Konferenz der unabhängigen
Datenschutzbehörden
des Bundes und der Länder

Datenschutz bei Windows 10

– Prüfschema –

Impressum:

Titel:

Datenschutz bei Windows 10 – Prüfschema – Version 1.0

Herausgeber:

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Edition und Redaktion:

AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

Ansprechpartner/Autoren:

Rasmus Robrahn, Dr. Martin Krämer, Dr. Christoph Lahmann und Uwe Robra
(Die Landesbeauftragte für den Datenschutz Niedersachsen)

1. Einleitung

Das vorliegende Prüfschema soll Verantwortliche, die Windows 10 bereits einsetzen oder dies beabsichtigen in die Lage versetzen, eigenständig die Einhaltung der rechtlichen Vorgaben der DSGVO in ihrem konkreten Fall zu prüfen und zu dokumentieren.

Die Frage, ob „Windows 10“ datenschutzkonform ist, kann nämlich nicht pauschal beantwortet werden. Windows 10 ist der Begriff für eine Produktfamilie, bei der das eigentliche Betriebssystem nur noch einen Teil der gelieferten Funktionalität ausmacht, die sich zudem durch Updates fortlaufend verändert. Von der konkreten Edition, der Version und der vorgenommenen Konfiguration hängen daher der Funktionsumfang und die Datenübermittlungen an Microsoft ab. Die Bestimmung des genauen Prüfgegenstands ist daher das Fundament für die datenschutzrechtliche Prüfung. Darüber hinaus müssen Feststellungen darüber vorliegen, unter welchen Umständen Windows 10 eingesetzt wird und welche Funktionen (z. B. Cortana oder Windows Defender) genutzt werden Das bedeutet, dass eine Aufstellung darüber vorliegen muss, welche Verarbeitungstätigkeiten unter Nutzung von Windows 10 durchgeführt werden und welche personenbezogenen Daten dort in welchem Umfang verarbeitet werden. Außerdem müssen Erkenntnisse darüber vorliegen, welche personenbezogenen Daten für welche Zwecke an Microsoft übermittelt werden.

Die Abarbeitung des nachfolgenden Prüfschemas ist deshalb erforderlich, weil sich die Übermittlung von Daten an Microsoft in bislang keiner Edition und Version durch eine Änderung der Konfigurationseinstellungen komplett abstellen lässt und sich das Kommunikationsverhalten und die Konfigurationsmöglichkeiten von Windows 10 mit neuen Versionen ändern können.

Das vorliegende Prüfschema ist als Handreichung für all diejenigen gedacht, die mit Windows 10 (auch) personenbezogene Daten verarbeiten, diese also z.B. erheben, speichern oder weitergeben. Dies können natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen sein. Verantwortlicher im Sinne des Datenschutzrechts kann je nach Verarbeitung (zusätzlich) aber auch Microsoft selbst sein.

Im rechtlichen Teil werden wichtige Hinweise für die rechtliche Prüfung gegeben. Es werden die wesentlichen Normen der DSGVO bei der Prüfung von Windows 10 genannt und erläutert, wie diese Normen im Rahmen der Prüfung anzuwenden sind. Die Subsumtion selbst kann an dieser Stelle nicht geleistet werden. Sie hängt nämlich von der Einsatzumgebung sowie der verwendeten Edition und Version ab und kann schon durch den nächsten Versionswechsel überholt sein. Es ist zunächst Aufgabe des Verantwortlichen sicherzustellen und zu dokumentieren, dass die datenschutzrechtlichen Anforderungen beim Einsatz von Windows 10 jederzeit eingehalten werden. Dazu muss geprüft werden, ob und ggf. welche personenbezogenen Daten an Microsoft übermittelt werden und ob für diese Übermittlungen eine Rechtsgrundlage vorliegt. Soweit die Übermittlung unzulässig ist, hat sie zu unterbleiben und es ist mit geeigneten und angemessenen Maßnahmen sicherzustellen, dass eine solche Übermittlung unterbleibt. Daneben ist auch zu beachten, dass eine Übermittlung in ein Drittland vorliegt und daher die Art. 44 ff. DSGVO Anwendung finden.

Unter A. wird ein Überblick über Windows 10 und die datenschutzrelevanten Besonderheiten dieses Produkts gegeben. Unter B. wird dargestellt, welche Normen der DSGVO zu prüfen sind und unter C. wird ein daraus resultierendes Prüfungsschema dargestellt, das den Anspruch hat, die Prüfung von Windows 10 in unterschiedlichen Editionen, Versionen und Konfigurationen zu ermöglichen.

Im Anhang wird detaillierter auf technische Aspekte der Prüfung eingegangen.

A. Überblick über Windows 10

Das Produkt Windows 10

Windows 10 ist der Überbegriff über eine Produktfamilie, die von der Microsoft Corp., USA, im Jahre 2015 auf den Markt gebracht wurde. Die (Standard-) Installation von Windows 10 stellt dem Nutzer eine Systemumgebung zur Verfügung, die neben dem eigentlichen Betriebssystemkern (Kernel) zusätzlich Treiber und verschiedene Anwendungen (Apps) beinhaltet.

