Datenschutzrechtliche Probleme bei der Einführung neuer Betriebssysteme – Eine Untersuchung am Beispiel von Windows 10

Inhalt

Die folgenden Ausführungen entsprechen unter Umständen nicht der ab dem 25. Mai 2018 geltenden Rechtslage. Dem hier zur Verfügung gestellten Text liegt die Rechtslage vor Geltung der Verordnung (EU) 2016/679, bekannt unter ihrem Kurztitel EU-Datenschutz-Grundverordnung (DS-GVO), zugrunde. Die Verordnung gilt ab dem 25. Mai 2018 verbindlich in allen Mitgliedsstaaten der Europäischen Union und verdrängt grundsätzlich alle nationalen Regelungen zum Datenschutzrecht.

Für den Regelungsbereich der elektronischen Kommunikation soll die DS-GVO durch die E-Privacy-Verordnung ergänzt und präzisiert werden. Diese befindet sich jedoch noch in der Beratungsphase und wird nicht rechtzeitig zum 25. Mai 2018 in Kraft treten. Es ist nicht auszuschließen, dass die E-Privacy-Verordnung für die hier dargestellten Sachverhalte wiederum neue Regelungen bereithält.

Die Forschungsstelle Recht im DFN beobachtet diese Entwicklungen und passt die datenschutzrechtlichen Ausführungen entsprechend an. Bis dahin bitten wir um Ihre Geduld.

A. Ergebnisübersicht

Der Einsatz eines Betriebssystems bei datenverarbeitenden Stellen muss immer auch aus datenschutzrechtlicher Perspektive zulässig sein. Daher ist bei der Einführung eines neuen Betriebssystems bei diesen Stellen vorab zu prüfen, ob dieses den datenschutzrechtlichen Anforderungen gerecht wird. Aktuell wird dies vor allem bei dem Einsatz von Windows 10 relevant, der aus datenschutzrechtlicher Sicht nicht unbedenklich ist. Einzelne Anwendungen, die Microsoft den Zugriff auf Daten der Nutzer und Dritter ermöglichen, werfen zahlreiche Probleme auf. Aus diesem Grund muss es das Ziel der datenverarbeitenden Hochschulen oder Forschungseinrichtungen sein, den Zugriff von Microsoft auf personenbezogene Daten zu unterbinden. In dieser Hinsicht stellt die Konfiguration durch den Administrator im Rahmen von Gruppenrichtlinien ein wirksames Mittel dar, um problematische Funktionen von vorneherein zu deaktivieren. Keinesfalls sollten die Standardeinstellungen von Windows 10 bezüglich der Datenverwendung übernommen werden. Auch sollte das Vorgehen mit dem zuständigen Datenschutzbeauftragten abgestimmt werden. Diese Überlegungen lassen sich auf andere Betriebssysteme übertragen.

Im Hinblick auf Windows 10 wird für die technische Konfiguration der Dienste und Funktionen auf die Quellen in der Literaturliste verwiesen (s. unter D.).

B. Einleitung

Bei der Einführung neuer Betriebssysteme müssen sich Hochschulen und Forschungseinrichtungen die Frage stellen, inwiefern der Einsatz des jeweiligen Betriebssystems mit den geltenden Datenschutzvorschriften vereinbar ist. Insbesondere der Einsatz von Windows 10 wirft derzeit zahlreiche Fragen im Hinblick auf die Vereinbarkeit mit dem Datenschutzrecht auf. In der Öffentlichkeit wird mit Sorge diskutiert, ob Microsoft sich möglicherweise ungehinderten Zugriff auf die Daten der Nutzer verschaffe.[1] Microsoft verfolgt das Ziel, dem Nutzer möglichst viele Dienstleistungen bereitzustellen, z.B. Cloud-Speicher und Apps. Der bloße Verkauf von Betriebssystemen steht nicht mehr im Mittelpunkt. Doch je mehr Funktionen dem Nutzer zur Verfügung gestellt werden, desto mehr potentielle Zugriffsmöglichkeiten auf personenbezogene Daten schafft sich Microsoft. Die Verbraucherzentrale NRW erhob jüngst sogar wegen der für die Nutzung von Windows 10 erforderlichen Datenschutzerklärung Klage gegen Microsoft, da diese ihrer Ansicht nach zu lang, unübersichtlich und unbestimmt sei.[2]

Die besondere Problematik bei der Einführung eines neuen Betriebssystems an Hochschulen oder Forschungseinrichtungen besteht zunächst darin, dass der Nutzer meist nicht selbst entscheiden kann, ob er das Betriebssystem einsetzen möchte oder nicht. Vielmehr veranlassen die Hochschulen und Forschungseinrichtungen ihre Mitarbeiter und sonstigen Nutzer (z.B. Studierende an Rechnern im Computerpool einer Hochschule) zur Arbeit mit dem Betriebssystem. Des Weiteren müssen die Hochschulen und Forschungseinrichtungen die Einhaltung der datenschutzrechtlichen Vorschriften gegenüber Dritten gewährleisten.

