Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Sync&Share-Policy

Version 1.0

22.08.2016

Einleitung

Diese Richtlinie beinhaltet grundsätzliche Regelungen für alle Mitglieder der Universität Hamburg, die im Rahmen ihrer dienstlichen Tätigkeit Sync&Share-Dienste zur Datenablage, Datensynchronisation und zum kooperativen Teilen nutzen. Sie informiert über allgemeine Risiken und hilft bei der Klärung der Frage, in welchen Fällen und unter welchen Bedingungen diese Dienste genutzt werden dürfen.

Wenn (personenbezogene) Daten mit Hilfe von Sync&Share-Diensten gespeichert bzw. verarbeitet werden, drohen spezielle Gefahren. Insbesondere die dynamische Verteilung der Speicherkapazitäten, möglicherweise über verschiedene Standorte, die in der Regel dem Nutzer nicht bekannt sind, verlangen eine spezifische Vorsorge hinsichtlich der Informationssicherheit und des Schutzes der Daten.

Für die Verarbeitung personenbezogener Daten in Sync&Share-Diensten gelten die Bestimmungen des Datenschutzgesetzes des Landes Hamburg (HmbDSG). Es fordert entweder die Einwilligung der Betroffenen (im Fall der Datenverarbeitung außerhalb der EU), oder die Anwendung der Regelungen zur Auftragsdatenverarbeitung (Datenverarbeitung innerhalb der EU). Zusätzlich sind universitätsinterne Regelungen (z. B. Dienstvereinbarungen) zu beachten.

Im privaten Umfeld werden Sync&Share-Dienste häufig relativ sorglos genutzt. Vor dem Hintergrund der sich immer mehr auflösenden Trennung von privaten und dienstlichen Belangen, speziell im IT-Umfeld, soll diese Richtlinie zur Sensibilisierung gegenüber den potentiellen Risiken beitragen und entsprechende Handlungsanleitungen geben.

Dieses Dokument basiert auf der „Richtlinie zur Auslagerung von Daten in die Cloud“ der Freien Universität Berlin[1].

[1] AG IT-Sicherheit, Freie Universität Berlin, Kaiserswerther Str. 16/18, 14195 Berlin, „Richtlinie zur Auslagerung von Daten in die Cloud“, 2. Dezember 2011. www.mi.fu-berlin.de/wiki/pub/IT/ItProcess/Richtlinie_Cloud-Datenablage_-_1_0.pdf

1 Geltungsbereich

Diese Richtlinie gilt für alle Mitglieder der Universität Hamburg, die im Rahmen dienstlicher Tätigkeiten für die Universität Hamburg Daten erheben, speichern, kooperativ teilen, auf verschiedenen Geräten synchronisieren oder verarbeiten.

2 Abgrenzung und Begriffsdefinition

Dateidienste sowie Dienste zur Datensynchronisation und zum kooperativen Teilen, die unabhängig von Ort und Zeit über ein Kommunikationsnetz genutzt werden können, werden in dieser Richtlinie kurz als „Sync&Share“ bezeichnet.

> *Sync&Share bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von Dateidiensten über ein Netz. In der Regel können diese Dateidienste unabhängig von Ort und Zeit mit Hilfe aller gängigen IT-Geräte genutzt werden. Für die Nutzer bleibt die bereitgestellte IT-Infrastruktur verborgen. Weiterhin können Daten mit weiteren Personen organisationsübergreifend geteilt werden, um z. B. kooperativ an gemeinsamen Projekten zu arbeiten. Mit Sync&Share ist es möglich, Daten auf verschiedene Geräteklassen zu synchronisieren.*

Diese Richtlinie betrachtet Aspekte der Speicherung von Daten, also der kurzzeitigen oder längerfristigen Überlassung von Daten an interne oder externe Dienstanbieter, mit Hilfe von Sync&Share-Diensten.

3 Datenkategorien und ihre Eignung zur Sync&Share-Nutzung

Für die Entscheidung, unter welchen Bedingungen eine Auslagerung von Daten in einen Sync&Share-Dienst in Frage kommt, bildet der Schutzbedarf der Daten die grundlegende Richtschnur.