Historisch betrachtet ist Windows 10 die Fortführung von Windows NT 3.1, Microsofts erstem netzwerkfähigen Mehrbenutzer-Betriebssystem mit grafischer Oberfläche aus dem Jahr 1993.Die Anforderung, unterschiedliche Peripheriegeräte (Drucker, Tastaturen, Mäuse, Scanner,…) an den PC anzuschließen und die zunehmende Vernetzung von PCs in Unternehmen führte dazu, dass mit Windows 2000 im Jahre 1999 und Windows XP im Jahre 2001 und die Betriebssystemfunktionalität immer mehr um hardwarenahe Komponenten (Treiber) und Verwaltungskomponenten (z. B. ActiveDirectory) ergänzt wurde. Die Verbreitung des Internets und immer leistungsfähigere Prozessoren erweiterten die Funktionalität der darauf folgenden Versionen Windows 7 und Windows 8 (2012) weiter, so dass auch betriebssystemferne Anwendungen (Virenscanner, Multimediaplayer, Internetbrowser, Virtualisierungen, Festplattenverschlüsselungen und Backupfunktionen) nun unter dem Produkt „Windows“ gebündelt wurden.

Microsoft stellt seinen Kunden seine Produkte in verschiedenen Editionen zur Verfügung. Diese Editionen unterscheiden sich im Wesentlichen durch ihre Funktionalität (z. B. ob eine Verschlüsselungssoftware integriert ist), durch die Konfigurationsmöglichkeiten des Produktes durch den Nutzer und durch ihren Preis. Windows 7 war z. B. in folgenden Editionen erhältlich: Home, Premium, Professional, Ultimate und Enterprise. Darüber hinaus stehen die Produkte in der 32- und 64-Bit Variante zur Verfügung. Trotz der Entwicklungen über die Jahrzehnte stand bis Windows 8 im Wesentlichen die Betriebssystemfunktionalität der Produkte im Vordergrund. Die Produkte wurden auf einem einzelnen PC installiert, bei Bedarf durch den Nutzer aktualisiert (Updates und Servicepacks) und benötigten keine Internetverbindung. Der Nutzer konnte insbesondere das Kommunikationsverhalten der Produkte (Datentransfer zu Microsoft) selbst steuern.

Mit der Einführung von Windows 10 ändert Microsoft sein Geschäftsmodell. Microsoft hat weitere Funktionalitäten (z. B. den Sprachassistenten Cortana) zu dem Produkt hinzugefügt, die über den eigentlich benötigten Funktionsbedarf eines Betriebssystems hinausgehen.[1] Zusätzlich wird Microsoft durch die Übermittlungen des Betriebssystems in die Lage versetzt, technische Parameter und Logfiles, aber auch personenbezogene Daten zu speichern und auszuwerten.

Auch für Windows 7, sowie Windows 8 und 8.1 hat Microsoft Telemetriefunktionen nachgerüstet, wobei diese im Funktionsumfang hinter denen von Windows 10 zurückbleiben[2].

Das Vertriebskonzept änderte sich von einem Produktverkauf, bei dem jede neue Version gekauft werden musste, in ein Servicekonzept.[3] Bei diesem Konzept werden z. B. zweimal jährlich neue Versionen (Featureupdates) bereitgestellt. Diese werden durch eine vierstellige Zahl beschrieben, wobei die ersten zwei Stellen die Jahreszahl und die letzten zwei Stellen den Monat angeben (d. h. Version 1803 steht für die Version vom März 2018). Systemaktualisierungen (Updates), die Fehler beheben und neue Funktionalitäten beinhalten, werden kontinuierlich aktualisiert und verändern

[1] https://en.wikipedia.org/wiki/Windows_10_editions
[2] Vergl.: https://www.heise.de/newsticker/meldung/Telemetrie-Daten-Windows-7-und-8-1-erhalten-Diagnose-Updates-jetzt-automatisch-4118229.html
[3] https://docs.microsoft.com/de-de/windows/deployment/update/waas-quick-start

damit das System des Nutzers nach jedem Update. Diese werden kumuliert zusammengefasst und als „builds“ bereitgestellt.[4]

Für die unterschiedlichen Anforderungen der Nutzer stellt Microsoft Windows 10 auch in verschiedenen Editionen (z. B. Home, Pro, Education, Enterprise, IoT) zur Verfügung.[5]

Windows 10 ist also der übergreifende Begriff für unterschiedliche von Microsoft bereitgestellte Systemumgebungen (Produktvarianten). Im Kern beinhalten alle diese Systemumgebungen ein Betriebssystem für Computer, das je nach Edition unterschiedliche Konfigurationsmöglichkeiten und Zusatzfunktionalitäten bietet. Durch den Updatemechanismus unterliegt die jeweilige Installation kontinuierlichen Veränderungen. Das Betriebssystem und die aktivierten Zusatzfunktionalitäten tauschen, je nach Konfiguration, Daten zwischen dem Computer und Microsoft aus.