Hochschulen und Forschungseinrichtungen sind in der Regel öffentlich-rechtliche Körperschaften der Länder. Als öffentliche Stellen der Länder müssen sie den Anforderungen gerecht werden, die die jeweiligen Datenschutzgesetze der Länder ihnen im Umgang mit personenbezogenen Daten auferlegen (vgl. § 2 Abs. 1 Datenschutzgesetz NRW (DSG NRW)[3]).

---

[1] *FAZ*, So drehen Sie Windows 10 den Datenhahn zu ‘, 21.02.2016, http://www.faz.net/aktuell/technik-motor/computer-internet/so-drehen-sie-microsoft-windows-10-den-datenhahn-zu-14070291.html (zuletzt abgerufen am: 28.07.2016); *SZ*, Hallo Windows 10, Tschüss Privatsphäre, 05.08.2015, http://www.sueddeutsche.de/digital/windows-vertrauter-spion-1.2594765 (zuletzt abgerufen am: 28.07.2016)

[2] *Heise online*, Datenschutz bei Windows 10: Verbraucherschützer verklagen Microsoft, 29.02.2016, http://www.heise.de/newsticker/meldung/Datenschutz-bei-Windows-10-Verbraucherschuetzer-verklagen-Microsoft-3120481.html (zuletzt abgerufen am: 28.07.2016).

[3] Im Folgenden werden exemplarisch die Vorschriften des Datenschutzgesetzes NRW dargestellt. Die Datenschutzgesetze anderer Bundesländer enthalten vergleichbare Regelungen.

Personenbezogene Daten sind alle Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (vgl. § 3 Abs. 1 DSG NRW). Überall dort, wo Hochschulen oder Forschungseinrichtungen personenbezogene Daten Hochschulangehöriger oder ihrer Mitarbeiter verarbeiten, müssen sie den datenschutzrechtlichen Anforderungen gerecht werden. Jede Verarbeitung personenbezogener Daten muss entweder durch eine Rechtsvorschrift erlaubt sein oder auf die Einwilligung der betroffenen Person gestützt werden können (vgl. § 4 Abs. 1 DSG NRW). Eine zulässige Datenverarbeitung aufgrund einer gesetzlichen Erlaubnis besteht insbesondere dann, wenn dies zur Erfüllung der Aufgaben der jeweiligen Stelle erforderlich ist (vgl. § 12 Abs. 1 DSG NRW).

C. Notwendige Unterscheidung verschiedener Fallkonstellationen

Bei der Datenverarbeitung an Hochschulen und Forschungseinrichtungen ist zwischen verschiedenen Verarbeitungskonstellationen zu unterscheiden. Es werden einerseits personenbezogene Daten Dritter verarbeitet, z.B. persönliche Informationen der Studierenden. In diesem Fall nutzt die betroffene Person die IT-Infrastruktur nicht selbst. Die Daten werden vielmehr von Mitarbeitern der Hochschulen oder Forschungseinrichtungen verarbeitet. Andererseits nutzen aber Mitarbeiter und sonstige Nutzer auch selbst die von der Einrichtung bereitgestellten Rechner. Dabei wird auch immer ein Mindestmaß persönlicher Daten des Nutzers verarbeitet, z.B. die jeweilige Nutzerkennung.

Es muss im Hochschul- oder Forschungsbetrieb somit die Verarbeitung personenbezogener Daten Dritter durch Mitarbeiter der datenverarbeitenden Stelle (s. unter B. I.) von der Verarbeitung personenbezogener Daten des Nutzers selbst (s. unter B. II.) unterschieden werden.

I. Verarbeitung personenbezogener Daten Dritter

Verarbeitet ein Mitarbeiter der Hochschule oder Forschungseinrichtung personenbezogene Daten Dritter, so muss sichergestellt sein, dass im Verhältnis zwischen der Hochschule/Forschungseinrichtung und dem betroffenen Dritten eine zulässige Datenverarbeitung vorliegt. Welches Betriebssystem für die Datenverarbeitung eingesetzt wird, ist insoweit zunächst unerheblich. Bei der Verarbeitung darf es zu keiner unzulässigen Übermittlung von Daten an eine dritte Stelle kommen. Des Weiteren müssen die zur

Durchsetzung des Datenschutzrechts erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden. Insbesondere die Zugriffssicherung muss gewährleistet werden.

