Der Diözesandatenschutzbeauftragte

des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Arbeitshilfe
AH 704

Datenschutzfreundlicher Einsatz von Windows 10

im Erzbistum Hamburg,
den Bistümern Hildesheim und Osnabrück
und dem Bischöflich Münsterschen Offizialat in Vechta i.O.

Stand: 08/2018

Herausgegeben vom

Diözesandatenschutzbeauftragten
des Erzbistums Hamburg
der Bistümer Hildesheim, Osnabrück und
des Bischöflich Münsterschen Offizialats in Vechta i.O.

Unser Lieben Frauen Kirchhof 20
28195 Bremen

Tel.: 0421 / 16 30 19 25
Mail: info@datenschutz-katholisch-nord.de

Diese Arbeitshilfe können Sie auch auf unserer Internetseite abrufen unter:
https://www.datenschutz-kirche.de/

Inhaltsverzeichnis

I. Einleitung

Windows 10 ist das aktuelle Betriebssystem nach Windows 7 für Endverbraucher und Unternehmen. Bei diesem Einsatz stellt sich die Frage, ob und wie Windows 10 datenschutzkonform eingesetzt werden kann. Den Forderungen aus der EU-Datenschutzgrundverordnung nach Datenschutz durch Technik (data protection-by-design) oder Datenschutz durch Voreinstellungen (data protection-by-default) kommt Windows 10 in den Standardeinstellungen dabei zunächst nicht nach.

Windows 10 bietet aber eine Reihe von Möglichkeiten, um datenschutzrelevante Anpassungen vorzunehmen. Im Folgenden werden diese Einstellungsmöglichkeiten erläutert und die Möglichkeit einer datenschutzfreundlichen Konfiguration vorgestellt.

Auch kostenlose AntiSpy-Tools, wie z.B. „ShutUp10“ von dem Softwarehersteller O&O, können helfen, datenschutzkonforme Einstellungen unter Windows 10 vorzunehmen.

Im Abschnitt II werden zunächst die Einstellungsmöglichkeiten in Windows 10 erläutert. Abschnitt 3 befasst sich mit der Benutzeranmeldung und datenschutzrelevanten Einstellungen. Windows Updates und eine Empfehlung für Windows 10 Enterprise werden in den Abschnitten 4 und 5 behandelt. In Abschnitt 6 wird die Konfiguration von Windows 10 mit Empfehlungen aus der IT-Sicherheit aufgezeigt. Abschließend befasst sich Abschnitt 7 mit den rechtlichen Anforderungen, welche beim Einsatz von Windows 10 zu beachten sind.

II. Wichtige Menüpunkte für datenschutzrelevante Einstellungen in Windows 10

Ein Großteil der datenschutzrelevanten Einstellungsmöglichkeiten befindet sich im Menü **„Einstellungen>>Datenschutz“**. Weitere relevante Einstellungen sind unter **„Einstellungen>>Konten>>Einstellungen synchronisieren“**, sowie im Edge-Browser zu finden. Unter den Gruppenrechtlinien können erweiterte Einstellungen vorgenommen werden. Den Menüpunkt **„Einstellungen“** kann entweder mit einem Rechtsklick auf das Windows-Symbol unten links oder über die Tastenkombination **[Windows-Taste]+[I]** aufgerufen werden. Aber auch durch die Eingabe des jeweiligen Begriffs in dem Suchfeld (Lupe) unten links gelangt man in das jeweilige Menü.

III. Kontoanmeldung und Synchronisation

Unter **„Konten>>Ihre Infos“** wird festgelegt, ob eine Anmeldung mit dem lokalen Benutzerkonto oder mit einem Windows-Live-Konto am PC erfolgen soll. Bei der Nutzung eines Windows-Live-Kontos werden u.a. Konfigurationsdaten in der Microsoft OneDrive-Cloud gespeichert. Die Speicherung der Daten erfolgt auf Server weltweit, eine Auswahl zur Nutzung der europäischen bzw. der Microsoft Deutschland Cloud besteht nicht. Die Übermittlung von personenbezogenen Daten in Drittländer ist nur unter bestimmten, engen Voraussetzungen zulässig. Aus diesem Grund ist der dienstliche Einsatz des (privaten) Windows-Live-Kontos nicht zulässig, womit ausschließlich die Nutzung des lokalen Benutzerkontos in Betracht kommt.

Zusätzlich sind die OneDrive Einstellungen im Such Menü unter Gruppenrichtlinie **„Computerkonfiguration>>Administrative Vorlage>>Windows-Komponenten>>OneDrive“** anzupassen. Es ist empfohlen diese Richtlinie zu aktivieren bzw. zu deaktivieren.

