Technische Empfehlung

Technische Hinweise für Windows 10 im Rahmen der Verarbeitungstätigkeit

Windows 10 Webbrowser

Stand 09/2021

Konferenz der Diözesan-datenschutzbeauftragten
der Katholischen Kirche Deutschlands

Technische Empfehlung

Technische Hinweise für Windows 10 im Rahmen der Verarbeitungstätigkeit Windows 10 Webbrowser

Herausgeber:
Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands

Geschäftsstelle:
Katholisches Datenschutzzentrum (KdöR)
Brackeler Hellweg 144
44309 Dortmund
Tel. 0231 / 13 89 85 – 0
Fax 0231 / 13 89 85 – 22
E-Mail: ddsb@kdsz.de
www.katholisches-datenschutzzentrum.de

Autor:
Arbeitskreis Technik der Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschlands

Diese „Technischen Hinweise für Windows 10 im Rahmen der Verarbeitungstätigkeit“ sollen Hilfestellungen für eine möglichst datenschutzfreundliche Nutzung von Windows 10 geben und beschäftigen sich mit den bestehenden Problemen der Telemetriedatenübermittlung an Microsoft sowie weiteren notwendigen technischen Einstellungen zu einem datensparsamen Betrieb der Software. Die generelle Problematik, ob Windows 10 auf Grund der Übermittlung personenbezogener Daten an ein Drittland überhaupt datenschutzkonform einsetzbar ist, ist nicht Inhalt dieser Arbeitshilfe und ist daher getrennt zu bewerten.

Revision 2.0 /24.09.2021

Inhalt

Technische Hinweise für Windows 10 im Rahmen der Verarbeitungstätigkeit

Grundlage für diese Arbeitshilfen bildet das allgemeine **Manteldokument „Datensparsamer Betrieb von Windows 10“** in der Version 2.0.

Eine Prüfung der Rechtmäßigkeit der Verarbeitung ist nicht Gegenstand dieser Arbeitshilfe.

Themenbereich / Funktion	Dokument-Nr.
Windows 10 Webbrowser	W10.TH105a

1. Einleitung/Motivation

Microsoft liefert zusammen mit Windows 10 zwei Webbrowser: Microsoft Internet Explorer und Microsoft Edge. Letzterer wird den älteren Internet Explorer ablösen, dessen Support am 17. August 2021 eingestellt wird. Grundsätzlich steht es Microsoft-Kunden frei, statt oder neben den mitgelieferten Webbrowsern andere Webbrowser zu verwenden. Aufgrund des endenden Supports wird empfohlen, Microsoft Internet Explorer nicht mehr zu verwenden. Daher sind die vorliegenden Hinweise auf Microsoft Edge fokussiert.

Einige Funktionen von Microsoft Edge (wie auch von anderen Webbrowsern) verarbeiten Daten, die in vielen Fällen auf die Benutzerin oder den Benutzer beziehbar sind. Beispielsweise erfordern die Funktionen zum maschinellen Vorlesen oder Übersetzen von Texten eine Übermittlung personenbezogener Daten an die Dienste von Microsoft. Wird der Webbrowser mit einem Microsoft-Konto verknüpft, lassen sich Daten über mehrere Geräte hinweg synchronisieren. Allerdings erfordert dies ebenfalls eine Verarbeitung personenbezogener Daten durch Microsoft-Dienste. Werden diese Funktionen nicht benötigt, können sie zentral deaktiviert werden um, gemäß dem Prinzip der Datensparsamkeit, unnötige Verarbeitungen zu verhindern.

Diese Arbeitshilfe soll Einstellungen aufzeigen, die für gewöhnlich nicht notwendige Verarbeitungen vermeiden. In Einzelfällen kann es jedoch notwendig sein, von dieser Empfehlung abzuweichen, um benötigte Funktionen zu aktivieren.

Im Sinne eines datenschutzfreundlichen Betriebs von Systemen sollten, soweit wie möglich, Einstellungen vorgenommen werden, die einen datensparsamen Betrieb gewährleisten und Datenübermittlungen, die nicht erforderlich sind, unterbinden.

2. Möglichkeiten zur Konfiguration

Folgende Möglichkeiten zur Konfiguration stehen zur Verfügung.

Windows Einstellungen	Gruppenrichtlinie (GPO)	Windows Registry (REGKEY)
Microsoft Edge	☑	☑

Die hier beschriebenen Einstellungen beziehen sich auf die folgenden Versionen. Einstellungen in neueren Versionen können von dieser Beschreibung abweichen.

