Der Bayerische Landesbeauftragte
für den Datenschutz

Bayerische öffentliche Stellen und die Windows-Telemetriekomponente

Aktuelle Kurz-Information 50

Stichwörter: Administration – Betriebssystem – Datensparsamkeit | **Stand:** 1. August 2023

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- Microsoft Windows kann in den Versionen 10 und 11 „nach Hause telefonieren“: Insbesondere Telemetriedaten werden vom Rechner an den Hersteller übermittelt – und können je nach Konfiguration personenbezogene Daten enthalten.
- Die Übermittlung von Telemetriedaten kann standardmäßig aktiviert sein. Verantwortliche müssen die Einstellungen prüfen und erforderlichenfalls anpassen.
- Mehrere Wege führen zu Deaktivierungen. Was (überhaupt) geht, und was zu tun ist, hängt von der eingesetzten Windows-Edition ab.

Windows ist ein sehr beliebtes Betriebssystem. Das gilt vor allem für die Versionen 10 und 11, die wohl von weit mehr als einer Milliarde Menschen weltweit genutzt werden. Auch aus der IT-Landschaft bayerischer öffentlicher Stellen ist Windows nicht wegzudenken. Dabei ist für IT-Verantwortliche und Administratoren klar, dass die Sicherheit von Windows-Installationen nicht herstellergegeben ist, sondern – mitunter mühsam – erarbeitet werden muss: Insbesondere funktionierende Firewalls, regelmäßige Updates und eine zielführende, möglicherweise durchaus von den Standardeinstellungen abweichende Konfiguration sind erforderlich, um gegen Angriffe geschützt zu sein. 1

Bei der üblichen Priorisierung von Maßnahmen gegen Angriffe von außen sind sich vielleicht nicht alle IT-Verantwortlichen und Administratoren bei bayerischen öffentlichen Stellen bewusst, dass Windows selbst – je nach Version, Edition und Einstellungen – unbemerkt und auch unerwünscht Daten an den Hersteller übermitteln kann. Dass Microsoft für solche Datenströme harmlos-technisch klingende Bezeichnungen wie etwa „Telemetrie“, „Diagnosedaten“ oder „Feedback“ wählt, ändert dabei nichts an der Tatsache, dass auch personenbezogene Daten umfasst sein können. Eine Übermittlung personenbezogener Daten „per Telemetrie“ muss genauso rechtmäßig sein wie jede andere Datenübermittlung – im Fall eines Drittlandtransfers nach Maßgabe der dafür zusätzlich zu beachtenden Vorgaben. Die Erfüllung der Rechenschaftspflicht (Art. 5 Abs. 2 Datenschutz-Grundverordnung) ist insofern zumindest anspruchsvoll. Eine im Grundansatz vergleichsweise einfache Alternative liegt darin, die Übermittlung von Telemetriedaten durch geeignete Einstellungen zu unterbinden. 2

1. Ausgangslage

Moderne Betriebssysteme wie Windows 10 und 11 bestehen aus einer Vielzahl von Komponenten, Subsystemen, Treibern, Diensten und Dienstprogrammen, die verschiedene Funktionen erfüllen und vielfältig voneinander abhängen. Im konkreten Kontext des Einsatzes bei 3

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

einer bestimmten bayerischen öffentlichen Stelle sind manche Systembestandteile essenziell, manche jedoch weniger oder gar nicht relevant für die aufgabenbezogene Funktionalität des spezifischen Systems. Allerdings können einzelne Dienste und Funktionen notwendig darauf angewiesen sein, Informationen nach außen zu kommunizieren oder von dort zu erhalten. Das ist etwa bei der Lizenzverwaltung, bei Malwaredefinitionen, Updates oder Zertifikatswiderrufen der Fall. Dazu treten diese Dienste mit bestimmten „Endpunkten" in Kontakt, die in der Regel durch Microsoft betrieben werden.

