Der Diözesandatenschutzbeauftragte

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

DATENSCHUTZ
IN DER KATHOLISCHEN KIRCHE

Datenschutzfreundlicher Einsatz von Windows 10

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

datenschutz nord GmbH

April 2016

Inhaltsverzeichnis

1. Einleitung

Es zeichnet sich ab, dass Windows 10 die Nachfolge von Windows 7 als Betriebssystem für Endverbraucher und Unternehmen antreten wird. Bei diesem Einsatz stellt sich die Frage, ob und wie Windows 10 datenschutzkonformen 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.

Im Abschnitt 2 werden zunächst die Einstellungsmöglichkeiten in Windows 10 erläutert. In Abschnitt 3 wird der Einsatz von Windows 10 rechtlich in Bezug auf die KDO und die spätere EU-Datenschutzgrundverordnung bewertet, bevor in Abschnitt 4 anschließend eine datensparsame Konfiguration für Windows 10 vorgeschlagen wird. Abschließend wird in Abschnitt 5 die Konfiguration von Windows 10 mit Empfehlungen aus der IT-Sicherheit abgerundet.

2. Datenschutzrelevante Funktionen von Windows 10

Ein Großteil der datenschutz-relevanten Einstellungsmöglichkeiten findet sich im Menü „Einstellungen>>Datenschutz“. Weitere relevante Einstellungen finden sich aber auch unter „Konten>>Einstellungen synchronisieren“ sowie im Edge Browser, der den Nachfolger des Microsoft Internet Explorers darstellt.

2.1 Allgemeine Datenschutz Einstellungen

In den allgemeinen Datenschutzeinstellungen können folgende Einstellungen vorgenommen werden:

--- Werbungs-ID: Zur Identifizierung über verschiedene Webseiten und Apps hinweg wird eine Werbungs-ID mit dem hinterlegten Microsoft-Live-Konto verknüpft. Die Werbung soll personalisiert in installierten Apps und im Microsoft-Edge-Browser eingespielt werden. Zum vollständigen Abschalten der personalisierten Werbung muss außerdem ein Opt-Out auf der Seite https://choice.microsoft.com/de-de/opt-out# vorgenommen werden. Das Opt-Out wird nur im Browser gespeichert und muss ggf. für alle verwendeten Browser wiederholt werden.

--- 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.

2.2 Feedback und Diagnose

Hier kann eingestellt werden, wie häufig und in welchem Umfang Diagnose- und Nutzerdaten an Microsoft übermittelt werden. Diese Einstellung erfolgt unabhängig von der Datenweitergabe zur Verbesserung von Windows 10 und zur Problembehandlung (s. Abschnitt 2.3). Beim Umfang der Datensammlung gibt es folgende Einstellungsmöglichkeiten:

--- Sicherheit (nur Windows 10 Enterprise)[1]: 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.

--- Einfach[2]: 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.

--- Verbessert[3]: 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.

--- Vollständig[4]: 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

Für Windows Enterprise kann die Übertragung von Diagnosedaten über die „AllowTelemetry“-Richtlinie deaktiviert werden. Wenn diese Einstellung für Windows Home oder Pro vorgenommen wird, wird die Einstellung ignoriert und Diagnosedaten werden gemäß Ausprägung Einfach übertragen.

In diesem Menü kann außerdem die Häufigkeit der Feedbackanforderung durch Windows eingestellt werden, Feedback wird allerdings nur angefordert, wenn die Diagnosedaten auf Vollständig gestellt sind.

[1] https://technet.microsoft.com/library/mt577208(v=vs.85).aspx#BKMK_UTC_Security
[2] https://technet.microsoft.com/library/mt577208(v=vs.85).aspx#BKMK_UTC_Basic
[3] https://technet.microsoft.com/library/mt577208(v=vs.85).aspx#BKMK_UTC_Enhanced
[4] https://technet.microsoft.com/library/mt577208(v=vs.85).aspx#BKMK_UTC_Full

2.3 Datenweitergabe zur Verbesserung von Windows 10 und zur Problembehebung

In Windows 10 sind verschiedene Mechanismen enthalten, die zur Verbesserung von Windows 10 oder zur Behebung von Problemen automatisch Daten an Microsoft senden. Dazu gehört z.B. das Customer Experience Improvement Program, mit dem Informationen über den Computer, Hardware und die Nutzung gesammelt und zur Auswertung an Microsoft gesendet werden.

Außerdem können bei Problemen in Windows vom Windows Error Reportings, Inventory Collector oder Windows Defender automatisch Daten an Microsoft weitergeleitet werden, bzw. Daten später von Microsoft angefordert werden.