Microsoft Windows	Windows 10 Pro und höher
Microsoft Edge	Stable 92 (Build 92.0.902.62)
Vorlagen für Gruppenrichtlinien	MSEdge.admx

Microsoft Edge und die Vorlagendatei für die hier beschriebenen Gruppenrichtlinien sind bei Microsoft verfügbar [1]. Ebenso wird eine Dokumentation der für Microsoft Edge verfügbaren Gruppenrichtlinien angeboten [2].

Die im Folgenden beschriebenen Gruppenrichtlinien sind in der oben genannten Vorlagendatei enthalten und befinden sich nach einem Import sowohl in der Benutzer- als auch in der Computerkonfiguration unter folgendem Pfad:

```
Administrative Templates/Microsoft Edge/
```

Sie sind zu unterscheiden von den Gruppenrichtlinien unter:

```
Administrative Templates/Windows Components/Microsoft Edge/
```

Hinweise zum Import der Vorlagendatei werden von Microsoft bereitgestellt [3].

Die aktuellen Werte der Edge-spezifischen Gruppenrichtlinien können in Microsoft Edge unter `edge://policy` angezeigt werden.

Je nach Sprachversion und Stand der Vorlagendatei werden Objekte ggf. anders benannt.

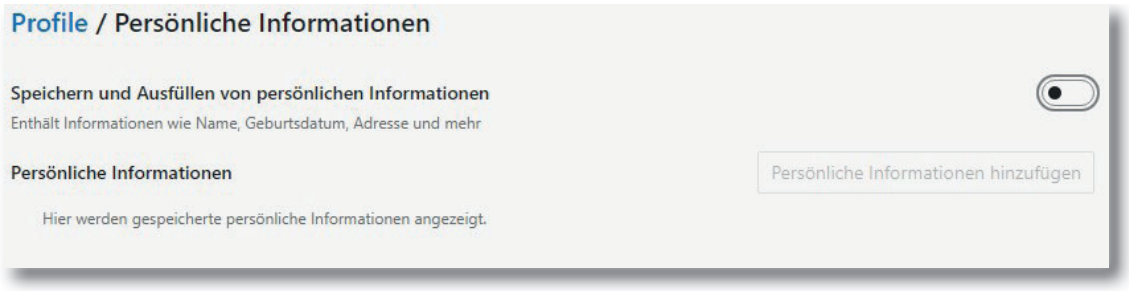
2.1 Microsoft-Konto

Es wird empfohlen, alle Funktionen zu deaktivieren, die ein Microsoft-Konto voraussetzen. Hierzu zählen das Einrichten eines Smartphones oder anderer Geräte, die Synchronisierung mit einem Microsoft-Konto und die Funktion „Family Safety“.

Gruppenrichtlinie	Status
BrowserSignin	Disable (0) = Disable browser sign-in
FamilySafetySettingsEnabled	Deaktiviert
SyncDisabled	Deaktiviert

2.2 Profile

Es wird empfohlen, nur notwendige Daten in Profilen des Webbrowsers zu speichern. Falls es nicht erforderlich ist, Profildaten zwischen Browsersitzungen zu speichern, wird empfohlen, kurzlebige Profile zu verwenden. Profildaten können in Edge in „Einstellungen > Profile > Persönliche Informationen“ verwaltet werden.



2.3 Suchmaschinen verwalten

Es wird empfohlen, nur datenschutzkonforme Suchmaschinen einzustellen und alle anderen Suchmaschineneinträge zu löschen. Die zu verwendenden Werte der folgenden Gruppenrichtlinien hängen vom gewünschten Verhalten ab (siehe Dokumentation [2]).

Gruppenrichtlinie
ManagedSearchEngines
Default search provider/DefaultSearchProviderEnabled
Default search provider/DefaultSearchProviderName
Default search provider/DefaultSearchProviderSearchURL

2.4 Beim Start

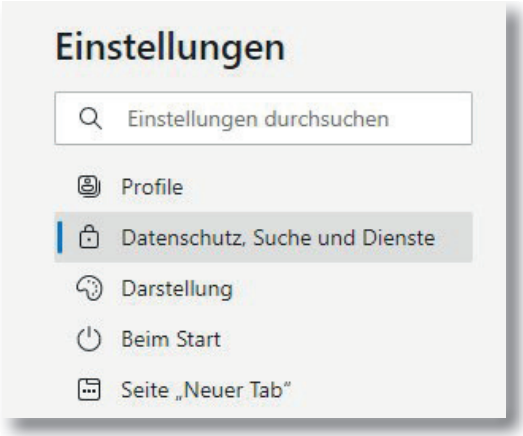
Um unnötige Datenübermittlungen beim Start des Webbrowsers oder beim Öffnen eines neuen Tabs zu vermeiden, wird empfohlen, eine leere Seite anzeigen zu lassen. **Für neue Tabs kann diese Einstellung nicht in der graphischen Benutzeroberfläche von Edge vorgenommen werden.**