4 Mit der Übermittlung von Telemetriedaten („Fernmessdaten") „telefoniert" das Betriebssystem des Arbeitsplatzes gleichsam „nach Hause". Telemetrie ermöglicht dem Hersteller, Informationen über die Nutzung und die Leistung des Betriebssystems zu sammeln, aber auch zu Kompatibilitäten (etwa bei Treibern) und Systemabstürzen. Schließlich fallen sogar Informationen an, die strategische Relevanz haben können, so etwa zur Ausbreitung neuer Malware.

5 Telemetrie hat also grundsätzlich eine sachliche Berechtigung, oft auch einen wenigstens für den Hersteller sinnvollen Zweck – und kann den Datenschutzzielen „Sicherheit" und „Verfügbarkeit" dadurch zumindest indirekt dienlich sein. Für den Hersteller ist potenziell eine Vielzahl an Daten relevant. Sein Interesse, möglichst aussagekräftige Daten zu erhalten, ist im Grundsatz nachvollziehbar. Gleichwohl ist aufgrund der „Blackbox"-Eigenschaft und der Komplexität des Betriebssystems grundsätzlich schwer einzuschätzen, welche Daten nun genau übermittelt werden. Verantwortliche Stellen können nicht ohne weiteres feststellen, welche Daten geteilt werden, ob sich personenbezogene Daten darunter befinden, und, wenn ja, welche. Fraglich bleibt zudem, ob der Empfänger die Telemetriedaten auch zu einem anderen Zweck als zur Optimierung des „sendenden" Betriebssystems nutzt (etwa für das eigene Marketing oder eine eigene Suchmaschine) oder sie gar an Dritte weitergibt, etwa als Trainingsdaten für KI-Produkte.

2. Editionen und Optionen

6 In Windows 11 können Sie unter „Einstellungen - Diagnose & Feedback" auswählen, in welchem Umfang Diagnose- und Nutzungsinformationen an Microsoft gesendet werden sollen:

Abb. 1 –Einstellungsdialog „Diagnose & Feedback" in Windows 11.

Die Dokumentation zu Windows 11[1] nennt drei Einstellungsmöglichkeiten für die Sammlung von Diagnosedaten unter Windows 11: 7

- Diagnosedaten aus (Sicherheit),
- Erforderliche Diagnosedaten senden (Standard),
- Optionale Diagnosedaten senden (Vollständig).

Die Einstellung „Sicherheit“ lässt sich nicht über die grafische Oberfläche einstellen. Unter Windows 10 gibt es noch die Einstellung „Erweitert“, deren Umfang zwischen „Standard“ und „Vollständig“ liegt. 8

Bei der Option „Diagnosedaten aus (Sicherheit)“ werden keine Windows-Diagnosedaten vom Gerät gesendet. Diese ist somit die aus Datenschutzsicht empfehlenswerte Option. Die Option „Diagnosedaten aus“ ist jedoch nur für die Windows-Editionen „Enterprise“ und „Education“ verfügbar und kann nur über eine Gruppenrichtlinie oder die Registry gewählt werden, nicht jedoch über das Graphical User Interface (GUI): Wie aus Abbildung 2 ersichtlich, wird dort eine Option „Sicherheit“ nicht angeboten. 9