1. Übermittlung

Beim Einsatz von Windows 10 können sich Probleme daraus ergeben, dass Microsoft u.U. Zugriff auf verschiedene Daten erhält bzw. diese an Microsoft gesendet werden. Aus rechtlicher Sicht kann es sich hierbei um eine Übermittlung von Daten an einen Dritten handeln. Dritter wäre in diesem Fall Microsoft und somit eine datenverarbeitende Stelle außerhalb des Verhältnisses zwischen der Hochschule/Forschungseinrichtung und der von der Datenverarbeitung betroffenen Person. Diese Überlegung lässt sich auch auf den Einsatz anderer Betriebssysteme übertragen.

Unter einer Übermittlung ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise zu verstehen, dass die Daten durch die verantwortliche Stelle weitergegeben oder zur Einsichtnahme bereitgehalten werden oder dass der Dritte zum Abruf in einem automatisierten Verfahren bereitgehaltene Daten abruft (vgl. § 3 Abs. 2 Nr. 4 DSG NRW). Eine Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs – wie z.B. Microsoft – ist nur erlaubt, wenn ein gesetzlicher Erlaubnistatbestand eingreift oder die betroffene Person einwilligt (vgl. § 16 Abs. 1 DSG NRW).

Den Datenschutzbestimmungen von Microsoft (Stand: Januar 2016) ist zu entnehmen, dass Microsoft Daten sowohl in den USA als auch in jedem anderen Land verarbeiten kann, in dem Tochterunternehmen, Niederlassungen oder Diensteanbieter-Einrichtungen ansässig sind.[4] Da insoweit eine Datenverarbeitung in den USA nicht ausgeschlossen werden kann, wären im Fall des Einsatzes von Windows 10 die Anforderungen zu beachten, die die Datenschutzgesetze an die Übermittlung an Stellen außerhalb der Mitgliedstaaten der EU stellen. Grundsätzlich ist hier entscheidend, dass ein angemessenes Datenschutzniveau gewährleistet wird (vgl. § 17 Abs. 1 DSG NRW). Nachdem der Europäische Gerichtshof im Oktober 2015 das Safe-Harbor-Abkommen für ungültig erklärt hat, besteht diesbezüglich eine gewisse Rechtsunsicherheit. Das Folgeabkommen (EU-US Privacy Shield), das im Juli

[4] *Microsoft Corporation*, Datenschutzbestimmungen von Microsoft, https://privacy.microsoft.com/de-de/privacystatement/ (zuletzt abgerufen am: 28.07.2016)

2016 verabschiedet wurde, wird bereits jetzt kritisch beurteilt. Ob eine Datenübermittlung auf dieser Grundlage zulässig ist, ist daher zumindest unsicher. Die Übermittlung von personenbezogenen Daten in die USA ist daher zu vermeiden.

Verschiedene Funktionen und Zusatzprogramme bei Windows 10 sehen eine Zugriffsmöglichkeit auf Daten von Microsoft oder die Weitergabe dieser an Microsoft vor, z.B. Cortana und OneDrive. Soweit persönliche Daten Dritter betroffen sind, sollten diese Funktionen unbedingt deaktiviert werden. Mangels einer gefestigten Rechtsprechung besteht bei der Frage, was eine Übermittlung im Rechtssinne letztlich ist, zwar eine gewisse Unsicherheit. Dennoch sollte der Zugriff auf Daten von Microsoft verhindert werden. Auch wenn die Voraussetzungen des Übermittlungsbegriffs nicht erfüllt sein sollten, kann zumindest ein Verstoß gegen die Verpflichtung zur Erfüllung technischer und organisatorischer Maßnahmen zur Durchsetzung des Datenschutzrechts vorliegen.

2. Technische und organisatorische Maßnahmen

Erlangt ein Dritter, wie z.B. Microsoft, unerlaubt Zugriff auf personenbezogene Daten, ist die Verpflichtung der datenverarbeitenden Stelle berührt, die Ausführung der Vorschriften des Datenschutzes durch technische und organisatorische Maßnahmen sicherzustellen (vgl. § 10 Abs. 1 DSG NRW). Der Begriff der technischen und organisatorischen Maßnahmen ist weit auszulegen und kann sich u.a. auf den Aufbau, den Ablauf und die Ausstattung der datenverarbeitenden Stelle beziehen.[5] Insbesondere sind solche Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können (vgl. § 10 Abs. 2 Nr. 1 DSG NRW). Die Vertraulichkeit der Daten soll sichergestellt werden, z.B. mithilfe von Verschlüsselungstechnik. Kommt die datenverarbeitende Stelle der genannten Verpflichtung nicht nach, kann eine unzulässige Datenverarbeitung vorliegen.[6] Es liegt nahe, dass auch die Wahl eines angemessenen Betriebssystems eine solche technisch-organisatorische Maßnahme darstellen kann. Setzt die Hochschule oder Forschungseinrichtung ein Betriebssystem ein, bei dem die Einhaltung des Datenschutzstandards nicht gewährleistet werden kann, kann ein Verstoß gegen die Verpflichtung aus § 10 DSG NRW vorliegen. Verwendet die Hochschule oder Forschungseinrichtung Windows 10, so muss durch die Konfiguration durch den Nutzer oder

