bratschi
wiederkehr
& buob

Markus Näf
Master of Law, Rechtsanwalt
Senior Project Manager IPMA Level B
Lehrbeauftragter für Informatikrecht und
Projektmanagement an der FHS St. Gallen
Telefon +41 58 258 10 00
markus.naef@bratschi-law.ch

Datenschutzrechtliche Pflichten beim Einsatz von Internet-Services und Software-Anwendungen

Anwendungen über Online-Services gehören heute zum Geschäftsalltag. In letzter Zeit hört man immer wieder von Online-Services, die Daten der Anwender sammeln und an den Anbieter oder Dritte im Ausland übermitteln. Dies betrifft nicht nur private Anwender von Apps oder Social Media Plattformen, sondern zunehmend auch Business Anwendungen. Zudem ist das Problem der Datenerhebung nicht nur auf Online-Services, die als Application as a Service (AaaS) oder Software as a Service (SaaS) angeboten werden, beschränkt.

Grundsätzlich ist ein Unternehmen mit zwei Ausnahmen frei zu entscheiden, ob es seine Geschäftsdaten ins Ausland übermittelt oder einem Dritten verfügbar macht. Die beiden Ausnahmen sind erstens, wenn es sich um Personendaten im Sinne des Datenschutzgesetztes (DSG) handelt und zweitens, wenn Daten betroffen sind, die einer gesetzlichen Geheimhaltungspflicht unterliegen, wie zum Beispiel dem Bank-, Anwalts- oder Arztgeheimnis. Solche Daten dürfen nicht ohne ausdrückliche Entbindung vom Berufsgeheimnis ins Ausland übermittelt oder Dritten verfügbar gemacht werden.

1. Kritische Unternehmensdaten

Unabhängig der Datenkategorie, sollten sich Unternehmen bei der Speicherung von Daten ausserhalb des Unternehmens, sei dies in einem Rechenzentrum, einer Cloud Anwendung oder einem Online-Service, vier relevante Fragen stellen:

(i) Wo werden Unternehmensdaten geografisch gespeichert? Nur in der Schweiz oder auch im Ausland?
(ii) Wie wird der Zugriff auf Unternehmensdaten, die bei Dritten gespeichert sind, jederzeit sichergestellt?
(iii) Wie wird sichergestellt, dass keine Drittpersonen Zugriff auf Daten des Unternehmens haben?
(iv) Wie stellt das Unternehmen sicher, dass nach einer Vertragsauflösung alle Daten vollständig gelöscht werden?

Die Unternehmensführung ist für die Daten des Unternehmens verantwortlich und verschiedene gesetzliche Vorschriften regeln Bekanntgabe, Auslagerung oder Aufbewahrung von Daten. Diese Fragen sind jedoch nicht nur beim Einsatz von Online-Diensten relevant, sondern zunehmend auch beim Einsatz von Standardsoftware.

2. Automatische Datenübermittlung bei Microsoft Windows

Das neue Betriebssystem Windows 10 von Microsoft aus dem Jahr 2015 ist stark mit den Cloud Diensten von Microsoft, wie zum Beispiel Office 365, verzahnt. Die Software übermittelt verschiedene Randdaten der Nutzung an Microsoft. Die übermittelten Daten sind je nach Version unterschiedlich (Home, Professional, Enterprise). Der User gibt mit der Akzeptanz der Lizenz- und Datenschutzbestimmungen von Microsoft seine Zustimmung zu dieser Datenübermittlung. Das Unternehmen kann jedoch nicht ohne weiteres für die Übermittlung oder Bekanntgabe von Daten seiner Kunden oder Mitarbeitenden an Dritte zustimmen.

2.1 Datenübermittlung an Microsoft

Neu ist, dass es sich dabei eben nicht um eine Cloud Anwendung, sondern um eine On-site Installation von Windows 10 auf Servern beim Kunden bezieht. Der Lizenzvertrag von Microsoft verweist unter Ziffer 3 auf die Microsoft-Datenschutzerklärung. Mit dem Lizenzvertrag stimmt das Unternehmen dieser Datenübermittlung zu.