2.4 Position

Standardmäßig ermittelt Microsoft den Standort des Gerätes, um standortspezifische Informationen einzublenden, z.B. Weginformationen oder Restaurants auf Karten. Der Positionsdienst kann generell ausgeschaltet werden oder seine Nutzungauf bestimmte Apps eingeschränkt werden.

Die Dienste Mein Gerät suchen und WLAN-Optimierung dürfen unabhängig von den Einstellungen auf die Position zugreifen (siehe [MS15LS] „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.

2.5 Personalisierte Spracherkennung, Freihand und Eingabe

Zur Verbesserung des persönlichen Assistenten Cortana (Vergleichbar mit Siri und Google Now) werden Kalender- und Kontaktdaten, sowie die Sprach- und Eingabeverlauf verwendet. Mittels der Namen der Kontakte wird z.B. ein personalisiertes Wörterbuch erstellt, das u.a. für die Rechtschreibvorschläge und zur Auto-Vervollständigung genutzt wird.

Über „Kennenlernen beenden“ wird dies deaktiviert, durch das Beenden werden aber auch Cortana und die Diktierfunktion von Windows 10 deaktiviert. Bereits gesammelte Daten werden nach dem Beenden auf dem lokalen IT-System gelöscht; vermutlich ausgenommen sind Daten, die zur Verarbeitung an die Cloud gesendet wurden.

2.6 Weitere Datenschutzeinstellungen

Unter den weiteren Einstellungen können die Nutzungsrechte für verschiedene Ressourcen des Betriebssystems, z.B. Kamera, Mikrofon, Kontakte, etc. eingestellt werden. Dabei gibt es immer die Möglichkeit, die Funktionen generell zu deaktivieren oder nur für bestimmte Apps einzuschränken.

2.7 Kontensynchronisation

Windows 10 bietet die Möglichkeit das lokale Benutzerkonto mit einem Windows-Live-Konto zu verbinden und Konfigurationsdaten von Windows in der Cloud abzulegen. Beim Einloggen an einem anderen Rechner werden dann diese Einstellungsdaten aus der Cloud importiert. Standardmäßig werden in der Cloud ua. die Konfiguration des Webbrowsers und Kennwörter abgelegt. Welche Daten in der Cloud abgelegt werden dürfen kann unter „Einstellungen>>Datenschutz“ eingestellt werden.

Hinweis: Beim Einsatz einer Bitlocker-Verschlüsselung wird der Bitlocker-Key automatisch mit der Cloud-synchronisiert, um ein Wiederherstellungsverfahren zu ermöglichen. Es sollte daher geprüft werden ob die Schlüsselablage in der Cloud akzeptabel ist. In der Weboberfläche zur Windows Live-ID kann der hochgeladene Schlüssel nachträglich gelöscht werden.

2.8 Microsoft Edge

Im Edge-Browser gibt es die „Seitenvorhersage-Option“ mit dem die Liste der aufgerufenen Webseiten an Microsoft übertragen wird und auf dieser Basis, wahrscheinliche zukünftige Seite bereits im Vorfeld vom Browser geladen, damit die Ladezeit kürzer wird.

Außerdem sind übliche Browser-Einstellungen, z.B. für Cookies zu beachten.

2.9 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 könnten. Windows fragt außerdem nach Feedback zu den angezeigten Bildern, um diese gemäß dem eigenen Interesse zu personalisieren. Die Spotlight-Funktion kann unter Personalisieren>>Login-Bildschirm deaktiviert werden, in dem der Hintergrund Bild oder Slideshow ausgewählt ist und die Option „Get fun facts, tips und Ticks“ deaktiviert wird.

2.10 WLAN-Optimierung

Standardmäßig ist die WLAN-Optimierung aktiviert. Hierbei werden WLAN-Namen und dazugehörige Zugangsdaten, als Hash, mit den Kontakten geteilt, um den einfachen Zugang zu bekannten WLAN-Netzwerken zu ermöglichen.

2.11 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.

3. Rechtliche Vorgaben

Nach § 2a der Anordnung über den kirchlichen Datenschutz (KDO) und der ab 2018 geltenden Datenschutz-Grundverordnung sind EDV-Verfahren so zu gestalten, dass bei der Nutzung so wenig personenbezogene Daten wie möglich verarbeitet werden. Die Datenschutz-Grundverordnung wird zudem ausdrücklich den Grundsatz des Datenschutzes by default (per Voreinstellung) kodifizieren. Es sind daher zumindest alle technisch möglichen Maßnahmen zu ergreifen, um einen sparsamen Datenaustausch mit Microsoft zu gewährleisten. Soweit Beschäftigte das System nutzen, ergibt sich diese Pflicht auch aus § 10a KDO und den dienstvertraglichen Nebenpflichten im Arbeitsverhältnis nach § 611 Bürgerliches Gesetzbuch.