In dem Internet Explorer unter **„Extra>>Internetoptionen>> im Register Erweitert >>Browsen“** ist der Punkt **„Synchronisierung von Internet-Einstellungen und Daten aktivieren“** zu kontrollieren und ggf. zu deaktivieren.

https://trusted.de/microsoft-onedrive-test

1. Datenschutz Einstellungen Allgemein

In **„Einstellungen>>Datenschutz“** sind die meisten Optionen, die den Schutz der Privatsphäre in Windows 10 beeinflussen.

Im Menü **„Allgemein“** wird festgelegt, ob Apps und Browser die Werbe-ID zur Identifizierung verwenden darf. Diese Anwendungen analysieren und speichern das Nutzerverhalten für Werbezwecke. Diese soll personalisiert in installierten Apps und im Microsoft-Edge-Browser eingespielt werden. Die Punkte unter **„Allgemein“** sind zu deaktivieren. Rechts auf der Seite sind weitere Einstellungen zum Datenschutz unter dem Begriff **„Datenschutz-Dashboard“** zu finden. Auf der weitergeleiteten Seite ist unter dem Punkt „Werbeeinstellungen“ die personalisierte Werbung zu deaktivieren.

Dieses Opt-Out wird nur im Browser gespeichert und muss ggf. für alle verwendeten Browser wiederholt werden.

https://account.microsoft.com/privacy/ad-settings/signedout?ru=https:%2F%2Faccount.microsoft.com%2Fprivacy%2Fad-settings

2. **Spracherkennung, Freihand und Eingabe**

- Informationen zum Schreibverhalten: Getippte und handgeschriebene Wörter werden gesammelt und Microsoft bereitgestellt. Die Daten sollen u.a. zur Verbesserung der Schrifterkennung und der Eingabevorschläge verwendet werden.
- Zugriff auf Sprachliste: Anhand der übertragenen Sprachliste möchte Microsoft dem Benutzer regionalrelevante Vorschläge und Angebot unterbreiten. Es gibt keine Informationen dazu, welche Daten genau im Rahmen der Spracheliste übertragen werden.

Unsere Empfehlung ist es die folgenden Anpassungen vorzunehmen und bei Nichtnutzung der Spracherkennung diesen Dienst komplett zu deaktivieren. Durch die Eingabe **„Cortana“** in dem Suchfeld (Lupe) und die Auswahl **„Cortana & Sucheinstellungen“** unter **„Berechtigungen & Verlauf“** können die Webergebnisse, Cloudsuche und der Geräteverlauf angepasst werden. Um **„Cortana“** vollständig zu deaktivieren, ist im Registrierungs-Editor unter dem Punkt **„Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search“** der Eintrag **„AllowCortana“** auf **„0“** zu setzen und mit **„OK“** zu bestätigen. Die **„Cortana-Suche“** ist nach einem **„Neustart“** des PCs deaktiviert.

3. **Diagnose und Feedback**

Hier kann eingestellt werden, wie häufig und in welchem Umfang Systeminformationen, Diagnose- und Nutzerdaten sowie Windows-Defender-Berichte an Microsoft übermittelt werden. Die Auswertung der Telemetriedaten sollen Microsoft zur Verbesserung von Windows 10 und zur Behebung von Problemen dienen. Der Eintrag unter **„Einstellungen>>Datenschutz>>Diagnosedaten und Feedback“** ist auf **„Einfach“** zustellen. Alle weiteren Einstellungsmöglichkeiten sind auf **„Aus“** zusetzen und **„Feedbackhäufigkeit“** auf **„Nie“**. Unter
„Gruppenrichtlinien bearbeiten>>Richtlinien für Lokaler Computer>>Computerkonfiguration>>Administrative Vorlagen>>Windows-Komponenten>>Datensammlung und Vorabversionen>>Telemetrie zulassen“
ist zwischen den Werten **„0-Sicherheit“** (nur bei Windows 10 Enterprise möglich), **„1-Einfach“**, **„2-Erweitert“** und **„3-Vollständig“** zu wählen. Bei welchem Wert, wie viele Daten erfasst werden ist hier aufgeführt:

- **„0-Sicherheit“** (nur Windows 10 Enterprise): Die Einstellung **„0-Sicherheit“** wird unter Windows 10 Home und Pro nicht berücksichtigt. Es wird eine Einstellungsdatei zur Telemetrie angefordert. Im Rahmen der Anforderung werden das verwendete Betriebssystem, die Geräte-ID und die Geräte-Klasse gesendet. Wenn das „Tool zum Entfernen bösartiger Software“ und Windows Defender eingesetzt werden, senden diese Infektionsberichte und relevante Informationen für die Malwarebekämpfung.
- Hinweis: Beim Einsatz der Einstellung Sicherheit kann Microsoft bei Windows Update keine Informationen zum Updatestatus sammeln, z.B. ob ein Update erfolgreich angewendet wurde. Der Einsatz von WSUS ist zu empfehlen.
- **„1-Einfach“**: Es werden außerdem Informationen über die Hardware des Gerätes, Diagnosedaten zum Betrieb des Gerätes (Nutzungsprofil zu genutzten Apps, Häufigkeit von Abstürzen, Prozessor-/Speichernutzung Informationen installierte Software und Treiber) gesendet. Bei der Nutzung vom Windows Store werden dazu auch genauere Informationen gesammelt und gesendet.
- **„2-Erweitert“**: Es werden zusätzlich Ereignisse des Betriebssystems, von Microsoft-Apps und von angeschlossenen Geräten übertragen. Wenn ein Problem erkannt wird, werden dazu passende Ereignisse aus den letzten zwei Wochen übermittelt. Bei Abstürzen (Betriebssystem oder App) werden Arbeitsspeicherinhalte vom fehlerhaften Prozess übertragen.
- **„3-Vollständig“**: Zur Fehlerbehebung werden auch beliebige Nutzerdaten gesammelt und übertragen. Es können Diagnosetools ausgeführt werden, Registrierungsschlüssel abgerufen werden und Benutzerinhalte wie Dokumente übertragen werden. Die Übertragung von Nutzerdaten erfolgt nach Freigabe durch das Microsoft Datenschutz-Governance-Team.

https://technet.microsoft.com/library/mt577208(v=vs.85).aspx#BKMK_UTC_Security

4. Aktivitätsverlauf

Windows 10 zeichnet in dem **„Aktivitätsverlauf“** auf, welche Apps benutzt wurden, welche Webseiten besucht worden sind und bietet die Möglichkeit, zu vergangenen Aktivitäten zu wechseln. Unter **„Einstellungen>>Datenschutz>>Aktivitätsverlauf“** ist das Kästchen **„Windows meine Aktivitäten auf diesem PC sammeln lassen**“ ausgewählt. Bei Windows 10 Pro sind die drei Richtlinien unter

„Gruppenrichtlinien bearbeiten>>Computerkonfiguration>>Administrative Vorlage>>System>>Betriebssystemrichtlinien“ mit einem Doppelklick zu öffnen und zu deaktivieren.

5. Position

Standardmäßig ermittelt Microsoft den Standort des Gerätes, um standortspezifische Informationen einzublenden, z.B. Weginformationen oder Restaurants auf Karten. Der Positionsdienst kann unter **„Einstellungen>>Datenschutz>>Position“** generell ausgeschaltet werden oder seine Nutzung auf bestimmte Apps eingeschränkt werden. Zu löschen ist der Positionsverlauf unter dem Punkt **„Verlauf auf diesem Gerät löschen“**.

Die Dienste **„Mein Gerät suchen“** und „**WLAN-Optimierung“** dürfen unabhängig von den Einstellungen auf die Position zugreifen. „Kann mein Gerätestandort erkannt werden, wenn der Windows-Positionsdienst für das Benutzerkonto deaktiviert ist?“. Über diese Einstellung wird außerdem nur die Standortbestimmung über den Windows-Positionsdienst gesteuert, App-spezifische Positionserkennungen, z.B. über WLAN sind hiervon unabhängig.

6. Weitere Datenschutzeinstellungen

Unter den weiteren **„Einstellungen>>Datenschutz“** können die Nutzungsrechte für verschiedene Ressourcen des Betriebssystems, z.B. **„Kamera“**, **„Mikrofon“**, **„Kontakte“**, etc. eingestellt werden. Dabei gibt es generell die Möglichkeit, die Funktion **„Gerätezugriff“** zu deaktivieren oder nur für bestimmte Apps einzuschränken. Es sollte genau geprüft und abgewogen werden, welche Dienste zwingend erforderlich sind. Ansonsten sollten Zugriffe auf die verschiedenen Daten und die App-Funktionen deaktiviert werden.