Zum Opt-out Verfahren schreibt Microsoft:[1]

> *„Einige der in diesem Artikel beschriebenen Netzwerkverbindungen können in Windows 10 Mobile, Windows 10 Mobile Enterprise und der Juliversion von Windows 10 verwaltet werden. Die Verwaltung aller Verbindungen ist jedoch nur mit Windows 10 Enterprise (Version 1511) oder Windows 10 Education (Version 1511) möglich. In Windows 10 Enterprise (Version 1511) oder Windows 10 Education (Version 1511) können Sie die Telemetrie auf der Sicherheitsstufe konfigurieren, Windows Defender-Telemetrie und MSRT Berichte deaktivieren sowie alle anderen Verbindungen mit Microsoft-Diensten wie in diesem Artikel beschrieben deaktivieren, um zu verhindern, dass Windows Daten an Microsoft sendet. Wir raten allerdings dringend davon ab, da uns diese Daten dabei helfen, ein sicheres, zuverlässiges und noch attraktiveres personalisiertes Benutzererlebnis bereitzustellen."*

Bei den Telemetrie-Daten sind drei Stufen der Datenübermittlung (vollständig, erweitert und allgemein) vorgesehen. Die Voreinstellung von Microsoft ist auf Stufe „vollständig". Damit erlaubt der Anwender Microsoft unter bestimmten Bedingungen alle Daten auf dem Rechner zu übermitteln und für die Fehlerdiagnose zu verwenden. Microsoft darf diese Daten zu diesem Zweck auch an Vertragspartner weitergeben. Sollte ein Fehlerbericht persönliche Informationen enthalten, werden diese nicht dazu verwendet, Sie zu identifizieren, zu kontaktieren oder gezielt Werbung zu schalten.

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

Damit ist mit der Einstellung „vollständig“ ein sehr weitgehender Datenzugriff möglich und die Daten können in die beliebigen Standorte von Microsoft übermittelt werden. Die vertragliche Einschränkung die Daten nicht für andere Zwecke zu verwenden, vermag den Tatbestand der Datenübermittlung von persönlichen Daten nicht zu rechtfertigen. Bei der Funktionswahl „allgemein“ (oder in gewissen Publikationen auch „einfach“ genannt) und dem Ausschalten aller Optionen werden trotzdem einzelne Daten übermittelt.

Einige Diagnosedaten sind für die Ausführung von Windows notwendig und können nicht deaktiviert werden. Darunter fallen hauptsächlich technische Daten ohne Identifizierungspotential aber zusätzlich auch die IP-Adresse, die im Sinn des Datenschutzgesetzes als Personendaten qualifiziert werden.

2.2 Datenherausgabe an Behörden

Ein US-Richter erliess auf der Basis des «Stored Communication Act» in den USA eine Durchsuchungs- und Beschlagnahmeverfügung (Warrant) gegen das Microsoft Hauptquartier in Redmond bezüglich der Daten eines Kunden, welche in einem Microsoft Web-Mail Account von «Outlook.com» auf einem Server im Microsoft Datacenter in Irland gespeichert waren. Die in den USA gespeicherten Randdaten des Kunden wurden aufgrund dieser Verfügung den amerikanischen Behörden ausgehändigt, nicht jedoch die ausserhalb der USA gespeicherten Inhaltsdaten. Der «District Court of the Southern District New York» lehnte einen Rekurs von Microsoft gegen die Lieferung der im Ausland gespeicherten Daten ab und auferlegte Microsoft zusätzlich eine Strafe bei Nichterfüllung der Datenlieferung. Microsoft legte gegen dieses Urteil Berufung ein.

Das US-Berufungsgericht – der «United States Court of Appeals for the second Circuit» – hat am 14. Juli 2016 nun entschieden, dass eine Datenherausgabe nach dem «Stored Communication Act» auf der Basis einer Verfügung nur Wirkung innerhalb des Territoriums der USA hat. Microsoft kann nicht verpflichtet werden, auf Kundendaten, die auf einem Server ausserhalb der USA liegen, zuzugreifen und diese Daten in die USA zu importieren, um sie den US Behörden zu übergeben.