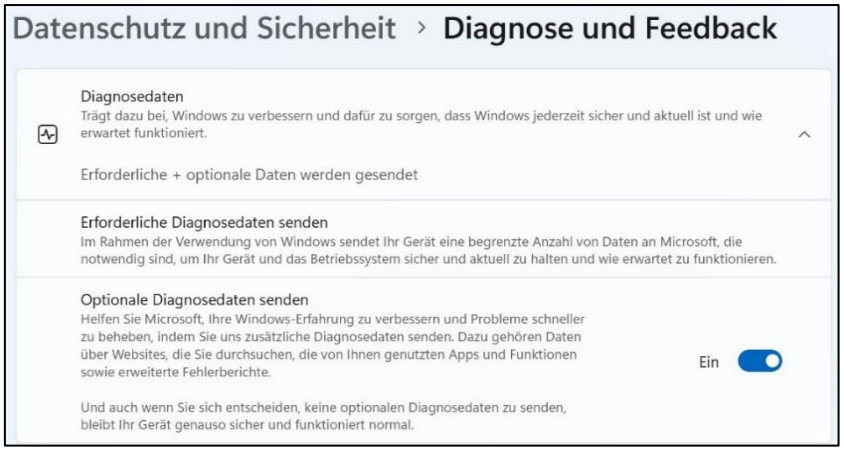

Abb. 2: Das Windows 11-GUI kann nur „optionale“ Diagnosedaten deaktivieren.

Auf die Gründe für das Weglassen der Option „Sicherheit“ bei den **„Pro“- und „Home“-Editionen** kann an dieser Stelle nicht vertieft eingegangen werden. Jedenfalls kann die Tatsache, dass die Option in diesen Editionen nicht verfügbar ist, für bayerische öffentliche Stellen kleiner und mittlerer Größe relevant sein, da sich die „Pro“-Edition explizit an kleine und mittlere Unternehmen richtet und auch von der öffentlichen Hand eingesetzt wird. Verantwortliche sollten deshalb ihre Möglichkeiten für die Nutzung der „Enterprise“- oder „Education“-Editon ausloten. Die Eigenschaften der „Home“-Edition können eine Rolle spielen, wenn Beschäftigte bayerischer öffentlicher Stellen Privatgeräte dienstlich nutzen (etwa unter bestimmten Voraussetzungen bei Lehrkräften). 10

3. Viele Wege führen zum Ziel

Eine **Gruppenrichtlinie** lässt sich mit Hilfe der Gruppenrichtlinien-Verwaltungskonsole einrichten. Die gewünschte Einstellung (vollständige Deaktivierung der Diagnosedaten) kann 11

dort unter „Computerkonfiguration – Administrative Vorlagen – Windows-Komponenten – Datensammlung und Vorabversionen – Diagnosedaten zulassen“ (siehe Abbildung 3a) ausgewählt werden. Ein wenig irreführend ist, dass zuerst die Gruppenrichtlinie „Diagnosedaten zulassen“ aktiviert werden muss, damit die Option „Diagnosedaten deaktiviert (nicht empfohlen)“ ausgewählt werden kann (siehe Abbildung 3b). Als langjährige Windows-Nutzer wissen Sie aber: Der „Aus“-Button kann sich unter „Start“ verstecken.