Gruppenrichtlinie	Status
Startup, home page and new tab page/RestoreOnStartup	RestoreOnStartupIsNewTabPage (5) = neue Registerkarte öffnen
Startup, home page and new tab page/NewTabPageLocation	about://blank
Startup, home page and new tab page/HomepageLocation	about://blank

Wenn die oben genannten Einstellungen zentral gesteuert werden, kann die Abfrage dieser Einstellungen beim ersten Starten des Webbrowsers mit der folgenden Gruppenrichtlinie unterbunden werden.

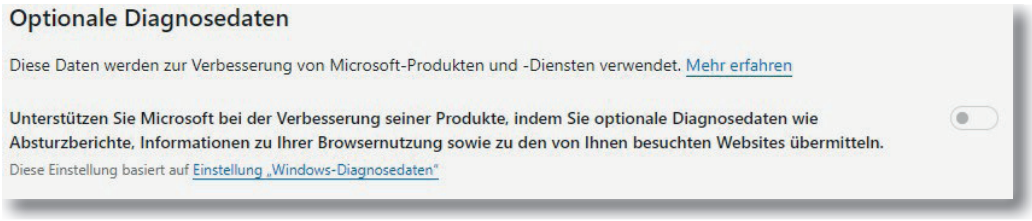
Gruppenrichtlinie	Status
HideFirstRunExperience	Aktiviert

2.5 Menü Einstellungen: Datenschutz, Suche und Dienste

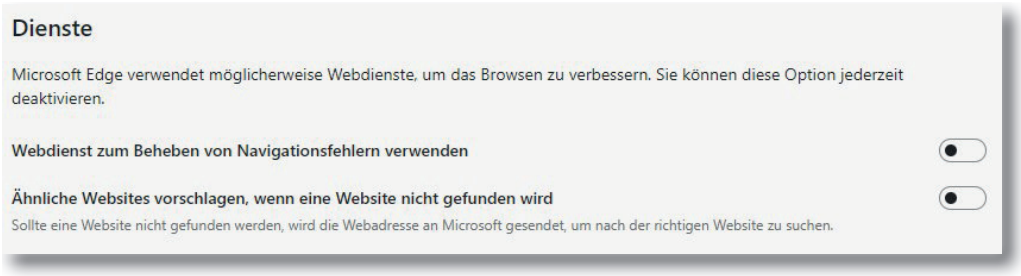


Es wird empfohlen, alle folgenden Funktionen zu deaktivieren, da sie vermeidbare Datenübermittlungen an Microsoft voraussetzen.

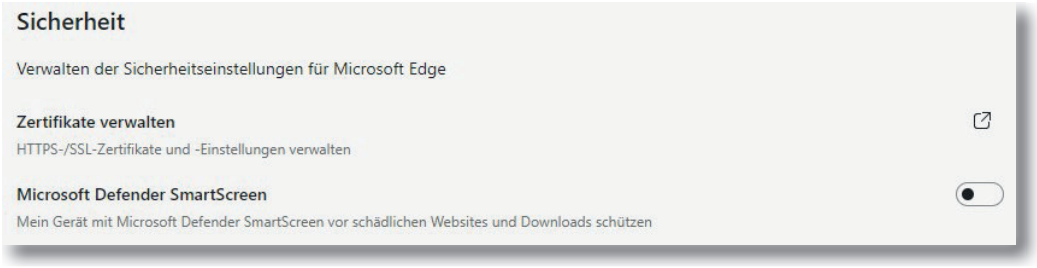
1 *Optionale Diagnosedaten*



2, 3 *Dienste:*
Webdienst zum Beheben von Navigationsfehlern verwenden
Ähnliche Websites vorschlagen, wenn eine Website nicht gefunden wird



4 *Microsoft Defender SmartScreen*



Die Deaktivierung der Funktion 1 bewirkt keine Beeinträchtigung für einzelne Benutzer und Benutzerinnen. Die Funktionen 2 und 3 sollen die Navigation zu Webseiten erleichtern. Funktion 4 soll vor dem Besuch bekannter Webseiten mit Schadcode oder Phishing warnen. Dafür werden alle aufgerufenen Webseiten an Microsoft übermittelt.

Dies zu deaktivieren stellt also einen Kompromiss aus Datensparsamkeit und Sicherheit vor bekannten Webseiten mit Schadcode oder Phishing dar.