2.3 Übermittlung von Randdaten

Wie aus dem US Gerichtsurteil hervorgeht, werden durch Microsoft bei einer Vereinbarung über die Datenspeicherung in Irland trotzdem Randdaten in die USA übermittelt.[2] Die betroffenen Daten mussten nicht herausgegeben werden, da das betreffende Gesetz dies für im Ausland liegende Daten nicht explizit vorsieht. Das Urteil legt aber offen, dass in allen Fällen einzelne Randdaten, wie z.B. E-Mail-Adressen, Usernamen oder IP-Adressen des E-Mail-Verkehrs sowie zufällige Testdaten von Webmail-Kunden in den USA gespeichert werden. Dagegen werden aber keine Inhalte von Kunden aus europäischen Rechenzentren in den USA gespeichert. Gemäss Gerichtsurteil ist es Microsoft jedoch theoretisch technisch möglich, von den USA aus auf die Daten im Datacenter in Irland zuzugreifen.

[2] http://digitalconstitution.com/wp-content/uploads/2016/07/Decision-opinion.pdf

Zudem enthalten einzelne Datenschutzbestimmungen eine pauschale Regelung, dass Microsoft von in Europa gespeicherten Daten Sicherheitskopien in jedem ihrer Rechenzentren überall auf der Welt erstellen darf. Dies ist in den Produktebestimmungen enthalten, jedoch nicht in den Online Service Terms.

Personalisierte Anwendungen, wie zum Beispiel Cortana von Microsoft oder die Onlineübersetzung fragen nicht nur Randdaten, sondern auch Inhaltsdaten, auf dem Rechner ab und übermitteln diese an Microsoft. Dies ist bei Personendaten oder Daten, welche Berufsgeheimnissen unterstehen ohne Einwilligung der betroffenen Personen nicht zulässig.

Derzeit läuft eine Voruntersuchung beim Eidgenössischen Datenschutz und Öffentlichkeitsbeauftragen (EDÖB) über die Konformität dieser Datenübermittlung von Microsoft mit dem Datenschutzgesetz. Die Antwort liegt noch nicht vor.[3] Das Ergebnis des EDÖB wird eine abschliessende Beurteilung sowie den konformen Umgang der Unternehmen mit dieser Datenübermittlung regeln. Bis dahin sind die Unternehmen gehalten, die Einstellungen und Vertragsbedingungen sorgfältig zu prüfen.

3. Online Services

Es werden heute viele hilfreiche und sehr effiziente Online-Services für Unternehmen bereitgestellt, so zum Beispiel Applikationen für Bewerberselektion, Personalverwaltung, Marketing und Kundenbeziehungsmanagement, Buchhaltung und viele mehr. Gemeinsam ist allen diesen Online-Angeboten, dass die Daten auf den Servern der Anbieter in der Cloud gespeichert werden. Damit ist auch eine Datenübermittlung ins Ausland verbunden. So speichern Dienste wie „Drop-Box“, „Microsoft Office365“ oder „GoogleDrive“ Daten in Rechenzentren in Europa oder auch in den USA.

4. Datenbearbeitung durch einen Dritten

Das Datenschutzgesetz lässt eine Bearbeitung von Personendaten durch Dritte unter vier Voraussetzungen zu:

(i) Es braucht dazu eine entsprechende Vereinbarung;
(ii) Der Dritte darf die Daten nur so bearbeiten, wie es der Auftraggeber selbst tun dürfte;
(iii) Keine gesetzliche oder vertragliche Geheimhaltungsplicht darf es verbieten;
(iv) Der Auftraggeber muss sicherstellen, dass der Dritte die Datensicherheit gewährleistet.

Eine Auftragsbearbeitung liegt nur vor, wenn die Bearbeitung ausschliesslich für die Zwecke des Auftraggebers erfolgt, nicht aber, wenn eigene Zwecke des Auftragsbearbeiters oder diejenigen eines Dritten verfolgt werden. Nur im ersteren Fall besteht ein sogenanntes Bekanntgabeprivileg, womit die Rechtsfolgen, welche mit der Bekanntgabe an Dritte verbunden sind, nicht ausgelöst werden. Bearbeitet der Auftragsbearbeiter die Daten auch für eigene Zwecke oder für Dritte, ist

[3] Mitteilung EDÖB: <https://www.edoeb.admin.ch/dokumentation/00153/01353/01365/index.html?lang=de>, abgefragt am 25.8.2016.

eine Registrierung der Datensammlung sowie eine Information der betroffenen Personen notwendig. Bei besonders schützenswerten Personendaten oder bei Persönlichkeitsprofilen ist ausserdem eine Einwilligung oder eine Rechtfertigung bei der Datenweitergabe angezeigt. Konzerngesellschaften gelten ebenfalls als Dritte und es ist entsprechend bei einer konzerninternen Datenbearbeitung zwingend eine schriftliche Datenbearbeitungsvereinbarung abzuschliessen.