Zur Bestimmung einer konkreten Produktvariante auf einem Computer ist also die Angabe der Produktfamilie (Windows 10), der Edition (z. B. Enterprise), der Architektur (z. B. 64-Bit), sowie der Version (z. B. 1803) und ggf. weiterer Merkmale (Sprache, Multimediapaket) notwendig.

Erst durch diese Angaben ist in einem Prüf- oder Beratungsfall festgelegt, welche Software eingesetzt wird, um darauf basierend entsprechende datenschutzrechtliche Aussagen treffen zu können.

Konfiguration von Windows 10

Nachdem der Verantwortliche die seinen Anforderungen entsprechende Produktvariante von Windows 10 gewählt hat, bietet Microsoft neben einer Standardinstallation auch die Möglichkeit, im Rahmen der Installation und auch später verschiedene Einstellungen an der Konfiguration vorzunehmen, um so den Service individuell anzupassen.

Allerdings unterscheiden sich die Einstellmöglichkeiten je nach gewählter Edition. So bietet die Enterprise-Edition die umfangreichsten Einstellmöglichkeiten, während bei der Home-Edition die geringsten Konfigurationsmöglichkeiten bestehen.

Bei einer Standardinstallation werden viele Einstellungen nicht so gesetzt, dass Windows 10 nur minimal personenbezogene Daten an Microsoft übermittelt.

Folgende Funktionen sind z. B. einzeln konfigurierbar: Position; Kamera; Mikrofon, Spracherkennung; Kontoinformationen, Kontakte, Kalender, Messaging, Funkempfang, Feedback & Diagnose, Hintergrund Apps, Browser Edge.

Eine detaillierte Darstellung von datenschutzfreundlichen Konfigurationseinstellungen findet sich z. B. in der Orientierungshilfe des Arbeitskreises Informationssicherheit der deutschen Forschungseinrichtungen.[6] Dabei ist zu beachten, dass die aufgezeigten Konfigurationsmöglichkeiten sich sowohl nach gewählter Edition und betrachteter Version unterscheiden können und dass durch Updates bestehende Konfigurationseinstellungen verändert werden können.

Datenübertragung an Microsoft

Die Nutzung von Windows auf privaten PCs und in Behörden- oder Unternehmensnetzwerken sowie der Anschluss an das Internet eröffnete Microsoft schon seit langer Zeit die Möglichkeit, Informationen über Betriebssystemaktivitäten und damit den Systemzustand eines Computersystems an eigene Server in den USA zu übertragen. Durch diese Datenübertragungen

[4] https://www.microsoft.com/de-de/itpro/windows-10/release-information
[5] s. z. B. https://en.wikipedia.org/wiki/Windows_10_editions
[6] https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf

können u. a. Fehler entdeckt, Produktverbesserungen initiiert und die Nutzung des Systems für den Nutzer optimiert werden.

Es werden eventuell auch personenbezogene Daten (z. B. IP-Adresse, Nutzerkonto, Position, Nutzerverhalten, Internetaktivität, Präferenzen, Suchaktivitäten und weitere) übermittelt. Dabei werden die Daten zum Teil verschlüsselt übertragen.

Microsoft selbst stellt Informationen über Konfigurationsmöglichkeiten bereit, mit denen die Kommunikation zu Microsoft unter Windows10 gesteuert werden kann.[7]

Verschiedene Untersuchungen zeigen allerdings, dass es aktuell nicht möglich ist, die Datenübertragung durch Konfiguration von Windows10 vollständig zu unterbinden.[8] Da die Datenübertragung verschlüsselt stattfindet, liegen keine detaillierten Erkenntnisse über die Natur der übertragenen Daten von einer unabhängigen Stelle vor.

B. Hinweise für die rechtliche Prüfung

Grundlage einer rechtlichen Prüfung ist die Beschreibung einer Verarbeitungstätigkeit. Der Einsatz von Windows 10 ist kein Selbstzweck, sondern wird von Verantwortlichen im Rahmen von Geschäftsprozessen bei der Verarbeitung personenbezogener Daten verwendet. Diese Verarbeitungstätigkeiten müssen beschrieben werden. Dazu gehört Art, Umfang, Umstände und Zwecke der Verarbeitung darzustellen. In diesem Rahmen ist zu ermitteln, ob und ggf. welche personenbezogenen Daten im Rahmen des Einsatzes von Windows 10 an Microsoft übermittelt werden.[9] Dabei sind die übermittelten Telemetriedaten und die Datenübermittlungen im Rahmen von sonstigen genutzten Funktionen von Windows 10 zu festzustellen.

Notwendigkeit einer Rechtsgrundlage für die Übermittlung von personenbezogenen Daten

Nachdem der Verantwortliche seinen Geschäftsprozess beschrieben und beispielsweise anhand der Dokumentation von Microsoft oder durch Einsatz entsprechender Tools wie MS Diagnostic Data Viewer festgestellt hat, welche personenbezogenen Daten an Microsoft für welche Zwecke übermittelt werden, ist zu prüfen, ob diese Übermittlungen rechtmäßig sind. Kann er dies nicht feststellen, so kann er auch nicht prüfen, ob eine Rechtsgrundlage für die Übermittlung vorliegt.