Die Funktion 1 wird unter Windows 10 zentral, abhängig von der Version über die Gruppenrichtlinie „Telemetrie zulassen“ oder „Diagnosedaten zulassen“, gesteuert. Es wird empfohlen, diese Einstellung auf „Sicherheit“ (bzw. die niedrigste verfügbare Stufe) zu setzen und die Sammlung von Browserdaten für Desktop Analytics zu deaktivieren (siehe Gruppenrichtlinien unter Administrative Vorlagen/Windows-Komponenten/Datensammlung und Vorabversionen/). Die Einstellung der Edge-spezifischen Gruppenrichtlinie „DiagnosticData“ entfällt in diesem Fall (wird nur bei anderen Betriebssystemen als Windows 10 verwendet). Die Funktionen 2 bis 4 lassen sich über folgende Gruppenrichtlinien festlegen.

Gruppenrichtlinie	Status
ResolveNavigationErrorsUseWebService	Deaktiviert
AlternateErrorPagesEnabled	Deaktiviert
SmartScreen settings/SmartScreenEnabled	Deaktiviert

2.6 Sprachen

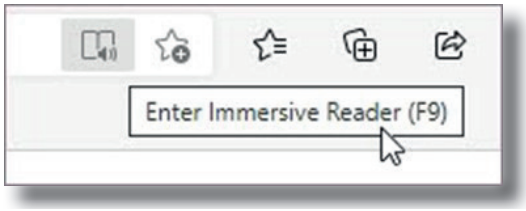
Um eine unnötige Übermittlung des vorzulesenden Textes an Microsoft zu verhindern, wird empfohlen die Funktion „Online Text zu Sprache“ zu deaktivieren.

Gruppenrichtlinie	Status
ConfigureOnlineTextToSpeech	Deaktiviert

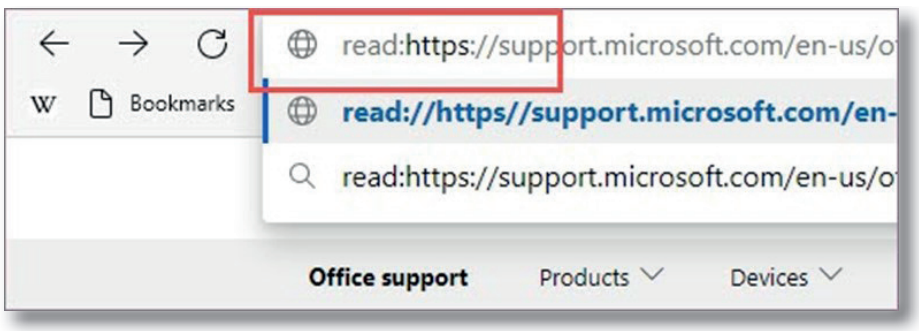
Darüber hinaus wird empfohlen, auch die automatisierte Übersetzung von Texten zu deaktivieren.

Gruppenrichtlinie	Status
TranslateEnabled	Deaktiviert

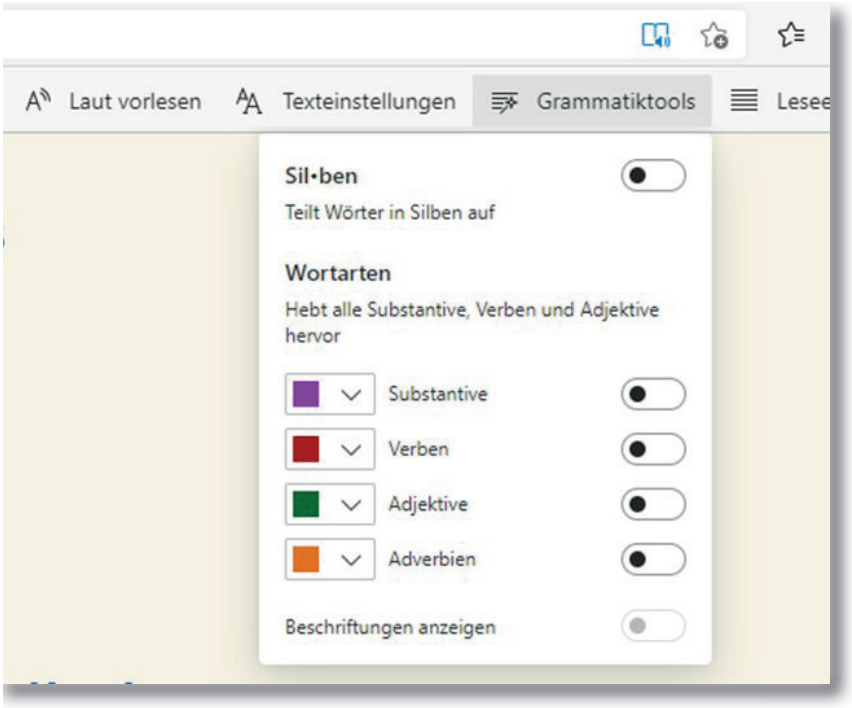
Darüber hinaus wird empfohlen, die „Grammartools“ nicht zu verwenden, um eine unnötige Übermittlung zu vermeiden. Die „Grammartools“ stehen im „Immersive Reader“ (bzw. im „Reading Mode“) zur Verfügung.