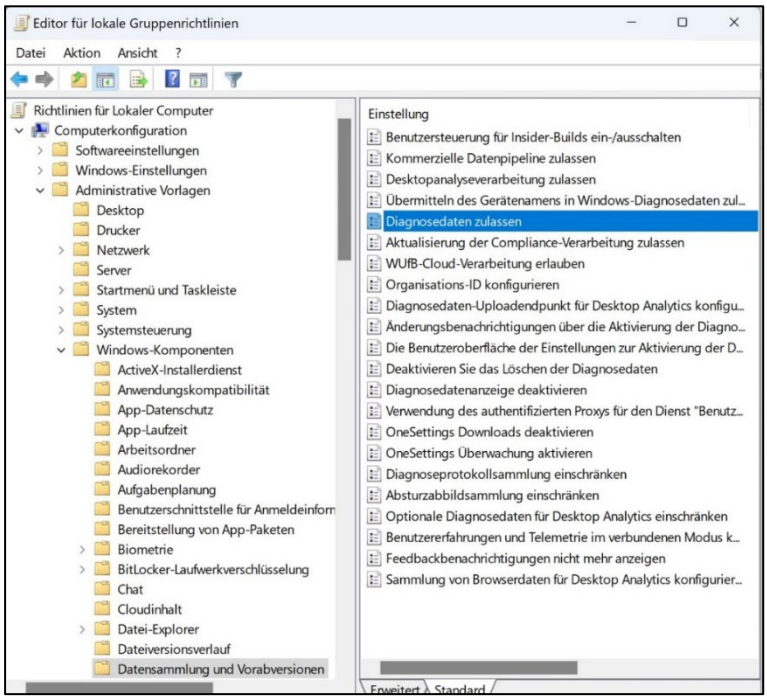

Abb. 3a –Gruppenrichtlinie für Diagnosedatensammlung

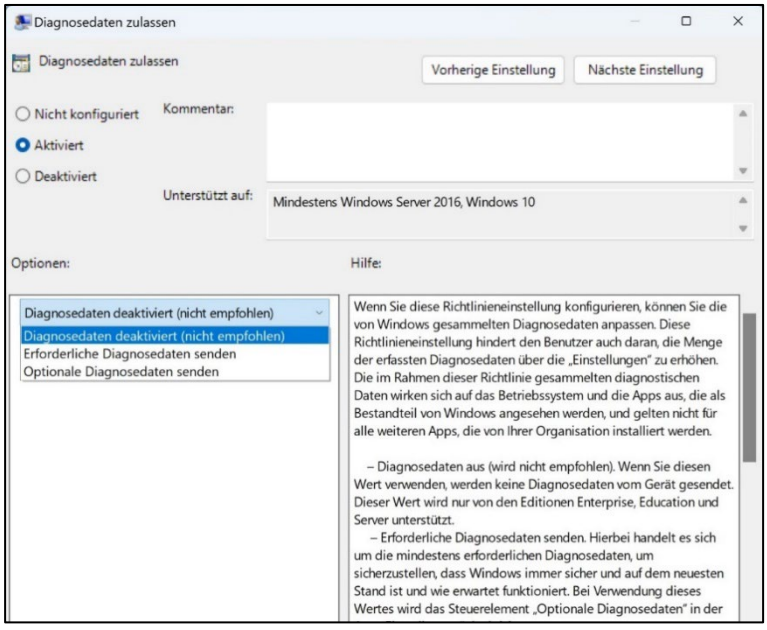

Abb. 3b – Deaktivierung der Diagnosedatensammlung

Alternativ kann die Anpassung auch mittels eines Eintrags in der **Registry** vorgenommen werden: Ändern oder erstellen Sie dazu die REG_DWORD-Registrierungseinstellung namens „AllowTelemetry“ mit dem Wert „0 (Null)“ unter dem Registrierungspfad „Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\DataCollection“. 12

4. Weitere Einschränkungsmöglichkeiten

Die in den Abschnitten 2 und 3 behandelten Windows-Diagnosedaten sind ein prominentes Beispiel für einen eingebauten Datenversand durch Windows. Die erläuterten Einstellungen gelten allerdings nur für Systemelemente, die Windows als eigene ansieht. Windows-Systemkomponenten können im Einzelfall weitere Informationen an Microsoft schicken, die keine Diagnosedaten sind. Zudem sind auch andere Microsoft-Anwendungen (wie etwa Office) gegenüber dem Hersteller nicht völlig schweigsam. 13

Aus diesen Erwägungen ist zu empfehlen, (vor-)installierte Apps und (standardmäßig) aktivierte Systemdienste systematisch zu prüfen und erforderlichenfalls zu deinstallieren oder zu deaktivieren. Dieses Vorgehen ähnelt dem „Härten“ in der IT-Sicherheit und reduziert die Angriffsfläche. Der radikale Ansatz, schlicht alle Systemdienste, die eine Netzwerkverbindung zu Microsoft aufbauen, ohne weitere Prüfung zu deaktivieren, ist dagegen nicht uneingeschränkt zu empfehlen: Manche Dienste benötigen für den ordnungsgemäßen Betrieb eine Verbindung oder hängen auf eine Art und Weise voneinander ab, dass eine Deaktivierung der Gesamtfunktionalität schaden kann: So könnten etwa nützliche Windows-Updates blockiert werden. 14