Bei der Übermittlung von Daten an Microsoft sind drei Fallgruppen zu unterscheiden.

- Verhinderung der Übertragung: Wird durch technische Maßnahmen verhindert, dass eine Übertragung von Daten an Microsoft stattfindet, dann benötigt der Verantwortliche auch keine Übermittlungsgrundlage. Er muss jedoch sicherstellen, dass die technischen Maßnahmen zur Verhinderung einer Übermittlung im Sinne von Art. 25 Abs. 1 DSGVO angemessen und wirksam sind. Gleichzeitig wäre damit eine mögliche Erhebung von personenbezogenen Daten durch Microsoft unter Nutzung der Mittel des Verantwortlichen unterbunden. Der Frage, ob Microsoft selber Verantwortlicher ist, müsste nicht weiter nachgegangen werden.
- Minimierung der Übermittlung: Die Enterprise-Edition lässt sich so konfigurieren, dass nur noch eingeschränkt Telemetriedaten[10] übermittelt werden. In diesen Fällen werden somit weiterhin Daten über die Nutzung des Systems übermittelt.

[7] https://docs.microsoft.com/de-de/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services

[8] z. B. https://www.lda.bayern.de/media/windows_10_report.pdf

[10] Zum Begriff der Telemetriedaten siehe Anlage 1

- Keine Minimierung der Übermittlung: In der dritten Konstellation werden Funktionen genutzt, durch die auch Dateiinhalte und somit auch personenbezogene Daten von Beschäftigten oder sonstigen betroffenen Personen durch den Verantwortlichen an Microsoft übermittelt werden können.

Sofern personenbezogene Daten an Microsoft übertragen werden (Fallgruppen 2 und 3), handelt es sich um rechtfertigungsbedürftige Übermittlungen durch den Verantwortlichen an Microsoft, da der Tatbestand des Art. 4 Abs. 1 Nr. 2 DSGVO durch die Übertragung von personenbezogenen Daten an Microsoft erfüllt wird.

In der Fallgruppe 2 richtet sich die datenschutzrechtliche Zulässigkeit der Übermittlung nach den Normen des Beschäftigtendatenschutzes, also in Niedersachsen beispielsweise nach § 88 NBG (für Tarifbeschäftigte i. V. m. § 12 NDSG) oder § 26 BDSG. Nach beiden Normen gilt der Grundsatz der Erforderlichkeit. D. h. die Übermittlung personenbezogener Daten von Beschäftigten an Microsoft müsste für die Durchführung der Beschäftigungsverhältnisse erforderlich sein. Es ist zu prüfen, ob der Zweck der Verarbeitung auch mit weniger intensiven Maßnahmen in etwa gleich gut erreicht werden kann. Also z. B. ob die gewünschte Funktion durch andere Anbieter auch ohne die Übermittlung von personenbezogenen Daten oder mit Übermittlung in geringerem Umfang angeboten wird. Darüber hinaus muss der Grundsatz der Verhältnismäßigkeit gewahrt bleiben.

In der Fallgruppe 3 richtet sich die datenschutzrechtliche Zulässigkeit regelmäßig nach Art. 6 DSGVO. Gemäß Art. 6 Abs. 1 S. 1 DSGVO muss für jede Verarbeitung personenbezogener Daten eine der Voraussetzungen des Art. 6 Abs. 1 lit. a bis f[11] DSGVO erfüllt sein. Die Verantwortlichen müssen prüfen, ob jede der festgestellten Übermittlungen rechtmäßig ist. Für die Verarbeitung von Beschäftigtendaten sind wieder die o. g. besonderen Rechtsvorschriften zu beachten.

Internationaler Datenverkehr

Die Übermittlung von personenbezogenen Daten erfolgt an Server in den USA. Daher sind die Normen über den internationalen Datenverkehr, die Art. 44 ff. DSGVO, anwendbar. Microsoft ist nach dem Privacy Shield zertifiziert. Auf der Grundlage von Privacy Shield hat die EU-Kommission beschlossen, dass personenbezogene Daten in die USA übermittelt werden dürfen, wenn das empfangende Unternehmen sich selbstzertifiziert hat, d. h. vereinfacht gesagt, sich auf die Einhaltung der Privacy Shield-Grundsätze verpflichtet hat, auf der Webseite des U.S. Department of Commerce als aktiver Teilnehmer geführt wird und der Umfang der Zertifizierung die fraglichen Datenübermittlungen abdeckt. Auf der Grundlage des Privacy Shields dürfen personenbezogene Daten in die USA gemäß Art. 45 Abs. 3 DS-GVO übermittelt werden.