Nach dem Aufruf einer Webseite im „Reading Mode“, ...



... wird die Option „Grammatiktools“ angezeigt, welche das An- und Abschalten von Grammatikhilfen erlaubt:



2.7 Hintergrund-Apps

Damit die aktuellen Browserdaten beim Schließen des Browserfensters tatsächlich gelöscht werden, wird empfohlen, die Ausführung des Webbrowsers im Hintergrund zu deaktivieren (Funktion „Ausführung von Hintergrund-Apps zulassen, nachdem Microsoft Edge geschlossen wurde“).

Gruppenrichtlinie	Status
BackgroundModeEnabled	Deaktiviert

2.8 „An Taskleiste anheften“

Es wird empfohlen zu beachten, dass für die Funktion „an Taskleiste anheften“ eine Verbindung zur gewählten Webseite aufgebaut wird und Daten übermittelt werden, auch wenn die neue Schaltfläche der Taskleiste nicht benutzt wird. Diese Funktion kann deaktiviert werden.

Gruppenrichtlinie	Status
PinningWizardAllowed	Deaktiviert

2.9 Benutzerfeedback und Empfehlungen

Es wird empfohlen, die Funktionen Spotlight-Experiences und Benutzer-Feedback zu deaktivieren, da sie in der Regel nicht erforderlich sind.

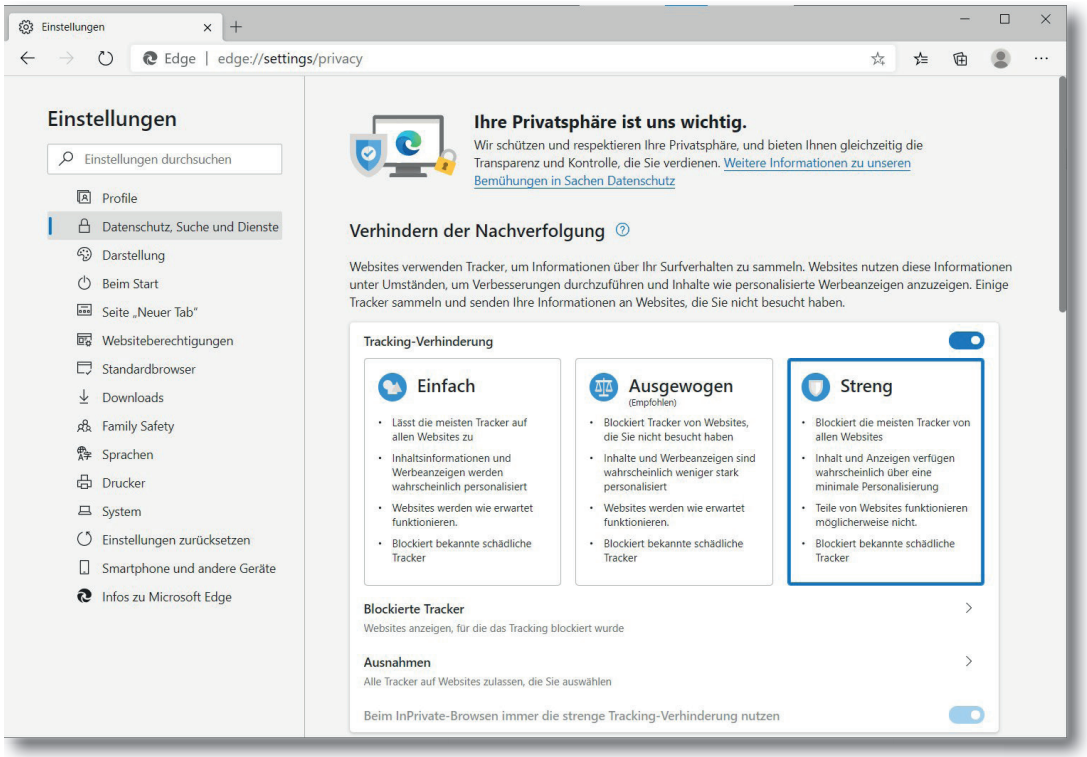
Gruppenrichtlinie	Status
Content settings/SpotlightExperiencesAndRecommendationsEnabled	Deaktiviert
UserFeedbackAllowed	Deaktiviert