7. Microsoft Edge

Im Edge-Browser gibt es die **„Seitenvorhersage-Option“.** Mit Hilfe dieser Funktion werden Daten von aufgerufenen Webseiten an Microsoft übertragen. Während des Besuchs einer Internetseite werden die Daten analysiert und im Hintergrund geladen, um den Zugriff auf Seiten, welche voraussichtliche besucht werden, zu beschleunigen. Dieser Vorgang wird auch als „Prefetching“ bezeichnet. Die Funktionalität der Seitenvorhersage wird beinahe von allen gängigen Browsern unterstützt, um dem Anwender ein schnelleres Nutzungserlebnis bieten zu können. Im Edge-Browser findet man die Einstellung unter **„Einstellungen und**

mehr>> (drei Punkte oben rechts) Einstellungen>>Erweiterte Einstellungen anzeigen“ als vorletzte Position.

Weitere Browser-Einstellungen, z.B. für **„Cookies“** oder **„Beste Websites“** sollten hier ebenfalls Beachtung finden.

8. Windows Spotlight

Das **„Windows Spotlight“**-Feature erlaubt es, zufällige Bilder im Login-Screen anzuzeigen, zu den angezeigten Bildern gehört auch Werbung zu Artikeln die im Windows Store gekauft werden können. Windows fragt außerdem nach Feedback zu den angezeigten Bildern, um diese gemäß dem eigenen Interesse zu personalisieren. Die Spotlight-Funktion kann unter **„Einstellungen>>Personalisierung>>Sperrbildschirm“** deaktiviert werden, in dem der Hintergrund **„Bild oder Diashow“** ausgewählt ist und die Option **„Unterhaltung, Tipps, Tricks und mehr auf dem Sperrbildschirm anzeigen“** ausgestellt wird.

9. WLAN-Optimierung

Die Funktion **„WLAN-Optimierung“** setzt die Anmeldung mit einem Windows-Live-Konto voraus. Bei der **„WLAN-Optimierung“** werden WLAN-Namen und dazugehörige Zugangsdaten, als Hash, mit den Kontakten geteilt, um den einfachen Zugang zu bekannten und öffentlichen WLAN-Netzwerken zu ermöglichen. Unter **„Einstellungen>>Netzwerk und Internet>>WLAN“** sind die Anpassungen vorzunehmen und die Freigaben zu deaktivieren.

10. Windows-Suche

In Windows 10 ist es möglich, direkt über die Desktop-Suche Anfragen an Web-Suchmaschinen zu stellen. Es können auch weitere Informationen, wie Benutzerinformationen und Position, an die Suchmaschine weitergegeben werden, um das Suchergebnis zu verbessern. Außerdem ist es möglich, verschlüsselten Dateien indizieren zu lassen und dadurch die verschlüsselte Datei in die Suche zu integrieren. Bei der Dateisuche kommt es darauf an, was in den Indizierungsoptionen eingestellt ist. Diese sind unter **„Indizierungsoptionen“** zu finden. Dort können Ordner hinzugefügt oder ausgeschlossen werden. Sollte dort ein Internetbrowser mit aufgeführt sein ist dieser zu löschen. In den erweiterten Optionen der Indizierung lassen sich auch Dateitypen hinzufügen oder entfernen.

IV. Windows Updates und neue Anwendungen

Generell sollten die monatlichen Sicherheitsupdates, die Microsoft zur Verfügung stellt, regelmäßig installiert werden. Häufig werden aber nicht nur Patches durch die Updates in das Windows 10 eingespielt, sondern auch neue Microsoft-Anwendungen. Diese Anwendungen sind auf Datenschutzkonformität zu prüfen und die Datenschutzeinstellungen anzupassen.

V. Empfehlungen für Windows 10 Enterprise

Die meisten datenschutzrelevanten Einstellungen können bereits ab den Windowsversionen Home oder Professional (Pro) vorgenommen werden. Die Windows 10 Home Version, für den Heimbereich, verfügt über keine Domänenmitgliedschaft und über keine Gruppenrichtlinien. Bei einer Domäne handelt es sich um einen Netzwerkbereich, in dem User Sicherheitsrichtlinien und Benutzerrechte erhalten. Bei Gruppenrichtlinien wird grundsätzlich zwischen domänenweiten Gruppen und lokalen Gruppenrichtlinien unterschieden. In den Windows 10 Pro Gruppenrichtlinien fehlen viele Einstellungen zum Datenschutz, der Sicherheit und vor allem zum Windows Store. Besonders interessant ist für Unternehmen die Edition Windows 10 Enterprise, die weitere Funktionen mit sich bringt und alle Einstellungsmöglichkeiten über Gruppenrichtlinien bietet. Auf Grund des höheren Datenschutzniveaus und dem geringeren Verwaltungsaufwand sollte, wenn möglich, die Enterprise-Edition bevorzugt werden.