Es ist darauf hinzuweisen, dass gegen die Rechtmäßigkeit des Privacy Shields derzeit Bedenken bestehen. Gegen den Angemessenheitsbeschluss der EU-Kommission zum Privacy Shieldwurden Ende 2016 zwei Klagen eingereicht. Auch das Verfahren „Schrems II“ (Az. C-311/18) könnte möglicherweise Auswirkungen auf den Angemessenheitsbeschluss der EU-Kommission zum Privacy Shield haben. Es wäre dann durch den Verantwortlichen zu prüfen, ob für Übermittlungen in die USA weiterhin die notwendigen Grundlagen existieren.

Technisch-organisatorischer Datenschutz

Die Prüfung des Einsatzes von Windows 10 in Behörden und sonstigen öffentlichen Stellen sowie in Unternehmen richtet sich zudem nach den Vorschriften über den technisch-organisatorischen Datenschutz.

[11] Hinweis: Nach Art. 6 Abs. 1 S. 2 DSGVO gilt der Buchstabe f nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

Grundlage einer Prüfung des technisch-organisatorischen Datenschutzes ist neben der Beschreibung der Geschäftsprozesse eine Strukturanalyse.

Art. 24 DSGVO sieht vor, dass der Verantwortliche unter Berücksichtigung des Risikos[12] für die Rechte und Freiheiten natürlicher Personen, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen zur Umsetzung der DSGVO trifft und dies nachweist. Art. 25 DSGVO regelt den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Nach Art. 32 DSGVO ist der Verantwortliche zur Herstellung eines angemessenen Sicherheitsniveaus bei der Verarbeitung personenbezogener Daten verpflichtet.

Insbesondere Art. 25 Abs. 1 DSGVO spielt bei der Auswahl eines Betriebssystems eine große Rolle. Danach ist der Verantwortliche verpflichtet, bereits bei der Festlegung der Verarbeitungsmittel sicherzustellen, dass geeignete technische und organisatorische Maßnahmen zur Wahrung der Datenschutzgrundsätze getroffen werden. Erwägungsgrund 78 verdeutlicht hierzu, dass den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen auch bei öffentlichen Ausschreibungen Rechnung zu tragen ist. Der Verantwortliche ist also verpflichtet, die Anforderungen der DSGVO für die Beschaffung seiner Verarbeitungsmittel zu konkretisieren und dasjenige auszuwählen, mit dem er die Grundsätze des Datenschutzes bei seinen Verarbeitungstätigkeiten nachweisbar wahrt. Es ist ihm verwehrt, sich darauf zu berufen, er setze lediglich ein fremdes Produkt ein, auf dessen Entwicklung er keinen Einfluss habe. Art. 25 Abs. 1 DSGVO verpflichtet nämlich den Verantwortlichen und nicht den Hersteller zu Datenschutz durch Technikgestaltung.

Mit dem eingesetzten Betriebssystem müssen die „Grundsätze“ des Datenschutzes eingehalten werden können. Wesentliche Prüfungsinhalte ergeben sich aus Art. 5 Abs. 1 DSGVO. Die Verarbeitung muss rechtmäßig erfolgen, sie darf nicht gegen Treu und Glauben verstoßen, muss transparent sein, die Zweckbindung wahren, dem Grundsatz der Datenminimierung entsprechen, nicht zur Unrichtigkeit von Daten führen, dem Grundsatz der Speicherbegrenzung entsprechen und die Integrität und Vertraulichkeit müssen durch angemessene technische und organisatorische Maßnehmen gewahrt werden.

Die Einhaltung der Grundsätze ist nach Art. 5 Abs. 2 DSGVO zu dokumentieren (Nachweispflicht des Verantwortlichen).

Für die Auswahl eines Betriebssystems ergibt sich aus diesen Normen für die Verantwortlichen, dass sie unter den auf dem Markt verfügbaren Betriebssystemen nur diejenigen einsetzen dürfen, welche die Datenschutzgrundsätze einhalten und dies im Rahmen der Rechenschaftspflicht dokumentieren müssen. Sofern diese Anforderungen nur durch ein Betriebssystem auf dem Markt erfüllt würden, stünde dem Verantwortlichen kein Entscheidungsspielraum bei der Auswahl zu. Sofern mehrere Betriebssysteme diese Anforderungen erfüllen oder durch eine entsprechende Konfiguration oder zusätzliche technische und organisatorische Maßnehmen erfüllen können, kann der Verantwortliche aus datenschutzrechtlicher Sicht frei zwischen diesen Betriebssystemen wählen.