Die Windows-Dokumentation enthält neben Ausführungen zur Deaktivierung von Diagnosedaten eine ganze Reihe **„Hinweise zum Verwalten von Verbindungen zu Microsoft-Diensten“**[2] mit entsprechenden Einstelloptionen. Den Administratoren der „Education“- und „Enterprise“-Editionen gibt Microsoft praktischerweise das **„Windows Restricted Traffic Limited Functionality Baseline“**-Paket[3] (RTLFB) an die Hand, um die durchaus zahlreichen Einstellungen zügig vornehmen zu können. In der Praxis sollten Sie für die entsprechende Windows 11-Version die Baseline als Grundlage nutzen und um Anpassungen ergänzen, die auf Ihre Anforderungen und Ihre Systemumgebung zugeschnitten sind. 15

Vor dem Einsatz müssen alle Auswirkungen genau geprüft und abgewogen werden, da diese Baseline beispielsweise auch die Zeitsynchronisation (sogar innerhalb des eigenen Netzwerks) deaktiviert. Die „Windows Restricted Traffic Limited Functionality Baseline“ kann somit insbesondere zu Sicherheits- und damit auch zu Datenschutzmängeln führen, wenn sie unbedacht eingesetzt wird. 16

Nach eingehender Prüfung bezüglich der Auswirkungen können Sie die **„Windows Restricted Traffic Limited Functionality Baseline“** so anwenden: 17

- Laden Sie das Windows Restricted Traffic Limited Functionality Baseline-Paket.
- Extrahieren Sie die Datei WindowsRTLFB.zip.