2.10 Weitere empfohlene Einstellungen

Es wird empfohlen,

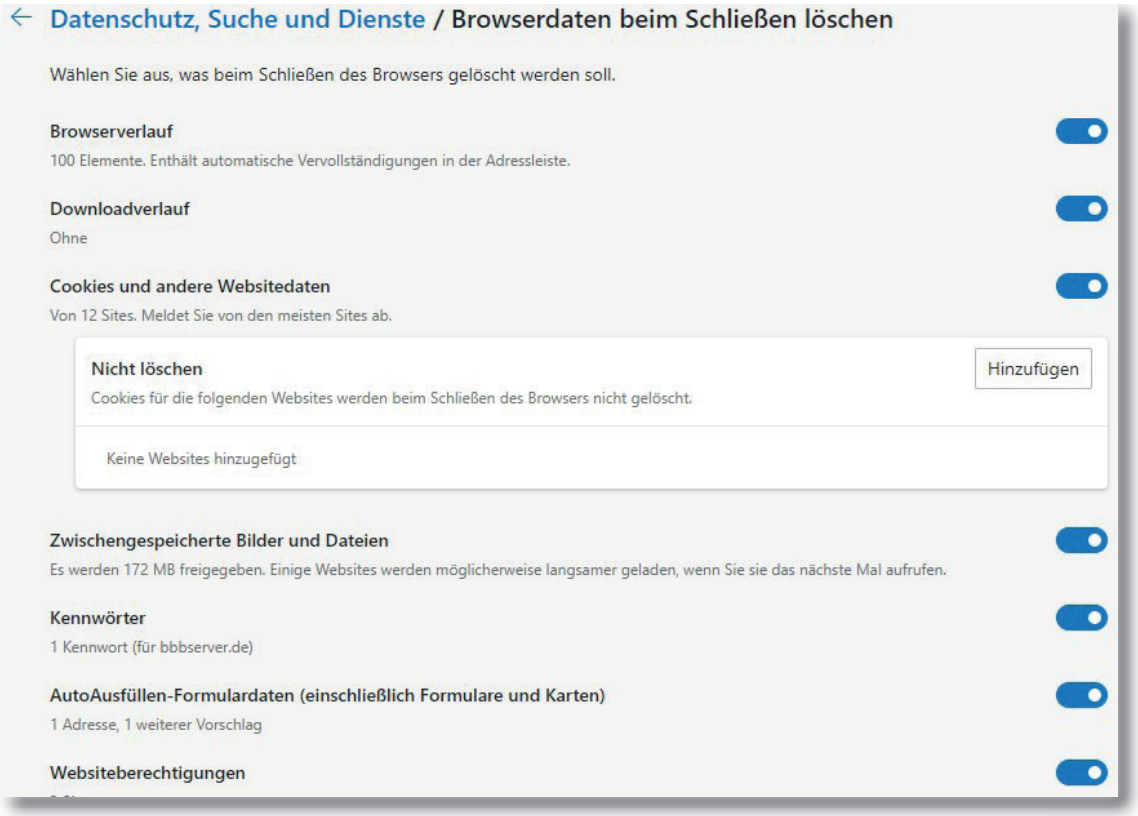
- einen Schutz gegen Trackingverfahren zu aktivieren und hier nur von der höchsten Stufe „streng“ abzuweichen, wenn andernfalls eine benötigte Funktion behindert wird.

Gruppenrichtlinie	Status
TrackingPrevention	TrackingPreventionStrict (3)



- beim Schließen des Webbrowsers alle Browserdaten zu löschen.

Gruppenrichtlinie	Status
ClearBrowsingDataOnExit	Aktiviert

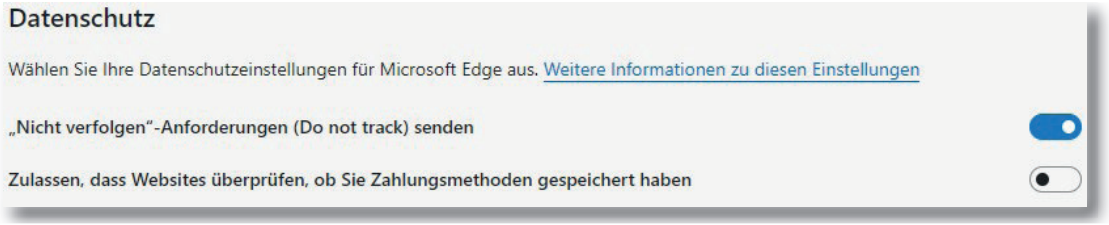


- das Senden von „Nicht verfolgen“-Anforderungen (DoNotTrack) zu aktivieren.