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 verfügbar sind, Datenflüsse an Microsoft nie vollständig unterbunden werden können und Zweifel an einer vollständigen Transparenz der Verarbeitung verbleiben. 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.

4. Empfehlungen für eine datensparsame Konfiguration von Windows 10

Die meisten datenschutzrelevanten Einstellungen können bereits ab den Windowsversionen Home oder Professional vorgenommen. Allerdings gibt es einige Optionen die nur ab der Enterprise-Version zur Verfügung stehen. Wenn die Möglichkeit besteht, sollte daher der Einsatz von Windows 10 Enterprise-Edition bevorzugt werden.

Innerhalb einer Domäne lassen sich viele der Einstellungen über Gruppenrichtlinien automatisch für IT-Systeme einstellen. Um Verwaltungsaufwand der Windows 10-Systeme möglichst gering zu halten sollten die entsprechenden Gruppenrichtlinien ebenfalls eingesetzt werden.

Zur Konfiguration der Gruppenrichtlinien werden die RSAT-Tools für Windows 10[5] benötigt, dabei ist zu beachten, dass diese nur auf einen IT-System mit Windows 10 installiert werden können.

[5] Herunterladbar unter: https://www.microsoft.com/de-DE/download/details.aspx?id=45520

In der folgenden Konfiguration wurden restriktive Empfehlungen gewählt und es werden alle relevanten Gruppenrichtlinien aufgelistet, alternative Konfigurationsschritte werden nur angegeben, wenn es keine Einstellungsmöglichkeit über Gruppenrichtlinien gibt:

- Werbungs-ID: Die Werbungs-ID kann mit der Gruppenrichtlinie „System\User Profiles\ Turn off the advertising ID“ deaktiviert werden und es wird empfohlen die Gruppenrichtlinie einzusetzen.

  Das Opt-Out unter https://choice.microsoft.com/de-de/opt-out# muss von jedem Anwender individual vorgenommen werden und die Anwender sollten daher in geeigneter Form darüber Informiert werden.
- Informationen zum Schreibverhalten: Die Übermittlung von getippten und handgeschriebenen Wörtern kann nicht direkt deaktiviert werden. Diese Option wird aber automatisch deaktiviert, wenn der Telemetrieclient auf „Sicherheit“ oder „Basis“ eingestellt wird.
- Zugriff auf Sprachliste: Diese Einstellung lässt sich nicht direkt über Gruppenrichtlinien vornehmen, stattdessen muss der Registry-Eintrag „HttpAcceptLanguageOptOut“ unter „HKEY_CURRENT_USER\Control Panel\International\User Profile“ mit dem Wert „1“ angelegt werden und es wird empfohlen, den Registry-Eintrag anzulegen.
- Diagnosedaten: Die Telemetrie-Einstellungen können mit der Gruppenrichtlinie „Windows Components\Data Collection and Preview Builds\ Allow Telemetry“ angepasst werden. Als Wert kann für die Richtlinie folgendes eingestellt werden:
  - 0 für Sicherheit (nur Enterprise)
  - 1 für Einfach
  - 2 für Verbesserter
  - 3 für Vollständig

  Es wird empfohlen, beim Einsatz von Windows 10 Enterprise die Einstellung auf „Sicherheit“ zusetzen und ansonsten „Einfach“ auszuwählen.
- Feedback: Die Nachfrage nach Feedback kann mit der Gruppenrichtlinie „Windows Components\Data Collection and Preview Builds\ Do not show feedback notifications“ deaktiviert werden und es wird empfohlen die Gruppenrichtlinie einzusetzen.
- Datenweitergabe: Zur Deaktivierung der verschiedenen Datenweitergaben müssen mehre Gruppenrichtlinien konfiguriert werden. Die dazugehörigen Richtlinien können der beigelegten Excel-Liste entnommen werden.
- Position: Die komplette Deaktivierung des Positionsdienstes bzw. die Deaktivierung für Windows-Apps kann über Gruppenrichtlinien ausgeführt werden, die dazugehörigen Richtlinien können der beigelegten Excel-Liste entnommen werden.

  Es wird empfohlen, den Positionsdienst zu deaktivieren oder zumindest die Nutzungsrechte auf das notwendigste zu reduzieren.

  Klassische Windows-Apps (z.B. Installation über EXE oder MSI-Installer, Zugriff auf .NET) sind von diesen Einstellungen nicht betroffen, und können weiter auf die Position zugreifen.