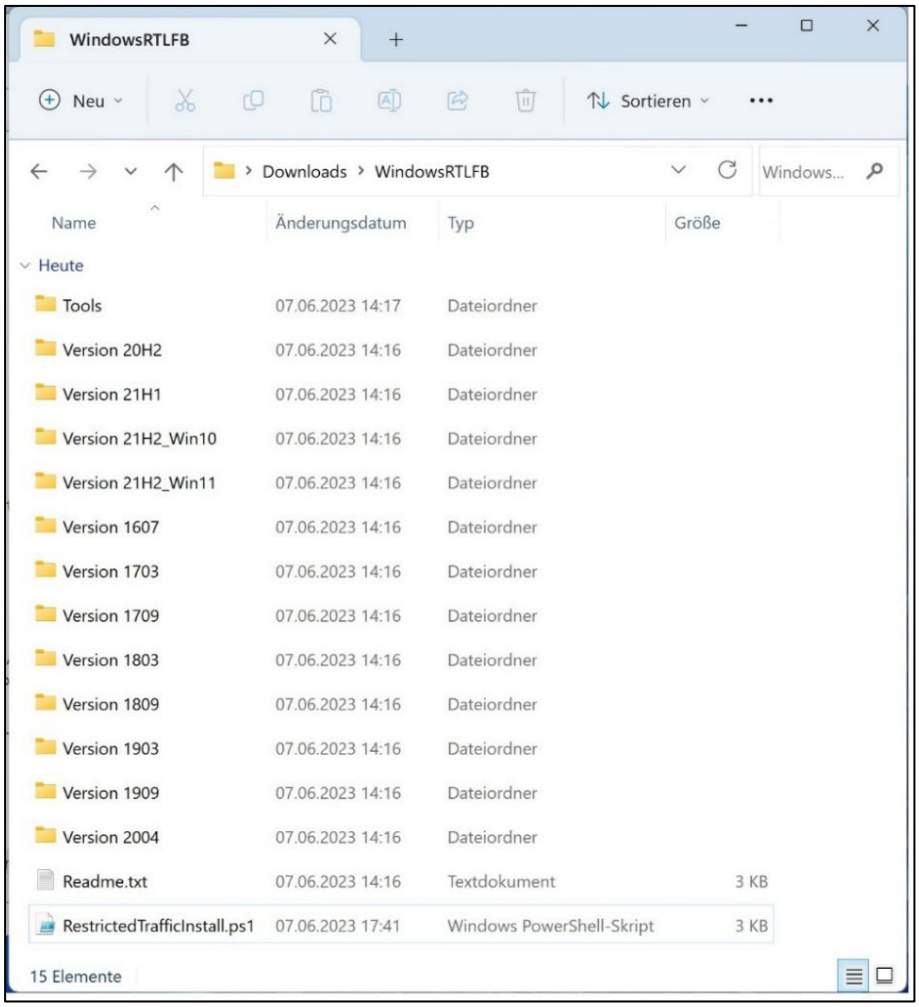

Abb. 4 – Entpacktes Windows RTLFB-Paket

- Nehmen Sie hier eventuell notwendige, behördenspezifische Anpassungen vor. Eine Hilfestellung dazu finden Sie in der Microsoft Dokumentation.
- Laden Sie das „Local Group Policy Object Utility“ (LGPO) herunter, welches Teil des Microsoft Security Compliance Toolkits 1.0 ist.
- Extrahieren Sie nun das soeben heruntergeladene Archiv „LGPO.zip“ in das Verzeichnis „WindowsRTLFB\Tools\“.
- Prüfen Sie, ob das Verzeichnis „WindowsRTLFB“ Ihre Windows Version enthält (wie in Abb. 4 etwa „21H2“).
- Führen Sie nun das PowerShell-Skript „RestrictedTrafficInstall.ps1“, das sich im WindowsRTLFB-Verzeichnis befindet, mit Administratorrechten aus (die Systemrechte für das Ausführen von Skripten müssen erforderlichenfalls erteilt werden).
- Starten Sie abschließend Windows neu.