Beim Einsatz von Windows 10 hat der Verantwortliche hinsichtlich des Nachweises der Einhaltung der Grundsätze des Art. 5 Abs. 1 DS-GVO die Konfigurationsmöglichkeiten und damit einhergehenden Datenübertragungen an Microsoft kritisch zu würdigen. Der Grundsatz der Datenminimierung verlangt nach Art. 5 Abs. 1 lit. c DSGVO, dass personenbezogene Daten dem Zweck angemessen und erheblich sein müssen sowie auf das für die Zwecke der Verarbeitung

[12] Zum Risikobegriff siehe auch Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen, abrufbar unter https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html.

notwendige Maß beschränkt sein müssen. Der Grundsatz der Rechtmäßigkeit nach Art. 5 Abs. 1 lit. a DSGVO verpflichtet den Verantwortlichen dazu, personenbezogene Daten nur auf rechtmäßige Art und Weise zu verarbeiten. Durch die zahlreichen, über die reine Betriebssystemfunktionalität hinausgehenden Funktionen und die damit verbundenen Datenübertragungen (s. o.) besteht das Risiko, dass personenbezogene Daten von Beschäftigten oder sonstigen betroffenen Personen unrechtmäßig an Microsoft übermittelt werden. Diesem Risiko muss mit angemessenen technisch-organisatorischen Maßnahmen begegnet werden. Die Identifikation und Behandlung dieses Risikos durch technisch-organisatorische Maßnahmen bedeutet nicht, dass deswegen auf eine Rechtsgrundlage verzichtet werden kann. Es geht vielmehr darum, die Verarbeitung so auszugestalten, dass sie „den Anforderungen dieser Verordnung“ genügt (Art. 25 Abs. 1 DSGVO), also in diesem Fall durch angemessene technisch-organisatorische Maßnahmen zu verhindern, dass es zu unrechtmäßigen Übermittlungen an Microsoft kommt.

Nach Art. 25 Abs. 1 DSGVO ist zu prüfen, welche Maßnahmen im konkreten Fall wirksam und angemessen sind. Grundlage hierfür ist die Schwere und Eintrittswahrscheinlichkeit des Risikos. Die Schwere des Risikos hängt von den jeweils verarbeiteten Daten, aber auch vom Umfang und den von Microsoft verfolgten Zwecken ab. Die Bewertung der Schwere ist entsprechend zu begründen. Die Eintrittswahrscheinlichkeit hierfür kann durch die Maßnahmen verringert werden.

Bei der Auswahl der Maßnahmen zur Verhinderung der Offenlegung von personenbezogenen Daten sind neben der Höhe des Risikos, der Stand der Technik und die Implementierungskosten zu berücksichtigen. In Betracht kommt zunächst die datensparsame Konfiguration von Windows 10. Da Windows 10 bei der Standardinstallation nicht entsprechend vorkonfiguriert ist, muss dies durch den Verantwortlichen geleistet werden. Da sich derzeit aber nicht alle Übermittlungen an Microsoft durch eine entsprechende Konfiguration deaktivieren lassen, müssen daneben weitere technische Maßnahmen zur Verhinderung einer unbefugten Übermittlung zum Einsatz kommen. Neben der technischen Verhinderung der Datenübermittlung von Windows 10 an Microsoft muss wegen dem fortlaufenden Verändern und Hinzufügen von Funktionalität zudem ebenso fortlaufend überwacht werden, ob anlässlich eines Updates eine erneute Prüfung durchgeführt werden muss.

C. Übersicht über die Prüfung des Einsatzes von Windows 10

Die folgende Übersicht ersetzt nicht die Auseinandersetzung mit den obigen Ausführungen. Es soll vielmehr zusammenfassend ein Überblick über die herausgearbeiteten Prüfungspunkte gegeben werden.

1. Beschreibung der Verarbeitungstätigkeit

Grundlage für die Prüfung ist die Bestimmung des Prüfungsgegenstandes. Art, Umfang und Umstände der Verarbeitung müssen erfasst werden. Welche Edition soll in welcher Version zum Einsatz kommen und welche Funktionen und Datenübermittlungen sind damit verbunden? Welche Verarbeitungsvorgänge (z. B. Fachverfahren) finden unter Nutzung von Windows 10 statt?

2. Prüfung der Rechtmäßigkeit der Datenübermittlungen

Die festgestellten Datenübermittlungen und die damit verbundenen Übermittlungen von personenbezogenen Daten sind auf ihre Rechtmäßigkeit zu prüfen. Die möglichen Rechtsgrundlagen hängen von der jeweiligen Funktion und den übermittelten Daten ab. Soweit für die Übermittlung eine Rechtsgrundlage vorliegt, kann Windows 10 oder können bestimmte Funktionen von Windows 10 genutzt werden. Konnte nicht festgestellt werden, welche Daten übermittelt werden, so kann auch nicht die Rechtmäßigkeit der Übermittlung festgestellt werden.

3. Auswahl angemessener Maßnahmen

Es sind Maßnahmen zu treffen, mit denen eine unrechtmäßige Offenlegung von Daten verhindert wird. Die Auswahl von angemessenen Maßnahmen ist abhängig vom Stand der Technik, den Implementierungskosten und den Risiken für die Rechte und Freiheiten der betroffenen Personen. Neben der technischen Verhinderung einer unrechtmäßigen Offenlegung von personenbezogenen Daten sind auch Maßnahmen zu treffen, durch die überprüft wird, ob diese getroffenen Maßnahmen auch nach Updates weiterhin einen angemessenen Schutz gewährleisten. Die getroffenen Maßnahmen und ihre Einhaltung sind nach Art. 5 Abs. 2 DSGVO zu dokumentieren.