Gruppenrichtlinie	Status
ConfigureDoNotTrack	Aktiviert

- die Funktion zur Abfrage von Zahlungsmethoden zu deaktivieren.

Gruppenrichtlinie	Status
PaymentMethodQueryEnabled	Deaktiviert

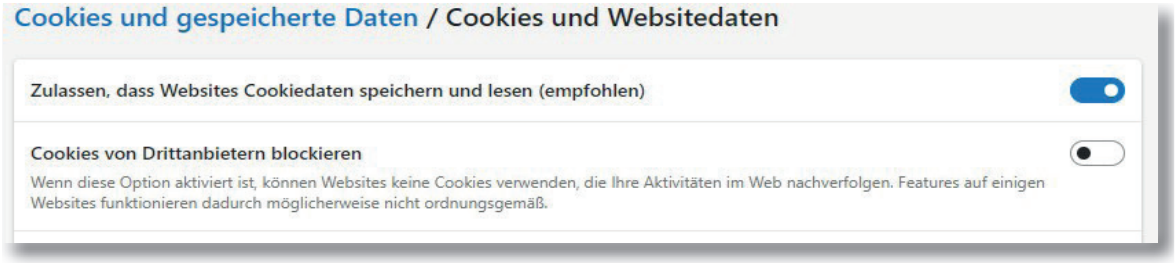


- die Funktion für Vorschläge bei der Eingabe von Zeichen in die Adressleiste zu deaktivieren, da hierfür eine Datenübermittlung an den Anbieter der Standardsuchmaschine verwendet wird.

Gruppenrichtlinie	Status
SearchSuggestEnabled	Deaktiviert
AddressBarMicrosoftSearchInBingProviderEnabled	Deaktiviert

- Cookies von Drittanbietern zu blockieren, da sie in der Regel keine notwendige Funktion haben, jedoch oft personenbezogene Daten enthalten.

Gruppenrichtlinie	Status
BlockThirdPartyCookies	Aktiviert



2.11 Zusätzliche Hinweise

Es sollte weiterhin beachtet werden,

- dass im für Downloads verwendeten Verzeichnis möglicherweise personenbezogene Daten gespeichert werden und diese nicht durch den Webbrowser gelöscht werden.
- dass Microsoft Edge möglicherweise an konfigurierte Drucker personenbezogene Daten übermittelt.
- dass die Funktion zum automatischen Vervollständigen im Webbrowser personenbezogene Daten verarbeiten kann.
- dass zu prüfen ist, in welchem Umfang der Webbrowser Hinweisen zu *prefetch* und *preload* folgen soll, da hierüber eine Rückverfolgung der aufgerufenen Webseiten möglich ist, ohne dass ein Benutzer die entsprechenden Verweise auf Webseiten aufruft.

3. Abgrenzung/wichtiger Hinweis

Windows 10 ist nach einer Standardinstallation nicht datensparsam eingerichtet. Darüber hinaus ist zu beachten, dass viele Einstellungen sich nur auf den aktuell angemeldeten Benutzer (Benutzerprofil) beziehen. Sobald sich ein neuer Benutzer an ein Windows 10 System anmeldet und erstmalig für diesen Benutzer ein Benutzerprofil eingerichtet wird, werden Standardvorgaben eingerichtet, die hinsichtlich ihrer Datenschutzfreundlichkeit zu überprüfen und ggfs. zu ändern sind. Durch Gruppenrichtlinien kann der Administrator viele der obengenannten Einstellungen verbindlich vorgeben.

Windows 10 selbst stellt viele Einstellmöglichkeiten zur Verfügung, die einen datensparsamen Betrieb erlauben. Etliche Einstellungen können direkt mit den entsprechenden Schaltern in der Windows-Konfiguration vorgenommen werden. Einige Einstellungen für einen datensparsamen Betrieb können aber nur mit Hilfe der System Registry oder auf Netzwerkebene reglementiert werden. Für eine zentrale Konfiguration der Windows 10 Clients in einer Organisation ist eine Konfiguration per Gruppenrichtlinie und Netzwerk nach einem betrieblichen Betriebskonzept/IT-Sicherheitskonzept die empfohlene Variante.