  Hinweis: Diese Einstellungen gelten auch für Kamera, Mikrofon, Kontoinformationen, Kontakte, Kalender, Messaging, Funkempfang und weitere Geräte.
- Personalisierte Spracherkennung, Freihand und Eingabe: Die Auswertung von Kalender, Nachrichten usw. zur Verbesserung von Cortana können mit der Richtlinie „Control Panel\Regional and Language Options\Handwriting personalization\ Turn off automatic learning“ deaktiviert werden und es wird empfohlen, die Gruppenrichtlinie einzusetzen.

--- Kontensynchronisation: Die Kontosynchronisation erfolgt mit der hinterlegten Windows-Live-ID. Über Gruppenrichtlinien kann detailliert eingestellt werden, z.B. ob Browsereinstellungen, App-Einstellungen oder gespeicherte Passwörter in der Cloud abgelegt werden sollen. Eine Auflistung der entsprechenden Richtlinien für die Synchronisation kann der beigelegten Excel-Liste entnommen werden.

Es ist zu empfehlen, die lokalen Benutzerkonten nicht mit Windows-Live-IDs zu verbinden. Sollte die Verknüpfung mit der Windows-Live-ID gewünscht sein, sollten hierzu dienstliche Windows-Live-IDs von den Mitarbeitern erstellt werden. Es ist empfehlenswert, die Cloud-Synchronisation generell zu deaktivieren oder zu mindestens die Synchronisation von vertraulichen Daten zu verhindern und die weiteren Synchronisation-Einstellungen durch die Anwender aktivieren zu lassen. Die dazugehörigen Richtlinien können der beigelegten Excel-Liste entnommen werden.

--- Microsoft Edge: Beim Einsatz von Microsoft Edge als Browser können viele Datenschutzeinstellungen zentral über Gruppenrichtlinien vorgenommen werden. Eine Auflistung der Richtlinien kann der beigelegten Excel-Liste entnommen werden.

Es wird empfohlen, beim Einsatz von Microsoft Edge den Einsatz von „Do Not Track Cookies“ und die erlaubten Cookies zentral einzustellen. Leider kann der Versand von „Do Not Track“-Cookies und die Seitenvorhersage nicht zentral verwaltet werden. Die Mitarbeiter sollten daher zu diesen Einstellungsmöglichkeiten beim Einsatz von Microsoft Edge (Einstellungen >> Erweiterte Einstellungen >> Seitenvorhersage) geschult werden.

--- Windows Spotlight: Die Einstellungen zum Lock-Screen und zu Windows Spotlight können über Gruppenrichtlinien vorgenommen werden. Eine Auflistung der Richtlinien kann der beigelegten Excel-Liste entnommen werden.

Es wird empfohlen, dass zumindest die Werbung im Lock-Screen deaktiviert wird.

--- WLAN-Optimierung: Die WLAN Optimierung kann mit der Richtlinie „Network\WLAN Service\WLAN Settings\ Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services” aktiviert werden. Es wird empfohlen, diese Richtlinie nicht zu aktivieren.

--- Windows-Suche: Das Senden von Informationen und Suchanfragen an Onlinesuchmaschinen kann über mehrere Richtlinien konfiguriert werden und es ist zu empfehlen dies zu unterbinden. Eine Auflistung der Richtlinien kann der beigelegten Excel-Liste entnommen werden.

Auch das indizieren von verschlüsselten Dateien sollte nicht erlaubt werden, denn über die Indizes werden Metadaten zu den verschlüsselten Dateien angelegt, über die vertrauliche Informationen veröffentlicht werden können. Standardmäßig ist das indizieren deaktiviert und diese Einstellung sollte beibehalten werden.

5. 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 Andorid 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. Eine Auflistung der Richtlinien für die Konfiguration des Windows Stores kann der beigelegten Excel-Liste entnommen werden.

--- One Drive deaktivieren: In Windows 10 ist OneDrive 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 „Windows Components\OneDrive\ Prevent the usage of OneDrive for file storage“ verhindert werden, und es ist empfohlen diese Richtlinie zu aktivieren.

A Literatur

[Bott16] Ed Bott, „Introducing Windows 10 for IT Professionals - Technical Overview“. Microsoft, 2016, Url: http://blogs.msdn.com/b/microsoft_press/archive/2016/02/08/free-ebook-introducing-windows-10-for-it-professionals-technical-overview.aspx, Quellen-Angaben, 09.02 2016.

[MS15SSP] http://windows.microsoft.com/de-de/windows-10/services-setting-preferences

[MS15Telemetrie] https://technet.microsoft.com/de-de/library/mt577208(v=vs.85).aspx

[MS15LS] http://windows.microsoft.com/de-de/windows-10/location-service-privacy

Hinweis: Dieses Dokument wurde im Auftrag des Diözesandatenschutzbeauftragten der Nordbistümer der katholischen Kirche erstellt unter Mitwirkung der datenschutz nord GmbH.