5. Datenübermittlung ins Ausland

Die Datenübermittlung ins Ausland ist mit den heutigen Internetanwendungen und Cloud-Lösungen eher die Regel als die Ausnahme. So speichern Dienste wie „Drop-Box", „Microsoft Office365" oder „GoogleDrive" Daten in Rechenzentren in Europa oder auch in den USA.

Das Datenschutzgesetz macht über die Zulässigkeit der Datenübermittlung eine Negativabgrenzung:

> *„Personendaten dürfen nicht ins Ausland übermittelt werden, wenn durch eine Übermittlung die Persönlichkeit der betroffenen Person gefährdet würde, namentlich weil im Land eine Gesetzgebung fehlt, die einen angemessenen Schutz der Daten und der Persönlichkeit gewährleistet (Art. 6 Abs. 1 DSG)."*

Der EDÖB veröffentlicht auf seiner Internetseite eine Liste der Länder mit gleichwertigem Datenschutz. Dazu gehören alle Länder der EU, jedoch nicht die USA. Für die USA galt bis vor kurzem das „Safe Harbour Agreement" als vertragliche Datenschutzregelung, die jedoch mit dem Entscheid des Europäischen Gerichtshofs im Oktober 2015 als ungenügend qualifiziert wurde. Entsprechend kommen für die Datenübermittlung entweder die Einwilligung der betroffenen Person oder eine vertragliche Vereinbarung mit hinreichenden Garantien für einen angemessenen Schutz der Daten im Ausland als Rechtfertigung in Frage.

Der EDÖB veröffentlicht dazu auf seiner Webseite einen Mustervertrag. Der EDÖB ist über den Abschluss einer solchen vertraglichen Datenschutzvereinbarung zu informieren. Dies gilt auch bei der Datenübermittlung in Länder ohne angemessenen Datenschutz innerhalb von Konzerngesellschaften.

Bestehen besondere gesetzliche Vorschriften zum Schutz der Personendaten, wie im Bankgengesetz, Anwaltsgesetz, Arztgeheimnis, Gesundheitsgesetz etc., ist eine Datenübermittlung ins Ausland vermutungsweise nicht zulässig. Mit der Einwilligung der betroffenen Person nach einer Aufklärung über die bestehenden Risiken, kann eine solche Übermittlung zulässig sein, ist aber im Einzelfall zu prüfen.

6. Tatbestand der Datenübermittlung

Online Services, welche auf die gespeicherten Inhaltsdaten zugreifen, sind in Bezug auf die abgelegten Daten zu beurteilen, insbesondere ob dadurch keine Persönlichkeitsrechte von Dritten bei einer Datenübermittlung ins Ausland verletzt werden können.

Damit muss als Zwischenfazit festgestellt werden, dass eine Cloud-Speicherung von Daten im Ausland für Anwender mit Personendaten, Persönlichkeitsprofilen oder besonders schützenswerten Personendaten sowie Daten, die einem Berufsgeheimnis unterliegen, nach dem Datenschutzgesetz nicht zulässig ist.

Ebenfalls ist aus heutiger Sicht die Verwendung von Windows 10 mit der Sicherheitsoption „vollständig“ aufgrund der Datenübermittlung ins Ausland nicht ohne weiteres zulässig. Bei der Einstellung „allgemein“ sind keine Inhaltsdaten betroffen, sondern lediglich die Randdaten und die in den Systemen erfassten Nutzerdaten der Mitarbeitenden, welche für die Bereitstellung der Services von Microsoft erfasst werden müssen. Dabei darf der Arbeitgeber die Personendaten der Mitarbeitenden gemäss Art. 328b OR zwar bearbeiten, dies umfasst jedoch nicht die Übermittlung ins Ausland.