Hinweise auf den Schutzbedarf können zum einen aus der systematisch durchgeführten Schutzbedarfsanalyse und zum anderen aus der Datenkategorie abgeleitet werden. Daten lassen sich in die folgenden Kategorien einteilen:

Kategorie	**Hinweis auf typischen Schutzbedarf**
Daten, die aus öffentlich zugänglichen Quellen stammen	Keinen
Dienstliche (nicht wissenschaftliche) Daten (z. B. aus den Bereichen Verwaltung und Lehre)	Hoch bis sehr hoch
Wissenschaftliche Daten (z. B. Untersuchungsergebnisse, Messreihen)	Normal bis sehr hoch
Personalaktendaten	Sehr hoch
Private Daten (z. B. Kontaktdaten von Freunden)	Normal bis sehr hoch

In jedem Fall sind die folgenden Aspekte zu beachten:

- Für personenbezogene Daten (sowohl mit dienstlichem als auch privatem Bezug) gelten die Bestimmungen des Datenschutzes.
- Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Geheimhaltungsvereinbarungen).

Ein Schutzbedarf wird grundsätzlich hinsichtlich der drei Schutzziele **Verfügbarkeit, Integrität** und **Vertraulichkeit** differenziert bestimmt. Entsprechend differenziert müssen Vorkehrungen zur Sicherheit der Daten getroffen werden. Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung zur Speicherung in Sync&Share-Diensten:

Schutzbedarf	**Eignung für die Ablage**
Daten mit keinem oder normalen Schutzbedarf	Ja
Daten mit hohem Schutzbedarf	Verschlüsselt, wenn technisch umsetzbar
Daten mit sehr hohem Schutzbedarf	Nein

4 Regelungen

Bevor Daten in einem Sync&Share-Dienst abgelegt werden, müssen die im vorangegangenen Abschnitt 3 betrachteten Abhängigkeiten zwischen der Datenkategorie, dem Schutzbedarf der Daten und der Eignung beachtet werden. Darüber hinaus gelten die in diesem Abschnitt aufgestellten Regelungen.

(1) Sparsamer Umgang

Prinzipiell sollten bei der Nutzung entsprechender Sync&Share-Dienste die in Frage kommenden Datenmengen auf das notwendige Mindestmaß begrenzt werden. Beispielsweise kann bei der Übertragung ganzer Verzeichnisbäume in einen Sync&Share-Dienst leicht übersehen werden, dass in einem Unterverzeichnis sensible Daten abgelegt wurden, die den Bereich der Universität Hamburg nicht verlassen dürfen. Bevor Daten auf Speichersysteme externer Anbieter ausgelagert werden, müssen erwarteter Nutzen und damit verbundene Risiken gegeneinander abgewogen werden.

(2) Dienste der Universität Hamburg nutzen

Es sind die durch das RRZ bereitgestellten Basisdienste UHHShare (Sync&Share-Dienst, „Dropbox-Alternative“), UHHDisk (Dateidienste über WWW bzw. in Form von Netzlaufwerken) und Sharepoint (kooperative Kommunikations- und Informationsplattform, Portal) zu nutzen. Diese sind uneingeschränkt für Daten bis zur Schutzstufe hoch zu nutzen.

Nur wenn der benötigte Dienst nicht vom RRZ oder anderen Einrichtungen der Universität Hamburg bereitgestellt wird oder der bereitgestellte Dienst den Anforderungen nicht genügt, darf unter Beachtung der hier formulierten Grundsätze und entsprechender Beratung durch das RRZ auf Angebote externer Anbieter zurückgegriffen werden.