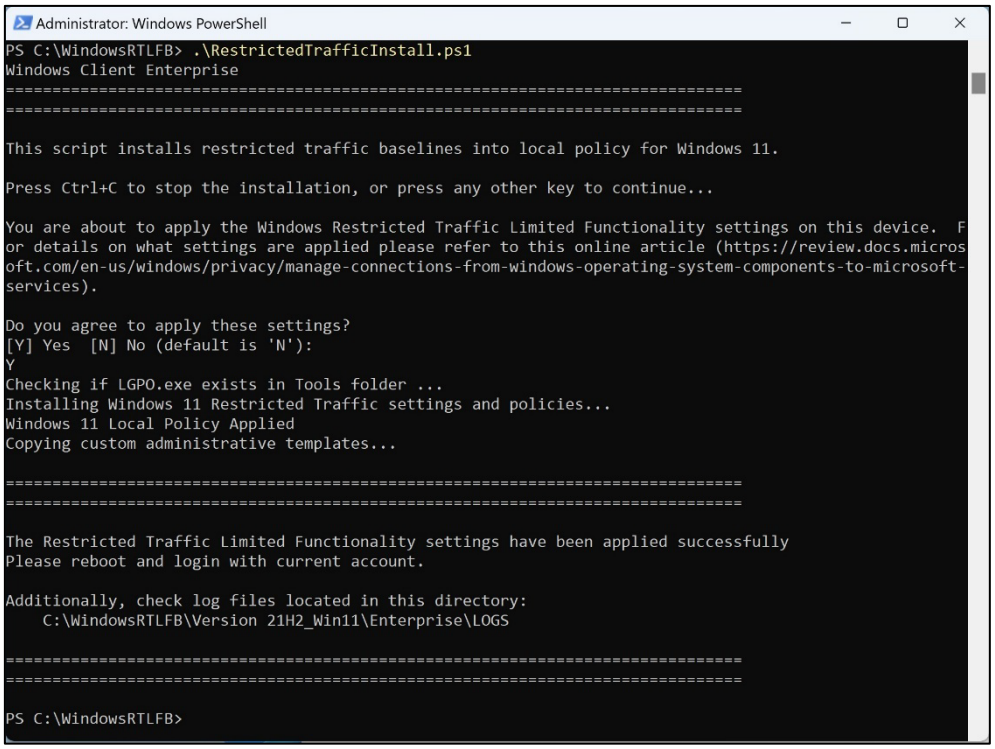

Abb. 5 – Beispielhafte Ausgabe des RestrictedTrafficInstall-Skripts

Sie können die **„Windows Restricted Traffic Limited Functionality Baseline“** in Ihren bestehenden Softwareverteilungsprozess einfügen und die nötigen spezifischen Anpassungen über die Gruppenrichtlinie vornehmen. 18

Eine Antiviruslösung, die Verfügbarkeit von Updates und die Überprüfbarkeit von Lizenzen sind zwingende Voraussetzungen für den ordnungsgemäßen Betrieb von Windows. Verbindungen zu Microsoft lassen sich somit nicht ohne Weiteres vollständig vermeiden. 19

Ergänzt man die dargestellten Maßnahmen um eine Antivirus-Lösung eines Drittanbieters, einen Server für die Verteilung von Windows Updates (Windows Server Update Services, WSUS) und ein Windows Key Management Service (KMS), lässt sich damit die Anzahl der Verbindungen zu Microsoft signifikant weiter reduzieren, wenn nicht sogar ganz vermeiden. Diese zusätzlichen Schritte empfehlen sich grundsätzlich für bayerische öffentliche Stellen, die über das dazu erforderliche technische Know-How verfügen, insbesondere aber für Netzwerkumgebungen mit erhöhten Sicherheitsanforderungen (etwa bei der Verarbeitung von personenbezogenen Daten mit erhöhtem Schutzbedarf wie beispielsweise Gesundheitsdaten). Trotzdem ist es insbesondere hier unerlässlich, mögliche Auswirkungen auf den Betrieb und die Sicherheit vorab eigenständig und eigenverantwortlich zu prüfen. 20

5. Fazit

21 Privacy-by-Design und Privacy-by-Default sind Datenschutzziele, die Hersteller möglicherweise anders bewerten und umsetzen als Verantwortliche des öffentlichen Sektors sowie Datenschutz-Aufsichtsbehörden. So sind bayerische öffentliche Stellen, die Microsoft Windows in den Versionen 10 und 11 auf ihren Arbeitsplätzen im Einsatz haben, gehalten, ihre Konfiguration zu prüfen und gegebenenfalls nachzubessern.

22 Immerhin hat Microsoft eine ausführliche und verständliche Dokumentation zu den verschiedenen Diensten und Programmen zur Verfügung gestellt, die eine Verbindung zum Hersteller aufbauen, und darin erläutert, wie eine Telemetriedaten-Übermittlung zum Zweck von Diagnose und Feedback abgestellt werden kann – wenngleich das außerhalb der „Enterprise"- und „Education"-Editionen nicht ganz einfach ist.

23 Für bayerische öffentliche Stellen wird das bereits angekündigte Supportende von Windows 10 am 14. Oktober 2025 und ein damit verbundener Umstieg auf Windows 11 eine gute Gelegenheit sein, sich auch mit dem Thema „Telemetriedaten-Übermittlung" zielführend auseinanderzusetzen.

[1] Siehe: https://learn.microsoft.com/de-de/windows/privacy/configure-windows-diagnostic-data-in-your-organization#diagnostic-data-settings.

[2] Abrufbar unter: https://learn.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services.

[3] Download-Link: https://download.microsoft.com/download/D/9/0/D905766D-FEDA-43E5-86ED-8987CEBD8D89/WindowsRTLFB.zip.