[5] *Ernestus/Simitis*, BDSG, 8. Aufl. 2014, § 9 Rn. 20; Stähler/Pohler, Datenschutzgesetz Nordrhein-Westfalen, 3. Aufl. 2003, Erl. § 10 DSG Rn. 3 f.
[6] *Stähler/Pohler*, Datenschutzgesetz Nordrhein-Westfalen, 3. Aufl. 2003, Erl. § 10 DSG Rn. 4.

den Administrator sichergestellt werden, dass den Anforderungen des Datenschutzrechts Rechnung getragen wird und kein Zugriff von Microsoft auf personenbezogene Daten Dritter möglich ist. Gleiches gilt bei dem Einsatz eines anderen Betriebssystems.

II. Verarbeitung personenbezogener Daten des Nutzers

Bei der Nutzung der IT-Infrastruktur der jeweiligen Hochschule oder Forschungseinrichtung durch die betroffene Person selbst, stellt sich die Situation anders dar. Die betroffene Person hat eine größere Kontrolle über die Verarbeitung der eigenen Daten. Sie kann selbst über die Nutzung verschiedener Funktionen eines Betriebssystems entscheiden. So kann sie bspw. beim Einsatz von Windows 10 in die Verarbeitung ihrer Daten durch Microsoft einwilligen.

Allerdings muss die jeweilige Hochschule oder Forschungseinrichtung gewährleisten, dass ihre Mitarbeiter und Studierenden durch den Einsatz des jeweiligen Betriebssystems nicht zwangsläufig Daten an den Hersteller übermitteln müssen. Wird z.B. Windows 10 so eingesetzt, dass notwendige Funktionen nur genutzt werden können, wenn personenbezogene Daten an Microsoft übermittelt werden, ist die Freiwilligkeit einer Einwilligung des jeweiligen Nutzers in die Datenverarbeitung aufgrund faktischen Zwangs zumindest sehr fraglich.

Eine Einwilligung ist nur wirksam, wenn sie freiwillig erteilt wird, also frei von Zwang. Dies ist insbesondere im Verhältnis zwischen Arbeitgeber (hier Hochschule/Forschungseinrichtung) und Arbeitnehmer problematisch, da der Arbeitnehmer in einem Abhängigkeitsverhältnis zum Arbeitgeber steht. Zwar besteht auch im Arbeitsverhältnis grundsätzlich die Möglichkeit, dass sich ein Arbeitnehmer frei dazu entscheidet, einer Datenverarbeitung zuzustimmen. Ob die Einwilligung aber freiwillig erteilt wird, ist nach den Umständen des jeweiligen Einzelfalls zu beurteilen. Bedeutung kann diese Frage auch im Verhältnis zwischen Hochschule und Studierenden gewinnen, wenn Hochschulen Angebote zur Verfügung stellen, auf die die Studierenden angewiesen sind und somit nicht gänzlich frei über die Nutzung entscheiden können, sondern einem faktischen Zwang unterliegen.

Soweit es sich um Dienste handelt, die der Nutzer nicht zwingend einsetzen muss, hat er selbst die Möglichkeit frei und ohne Zwang über den Einsatz der Dienste zu entscheiden und in die Datenverarbeitung einzuwilligen. Ist dies der Fall, muss die Hochschule oder Forschungseinrichtung die Einhaltung datenschutzrechtlicher Anforderungen ihrerseits nicht gewährleisten, denn es ist lediglich das Verhältnis zwischen Hersteller und Nutzer betroffen.

D. Literaturliste

- *Max-Planck-Gesellschaft*, Orientierungshilfe zur datenarmen Konfiguration von Windows 10, abrufbar unter: https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf (zuletzt abgerufen am: 28.07.2016);
- *Der Landesbeauftragte für den Datenschutz Baden-Württemberg*, Datenschutzeinstellung bei Windows 10 – Wie Sie Windows 10 datenschutzfreundlich nutzen können, abrufbar unter: http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2015/11/2015_okt-leitfaden-win-10.pdf (zuletzt abgerufen am: 28.07.2016);
- *Heiko Weckbrodt, Technische Universität Dresden*, Windows 10 telefoniert in jedem Fall „nach Hause“, abrufbar unter: http://oiger.de/2016/03/14/windows-10-telefoniert-in-jedem-fall-nach-hause/158527 (zuletzt abgerufen am: 28.07.2016).

Münster, Juli 2016

Forschungsstelle Recht im Deutschen Forschungsnetz

Die Forschungsstelle Recht ist ein Projekt an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung unter Leitung von Prof. Dr. Thomas Hoeren, Leonardo-Campus 9, D-48149 Münster, E-Mail: recht@dfn.de