(3) Schutzbedarf der Daten bestimmt den Umfang der Sync&Share-Nutzung

Aus dem Schutzbedarf der für eine Auslagerung vorgesehenen Daten folgt nicht nur, ob eine Auslagerung zulässig ist, sondern auch unter welchen Bedingungen dies geschehen kann. Dabei ist der Schutzbedarf getrennt nach den drei Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit zu betrachten:

(3.1) Verfügbarkeit

Es muss vorab geprüft werden, welche Aussagen der Anbieter des Sync&Share-Dienstes zur Verfügbarkeit macht. Wenn sehr hohe Anforderungen an die Verfügbarkeit gestellt werden, kommt eine Datenablage in einem Sync&Share-Dienst nur in Frage, wenn der Anbieter des Sync&Share-Dienstes eine sehr hohe Verfügbarkeit garantiert.

(3.2) Integrität

Die Unverfälschbarkeit der Daten (Integrität) wird im Allgemeinen von Anbietern von Sync&Share-Diensten nicht garantiert. Wenn in dieser Hinsicht hohe oder sogar sehr hohe Anforderungen bestehen, muss der Nutzer selbst geeignete Maßnahmen zur Gewährleistung der Integrität ergreifen. Beispielsweise können Prüfsummen verwendet werden, mit deren Hilfe eine Veränderung an den Daten erkannt werden kann. In Systemen zur Datenverschlüsselung (siehe folgender Absatz) sind derartige Verfahren in der Regel bereits integriert.

(3.3) Vertraulichkeit

Wenn hohe Anforderungen an die Vertraulichkeit gestellt werden, ist als adäquate Maßnahme der Einsatz eines Datenverschlüsselungssystems zwingend notwendig. Viele Anbieter von Speicherplatz in Sync&Share-Diensten bieten auch Dienste zur Datenverschlüsselung an. Bei der Nutzung dieser Verschlüsselungsdienste ist in der Regel nicht zuverlässig nachvollziehbar, wer Zugriff auf die Schlüssel und damit auf die Daten hat. Der Zugriff des Dienstanbieters auf die Schlüssel muss ausgeschlossen sein. Darum sollte die Verschlüsselung selbst vorgenommen werden, bevor die Daten in den Sync&Share-Dienst übertragen werden. Die Sicherheit verschlüsselter Daten hängt u.a. von der Qualität des Verschlüsselungsalgorithmus, der Verschlüsselungssoftware, der Schlüssellänge und dem Schlüsselmanagement ab. Beim Einsatz von Verschlüsselung muss darauf geachtet werden, dass sie nach allgemein anerkannten Regeln als sicher gilt. Bei Daten mit sehr hohen Anforderungen an die Vertraulichkeit ist grundsätzlich von der Ablage in einem Sync&Share-Dienst abzusehen. Wenn in sehr seltenen Fällen dennoch derartige Daten in einen Sync&Share-Dienst ausgelagert werden müssen, sind die Daten zwingend vorher zu verschlüsseln. In diesem Fall muss die Verschlüsselung inklusive des Schlüsselmanagements unter der vollständigen Kontrolle durch kompetente Stellen der Universität Hamburg (z. B. RRZ) erfolgen.

(4) Löschung von Daten

Anbieter von Sync&Share-Diensten setzen normalerweise Speichertechniken zur effizienten Ausnutzung der physikalischen Speicherkapazitäten ein (Deduplizierung). Aufgrund dieser Speichertechnik können Daten oft erst nach einer gewissen Zeitspanne gelöscht werden. Grundsätzlich kann nicht ausgeschlossen werden, dass beim Absetzen des Löschbefehls die Daten lediglich für den Anwender ausgeblendet, aber nicht gelöscht werden. Daher sind Daten, die einer beispielsweise gesetzlichen Löschverpflichtung unterliegen, für die Ablage in Sync&Share-Diensten ungeeignet.

(5) Dienstrechtliche Vorgaben beachten

Insbesondere für Daten der Verwaltung (vor allen Dingen Personal- und Haushalts- und Finanzdaten) existieren oft detaillierte Vorschriften, wie mit diesen Daten umzugehen ist. Beispielsweise regeln verschiedene Vorschriften, dass Personalakten die Personalabteilung nicht ohne weiteres verlassen dürfen. Somit dürfen derartige Personaldaten auch nicht auf Speicher außerhalb der Universität Hamburg bzw. der Freien und Hansestadt Hamburg abgelegt werden. Inwieweit bei der Datenspeicherung dienstrechtlich Vorschriften zu beachten sind, muss im Zweifel unter Einbeziehung des jeweiligen Vorgesetzten geklärt werden.