4. Restrisikobewertung

Sodann ist eine Restrisikobewertung durchzuführen. In Anbetracht der vom jeweiligen Einzelfall abhängenden Schwere und Eintrittswahrscheinlichkeit unter Berücksichtigung der getroffenen Maßnahmen ist das Restrisiko ggfs. auch im Rahmen einer Datenschutz-Folgenabschätzung zu bewerten und zu beurteilen, ob dieses Restrisiko tragbar ist. Ist das Restrisiko nicht tragbar, ist die zuständige Aufsichtsbehörde gemäß Art. 36 DS-GVO zu konsultieren. Ist es nicht möglich, das hohe Risiko mit weiteren Maßnahmen auf ein tragbares Maß zu reduzieren, muss der Einsatz von Windows 10 unterbleiben.

5. Implementierung der Maßnahmen und Überprüfung ihrer Wirksamkeit

Die ermittelten Maßnahmen sind zu implementieren und auf ihre Wirksamkeit zu überprüfen.

6. Nutzung von Windows 10

Wenn das Restrisiko durch die Implementierung der Maßnahmen tragbar ist, kann Windows 10, bzw. können bestimmte Funktionen von Windows 10 zum Einsatz kommen.

7. Update

Bei einem Update besteht die Möglichkeit, dass neue Funktionen aktiviert werden, bestehende Funktionen verändert werden, Konfigurationsmöglichkeiten verändert werden oder die durch den Verantwortlichen getätigte Konfiguration verändert wird. Der Verantwortliche wird prüfen müssen, inwieweit sich dadurch die Effektivität der Maßnahmen zur Verhinderung einer unrechtmäßigen Offenlegung verändert hat. Ggf. darf eine Versionsänderung nicht durchgeführt werden, bevor die Maßnahmen nicht angepasst wurden und ein fortwährender Einsatz im Einklang mit der Verordnung wieder gewährleistet werden kann.

Die Prüfung lässt sich z. B. folgendermaßen grafisch darstellen:

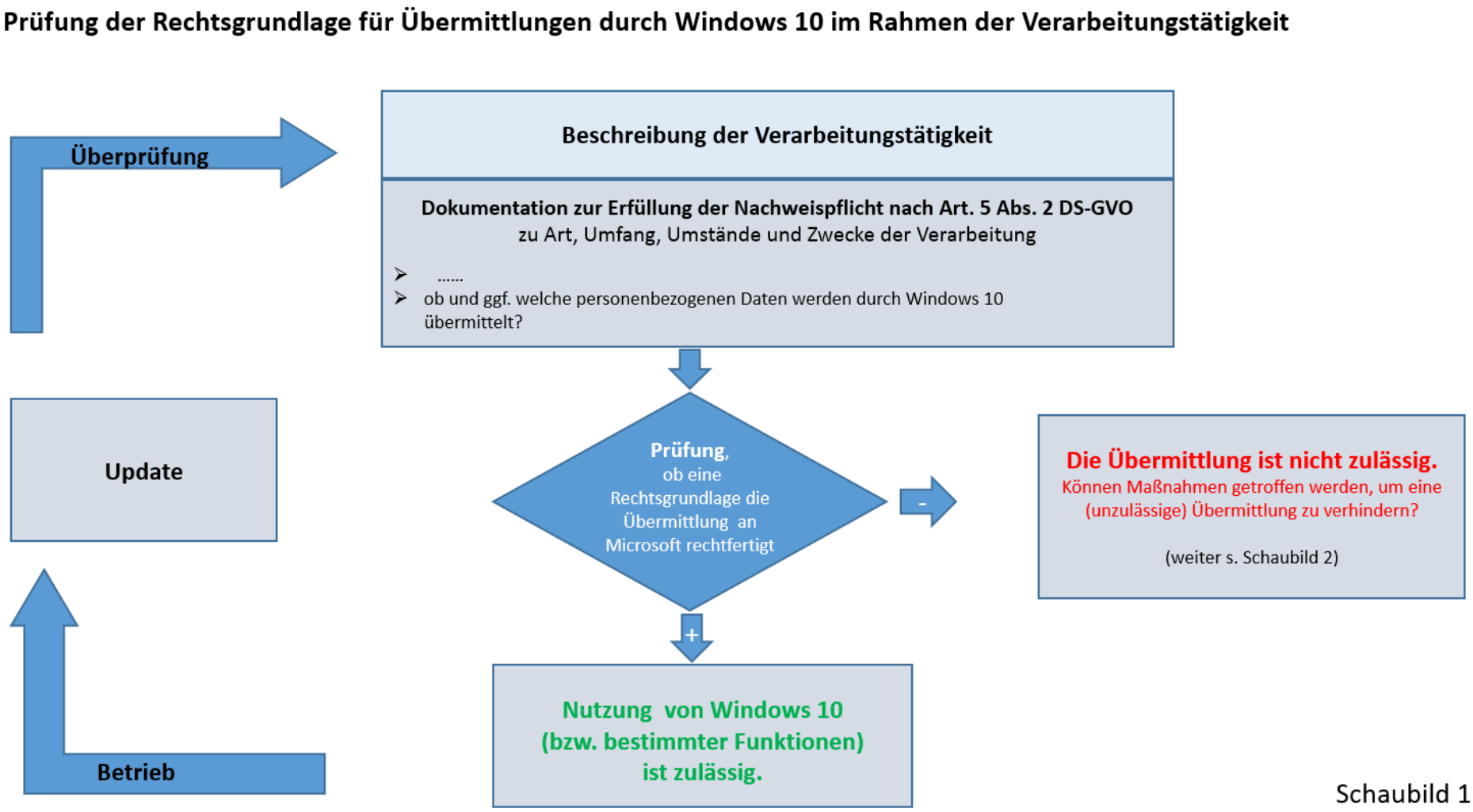

Schaubild 1

Prüfung der Maßnahmen zur Unterbindung von Übermittlungen

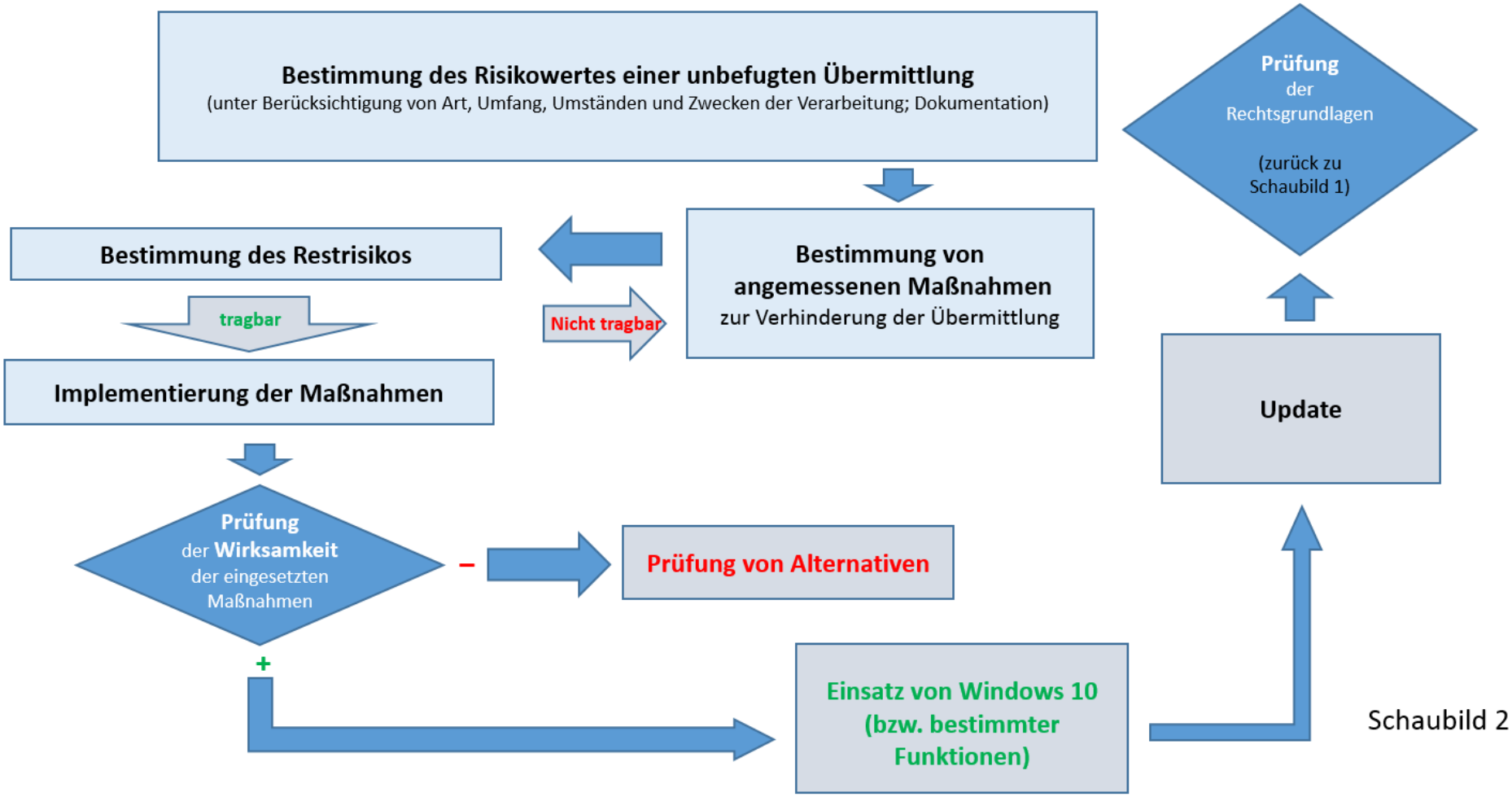

Schaubild 2