VI. Empfehlungen für eine sichere Konfiguration von Windows 10

Bei der Konfiguration von Windows 10 sollte nicht nur die Datensparsamkeit beachtet werden, sondern auch IT-Sicherheitseinstellungen vorgenommen werden. Aus Sicht der IT-Sicherheit sind zusätzlich folgende Aspekte zu beachten:

- Windows Store: Windows 10 verfügt genau wie iOS oder Android über einen App-Store, mit dem Apps gekauft und auf den Geräten installiert werden können. Auf dienstlichen IT-Systemen sollte der Zugriff auf den Windows Store aber verhindert werden, damit die Anwender keine nicht-freigegebene Software installieren können.
- OneDrive deaktivieren: In Windows 10 ist OneDrive-Cloud zur Ablage von Daten in vielen Apps integriert und wird oft auch als Standardspeicherplatz angeboten. Damit nicht ausversehen in der Cloud anstatt auf dem lokalen Computer oder einem Netzlaufwerk gespeichert werden, sollte OneDrive deaktiviert werden. Dies kann durch die

Richtlinie unter **„Gruppenrichtlinie>>Computerkonfiguration>>Administrative Vorlage>>Windows-Komponenten>>OneDrive“** erfolgen und es ist empfohlen die Einstellungen anzupassen. (Siehe 3.)

VII. Rechtliche Vorgaben

Nach § 7 Abs. 1 lit. c) Gesetz über den Kirchlichen Datenschutz (KDG) müssen personenbezogene Daten auf das „für den Zweck der Verarbeitung notwendige Maß beschränkt sein“ (Grundsatz der Datenminimierung). Zudem ist in § 27 die Grundsätze privacy by default (Grundsatz Datenschutz durch datenschutzfreundliche Voreinstellungen) aufgenommen worden. Es sind daher zumindest alle technisch möglichen Maßnahmen zu ergreifen, um einen sparsamen Datenaustausch mit Microsoft zu gewährleisten.

Die oben beschriebenen Funktionalitäten von Windows 10 bieten keinen erheblichen Zugewinn bzw. deren Abschaltung keine erheblichen Einschränkungen für den Nutzer, womit sich eine Datenübermittlung an Microsoft rechtfertigen ließe. Es ist IT-Administratoren daher zu empfehlen, das System so datensparsam wie möglich zu konfigurieren.

Erst bei erheblichen Einschränkungen der Funktionalität kann im Einzelfall eine abweichende Beurteilung möglich sein. Diese kann weitere Maßnahmen, z.B. Information des Windows-Nutzers, erforderlich machen.
Ganz unproblematisch bleibt der Einsatz von Windows 10 auch bei der sparsamsten Einstellung nicht, da bestimmte Datenschutzeinstellungen erst in der Enterprise-Version (s. Abschnitt 5.) verfügbar sind. Daher können Datenflüsse an Microsoft nie vollständig unterbunden werden und damit bleiben Zweifel an einer vollständigen Transparenz der Verarbeitung. Jedoch wird man angesichts der marktbeherrschenden Stellung von Microsoft von keiner schuldhaften Pflichtverletzung durch den Verwender ausgehen können, sofern alle technischen Möglichkeiten zur Reduzierung des Datenflusses ausgeschöpft werden.

VIII. Literatur

Windows 10 und Onlinedienste:

http://windows.microsoft.com/de-de/windows-10/services-setting-preferences

Verwalten von Verbindungen zwischen Komponenten des Windows-Betriebssystems und Microsoft-Diensten:

https://technet.microsoft.com/de-de/library/mt577208(v=vs.85).aspx

Windows 10 Positionsdienste und Datenschutz:

http://windows.microsoft.com/de-de/windows-10/location-service-privacy

Die Windows Einstellungen zur Privatsphäre:

https://www.heise.de/ct/ausgabe/2018-15-Die-Windows-Einstellungen-zur-Privatsphaere-4095760.html

Hinweis in eigener Sache

Der Inhalt dieser Arbeitshilfe wurde mit größter Sorgfalt erstellt und erhebt keinen Anspruch auf Vollständigkeit.

Diese Arbeitshilfe dient in erster Linie dazu, Ihnen bei der täglichen Arbeit die Einbindung der datenschutzrechtlichen Bestimmungen zu erleichtern. Sie berücksichtigt die Vorschriften des KDG durch den Diözesandatenschutzbeauftragten zum derzeitigen Zeitpunkt.

Sollten sich Unklarheiten oder offensichtliche Fehler aus dieser Arbeitshilfe ergeben, so bitten wir um einen entsprechenden Hinweis unmittelbar an den Diözesandatenschutzbeauftragten. Die Kontaktinformationen können Sie dieser Arbeitshilfe entnehmen.