(6) UHH-interne Regelungen beachten

Als Ergänzung oder Konkretisierung gesetzlicher Bestimmungen und Vorschriften gilt eine Reihe von universitätsinternen Regelwerken (z. B. Passwort-Richtlinie, Nutzungsordnungen etc.).

(7) Allgemeine Empfehlungen

Ergänzend zu den zuvor angesprochenen Themenbereichen sollten noch weitere Punkte beachtet werden:

S*ync&Share-Dienstanbieter mit Firmensitz außerhalb der EU:* Ein Umgang mit den Daten der Kunden gemäß den europäischen Datenschutzbestimmungen kann hier nicht vorausgesetzt werden. Insbesondere ist häufig unklar, welche Personen oder welche Stellen Zugriff auf die Daten erlangen. Für die Übermittlung personenbezogener Daten sind besondere Datenschutzvorschriften einzuhalten.

SLA (Service-Level-Agreement) bzw. AGB (Allgemeine Geschäftsbedingungen) des Anbieters: Vor der Inanspruchnahme eines Dienstes müssen die (vertraglichen) Bedingungen, unter denen der Dienst genutzt wird, bekannt und akzeptabel sein.

Zertifizierung des Anbieters: Wie ernst ein Anbieter die Sicherheit und den Schutz der Kundendaten nimmt, kann u.a. an dem Vorhandensein von anerkannten Prüfbescheinigungen (beispielsweise ISO 27001, entspricht BSI 100-1) abgelesen werden.

5 Checkliste und Fragenkatalog

Der folgende Fragenkatalog soll bei der Eignungsprüfung des Sync&Share-Angebots helfen.

1 *Prüfung interner Angebote*

- Wurde das Angebot des IT-Dienstleisters der Universität Hamburg (RRZ) geprüft?
- Ist ein UHH-Service zur Ablage der Daten geeignet?

2 *Prüfung der Vertragsbedingungen des externen Anbieters*

- Wurden die SLA (Service-Level-Agreement) bzw. AGB (Allgemeine Geschäftsbedingungen) des Anbieters angesehen?
- Passen die Bedingungen des Anbieters zu den Anforderungen?

3 *Prüfung der Verfügbarkeit*

- Erfüllt der Sync&Share-Dienst die Anforderungen an die Verfügbarkeit der Daten?

4 *Prüfung der Integrität*

- Erfüllt der Sync&Share-Dienst die Anforderungen an die Integrität der Daten?
- Wurden Vorkehrungen getroffen, hohe Integritätsanforderungen zu erfüllen?

5 *Unverschlüsselte Ablage*

- Gestatten die Anforderungen hinsichtlich der Vertraulichkeit der Daten eine unverschlüsselte Ablage in einem externen Sync&Share-Dienst?

6 *Verschlüsselte Ablage*

Wenn die Anforderungen hinsichtlich der Vertraulichkeit der Daten nur eine verschlüsselte Ablage in einem externen Sync&Share-Dienst erlauben:

- Wird die Verschlüsselung vor der Abspeicherung durchgeführt?
- Werden die Schlüssel ausschließlich im Bereich der Universität Hamburg abgelegt?

7 *Personenbezug*

Falls personenbezogene Daten in einem Sync&Share-Dienst abgelegt werden sollen:

- Wurde geprüft, ob alle datenschutzrechtlichen Anforderungen, insbesondere hinsichtlich der Auftragsdatenverarbeitung, erfüllt sind?

8 *Einhaltung der Vorschriften*

- Wurde geprüft, ob gesetzliche oder andere Vorschriften die Ablage der Daten auf Systemen außerhalb der Universität Hamburg gestatten?

9 *Löschung*

- Wurde geprüft, ob die Daten bestimmten Löschfristen unterliegen?
- Genügen die vom Sync&Share-Dienstanbieter bereit gestellten Dienste diesen Anforderungen?