Usernamen und E-Mail-Adressen stellen Personendaten dar, aber auch IP-Adressen werden als Personendaten qualifiziert. Damit ist bei einer Übermittlung dieser Daten der Tatbestand der grenzüberschreitenden Bekanntgabe von Personendaten erfüllt. Eine solche ist nur in Ländern mit einem gleichwertigen Datenschutz zulässig, was insbesondere auf die USA nicht zutrifft. Damit ist eine Datenbekanntgabe nur nach den folgenden Tatbeständen zulässig:

> *„DSG Art. 6 Grenzüberschreitende Bekanntgabe*
> *1 Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.*
> *2 Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn:*
> *a) hinreichende Garantien, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland gewährleisten;*
> *b) die betroffene Person im Einzelfall eingewilligt hat;*
> *c) die Bearbeitung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags steht und es sich um Personendaten des Vertragspartners handelt;*
> *d) die Bekanntgabe im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;*
> *e) die Bekanntgabe im Einzelfall erforderlich ist, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen*
> *f) die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.*
> *g) die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.*
> *3 Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (Beauftragte, Art. 26) muss über die Garantien nach Absatz 2 Buchstabe a und die Datenschutzregeln nach Absatz 2 Buchstabe g informiert werden. Der Bundesrat regelt die Einzelheiten dieser Informationspflicht.“*

Microsoft garantiert den Schutz dieser Daten durch verschiedene Massnahmen, was als Rechtfertigung nach Abs. 2 lit. a DSG qualifiziert werden kann. Die Standardklauseln des EDÖB, resp. des Europäischen Datenschutzbeauftragten sind in den Online Service Terms von Microsoft enthalten.

Problematisch ist dabei, dass diese vertraglichen Garantien nach dem oben zitierten Art. 6 Abs. 3 DSG dem EDÖB gemeldet werden müssen.

Die Unterlassung dieser Meldung stellt ein Straftatbestand dar.

7. Empfehlung

(i) Die Zulässigkeit der Datenübermittlung und Datenspeicherung ist bei Online Services zu prüfen.

(ii) Die Sicherheitseinstellungen der Windows Server sind datenschutzkonform einzustellen.

(iii) Daten-Transfer-Vereinbarungen sind bei Datenübermittlungen ins Ausland abzuschliessen. Dies gilt ebenfalls bei einer konzerninternen Datenübermittlung.

(iv) Da für die Verwendung der verschiedenen Microsoft-Applikationen die Übermittlung von Randdaten notwendig ist und die Übermittlung dieser Randdaten in Zukunft noch zunehmen werden, empfehlen wir, die IT Nutzungsreglemente der Unternehmen mit der folgende Formulierung zu ergänzen:

„Bei der Nutzung von Produkten und Services von Drittanbietern wie Microsoft können einzelne Personendaten der Nutzer (zum Beispiel E-Mail-Adresse oder Autorisierungsdaten) an die Rechenzentren von Microsoft im Ausland – insbesondere auch in Länder ohne gleichwertigen Datenschutz (z.B. USA) – übermittelt werden. Der Nutzer stimmt durch die Nutzung der Microsoft Produkte dieser Datenübermittlung und -speicherung im Ausland nach den Datenschutzbestimmungen von Microsoft zu.“

Bei der Verwendung von anderen Produkten ist die Bestimmung entsprechend anzupassen.

(v) Aufnahme einer analogen Zustimmungserklärung in Kunden- oder Lieferverträgen. Zuletzt ist zu prüfen, ob Kundenverträge Compliance Klauseln betreffend Datenschutzverletzungen enthalten. Diese sind allenfalls zu präzisieren.

Basel
Lange Gasse 15
CH-4052 Basel
Telefon +41 58 258 19 00
Fax +41 58 258 19 99
basel@bratschi-law.ch

Bern
Bollwerk 15
Postfach 5576
CH-3001 Bern
Telefon +41 58 258 16 00
Fax +41 58 258 16 99
bern@bratschi-law.ch

Lausanne
Avenue Mon-Repos 14
Postfach 5507
CH-1002 Lausanne
Téléfone +41 58 258 17 00
Téléfax +41 58 258 17 99
lausanne@bratschi-law.ch

St. Gallen
Vadianstrasse 44
Postfach 262
CH-9001 St. Gallen
Telefon +41 58 258 14 00
Fax +41 58 258 14 99
stgallen@bratschi-law.ch

Zug
Industriestrasse 24
CH-6300 Zug
Telefon +41 58 258 18 00
Fax +41 58 258 18 99
zug@bratschi-law.ch

Zürich
Bahnhofstrasse 70
Postfach
CH-8021 Zürich
Telefon +41 58 258 10 00
Fax +41 58 258 10 99
zuerich@bratschi-law.ch