muss jederzeit gewährleistet sein, dass diese innerhalb der Verwaltungen nur von denjenigen Beschäftigten zur Kenntnis genommen und verarbeitet werden können, die diese zur Erfüllung der ihnen zugewiesenen Aufgaben benötigen („**Need-to-know-Prinzip**“).

- Durch technisch-organisatorische Maßnahmen muss sichergestellt werden, dass die Einhaltung der Anforderungen an den Datenschutz und die Datensicherheit in den Verwaltungen dauerhaft **dokumentiert** ist und intern und extern **überprüft** werden kann. Hierzu gehören interne Konzepte zur Nutzerverwaltung, der Vergabe von Zugriffsrechten, der Datensicherung, der IT-Sicherheit, der Protokollierung und der Löschung sowie die Nachvollziehbarkeit ihrer jeweiligen Umsetzung.

- Der Einsatz von Dienstleistern, die personenbezogene Daten von Bürgerinnen und Bürgern beispielsweise im Rahmen der Fernwartung oder des IT-Supports zur Kenntnis nehmen können, setzt ausnahmslos das Vorhandensein einer **vertraglichen Vereinbarung im Sinne von Art. 28 Abs. 3 DS-GVO** voraus.

- Im Rahmen des Digitalisierungsprojekts sollten die Gesundheitsämter bei der Umsetzung der datenschutzrechtlichen Anforderungen so weit wie möglich durch das Land bzw. die im Projekt vorgesehene Leitstelle **unterstützt** werden. Hierzu gehören u.a. Festlegungen mit dem Hersteller der im ÖGD vorgesehenen Fachanwendungen zur Gewährleistung von Datenschutz und Datensicherheit in dessen IT-Produkten sowie eine landesweite Klärung der in den Gesundheitsämtern anzusetzenden Aufbewahrungsfristen. Auch an die einzelnen Kommunalverwaltungen gerichtete **Handreichungen** können hier ein geeignetes Mittel sein. Diese Handreichungen sollten konkrete Hinweise und Anleitungen enthalten, um eine effektive Verwirklichung der Anforderungen vor Ort sicherzustellen.