Alle Einstellungen und Systemkonfigurationen sollten von einer fachkundigen Person durchgeführt und unbedingt vorher auf einem System getestet werden. Änderungen an der Konfiguration, speziell durch Anpassung oder Veränderung von Einträgen in der Windows Registry, können unvorhersehbare Betriebsprobleme verursachen bis hin zu Systemabstürzen und einer Nichtverfügbarkeit von Funktionen und Diensten. Vor dem Bearbeiten der Registry sollte ein Systemwiederherstellungspunkt angelegt und entsprechende Änderungen dokumentiert werden. Dieses Dokument bietet keine Gewähr auf Vollständigkeit der beschriebenen Konfigurationsmöglichkeiten.

Ferner ist zu berücksichtigen, dass sich durch die monatlich von Microsoft herausgegebenen Updates Änderungen an den vorgenommenen Einstellungen ergeben können.

Auch mit der hier empfohlenen Konfiguration ist nicht garantiert, dass ein datensparsamer Betrieb von Microsoft Edge möglich ist. So liegen beispielsweise viele Verarbeitungen personenbezogener Daten außerhalb des Einflussbereichs eines Webbrowsers, wie etwa die Verarbeitungen durch den Server einer Webanwendung.

Darüber hinaus können nicht alle Verarbeitungen durch Microsoft Edge über Einstellungen beeinflusst werden; solche Verarbeitungen werden in diesem Dokument jedoch nicht behandelt. Insbesondere werden nicht alle über aufgerufene Webseiten hinausgehende Netzwerkverbindungen verhindert. Gänzlich unbetrachtet bleibt hier auch die Problematik des Fingerprintings von Webbrowsern, also der Identifikation einzelner Webbrowserinstallationen aufgrund übermittelter oder im Webbrowser verfügbarer Daten über das System. Fingerprinting von Webbrowsern erlaubt das Rückverfolgen von Benutzern und Benutzerinnen bei einem wiederholten Aufruf einer Webressource und eignet sich daher zum Erstellen von personenbezogenen Profilen. Ein Verhindern oder Erschweren des Fingerprintings ist jedoch durch die Konfiguration von Microsoft Edge nicht verlässlich möglich.

4. Referenzen[1]

[1] https://www.microsoft.com/de-de/edge/business/download
[2] https://docs.microsoft.com/de-de/deployedge/microsoft-edge-policies
[3] https://docs.microsoft.com/en-us/deployedge/configure-microsorft-edge

5. Anlage für den bDSB/IT-Sicherheitsbeauftragten

Risikoeinschätzung und **Dokumentation der Nachweispflichten** laut § 7 Abs. 2 KDG sowie Art. 5 Abs. 2 DS-GVO.

Prüfpunkt	Einschätzung	Kommentar
Könnten personenbezogene Daten übermittelt werden/betroffen sein?		
Könnten sicherheitsrelevante Daten übermittelt werden/betroffen sein?		
Übermittlung ist zulässig!		
Übermittlung wird akzeptiert!		
Übermittlung soll eingeschränkt werden (datensparsam)!		

Interne Bemerkungen

Ferner wurden noch folgende Maßnahmen ergriffen:

1 Referenz-URL bzw. Hyperlinks gültig und abgerufen am 03.08.2021

In dieser Reihe sind erschienen:

W10.TH100a	Manteldokument: Datensparsamer Betrieb von Windows 10
W10.TH101a	Windows 10 Suchfunktion
W10.TH102a	Windows 10 Installation
W10.TH103a	Windows 10 Entfernung automatisch installierter Apps bei Neuinstallation/Funktionsupdates
W10.TH104a	Online Spracherkennung
W10.TH105a	Windows 10 Webbrowser

Diese Schriftenreihe wird gemeinsam herausgegeben von

Katholische Datenschutzaufsicht Nord

Katholische Datenschutzaufsicht Nord für das Erzbistum Hamburg, die Bistümer Hildesheim und Osnabrück und das Bischöflich Münstersche Offizialat in Vechta i.O.

Katholisches Datenschutzzentrum

Katholisches Datenschutzzentrum (KdöR) als Datenschutzaufsicht der nordrhein-westfälischen (Erz-)Diözesen und für den Verband der Diözesen Deutschlands

Kirchliche Datenschutzaufsicht für die ostdeutschen Bistümer und den Katholischen Militärbischof

Katholisches Datenschutzzentrum Frankfurt/Main (KdöR) als Datenschutzaufsicht für die (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier

Gemeinsame Datenschutzaufsicht der bayrischen (Erz-) Diözesen