

**Technisches und rechtliches
Rezertifizierungs-Gutachten**
Einhaltung datenschutzrechtlicher
Anforderungen durch das
Produkt „PrimeSharing Team Drive 2.1“
(vormals PrimeSharing TeamDrive)
der
TeamDrive Systems GmbH
Hamburg

erstellt von:

Andreas Bethke

Dipl. Inf. (FH)

Beim Unabhängigen Landeszentrum für Da-
tenschutz Schleswig-Holstein anerkannter
Sachverständiger für IT-Produkte (tech-
nisch)

Papenbergallee 34
25548 Kellinghusen
tel 04822 – 37 89 05
fax 04822 – 37 89 04
mob 0179 – 321 97 88
email ab@datenschutzkontor.de

Stephan Hansen-Oest

Rechtsanwalt

Beim Unabhängigen Landeszentrum für Da-
tenschutz Schleswig-Holstein anerkannter
Sachverständiger für IT-Produkte (rechtlich)

Neustadt 56
24939 Flensburg
tel 0461 – 90 91 356
fax 0461 – 90 91 357
mob 0176 – 23 22 71 76
email sh@datenschutzkontor.de

Stand:
März 2009

Inhaltsverzeichnis

A. Einleitung.....	4
B. Zeitpunkt der Prüfung.....	4
C. Änderungen und Neuerungen des Produktes.....	4
I. Das Verhalten der lokalen Client Anwendung.....	4
II. Eindeutige Benutzernamen.....	4
III. Kosmetische Änderungen.....	5
IV. Cross Plattform Kompatibilität.	5
V. Aufteilung in kostenfreie Clients mit Werbung und kostenpflichtige Professional-Variante ohne Werbung.	5
D. Datenschutzrechtliche Bewertung.....	7
E. Zusammenfassung.....	7

Änderungs- und Versionsverwaltung des Gutachtens

Datum	Beschreibung	Kommentar
27.01.2009	Erstellung	
06.03.2009	Fertigstellung	

A. Einleitung

- 1 Mit dem vorliegenden Gutachten beabsichtigt die TeamDrive Systems GmbH (nachfolgend TDS genannt) ihr Produkt „TeamDrive“ (ehemals „PrimeSharing TeamDrive“) für das Gütesiegel für IT-Produkte des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) rezertifizieren zu lassen.

Die Vorlage des Gutachtens beim ULD erfolgt durch den Auftraggeber.

Dem Gutachten wird der Anforderungskatalog in der Version 2.0 zu Grunde gelegt.

- 2 TDS möchte mit diesem Gutachten den Nachweis führen, dass das Produkt mit den Änderungen und Neuerungen, die seit der Erteilung des Gütesiegels vom 14.03.2005 und der Rezertifizierung vom 14.03.2007 gemacht worden sind, nach wie vor die datenschutzrechtlichen Anforderungen erfüllt.

B. Zeitpunkt der Prüfung

- 3 Die Prüfung des Produktes fand vom 20.01. - 06.03.2009 statt.

C. Änderungen und Neuerungen des Produktes

- 4 Identisch zur Version 1.4 sind alle Prozesse der Schlüssel Generierung, des Schlüssel Austausches und der Server Kommunikation verändert wurden. Die Mac und die Linux Version sind kein Bestandteil des Gütesiegels.

7 I. Das Verhalten der lokalen Client Anwendung

In der neuen Version werden definierte Ordner im lokalen Filesystem überwacht und Änderungen in eine lokale Datenbank übertragen, die dann mit den anderen Clients synchronisiert wird. Die Synchronisation erfolgt wie gehabt. Es liegt immer die aktuelle Version eines Dokumentes im File System des Clients, alles Andere liegt in der lokalen Datenbank und dem lokalen Archiv. Die archivierten Dokumente sind verschlüsselt und auch sämtliche Passworte in der Datenbank sind ebenfalls verschlüsselt.

- 8 In der alten Version 1.4 wurde ein virtuelles Netzlaufwerk im Filesystem gemountet - in der neuen Version werden jetzt die Ordner im Filesystem überwacht. Für den Anwender hat das den großen Vorteil, dass er jederzeit auf seine aktuellen Dokumente zugreifen kann, selbst wenn TeamDrive nicht gestartet wurde.

9 II. Eindeutige Benutzernamen

Alle bisherigen Verschlüsselungs- und Übertragungsverfahren der alten TeamDrive Version wurden übernommen. Nur als Identifizierungskennzeichen wurde jetzt einen eindeutigen Benutzernamen hinzugefügt, damit die EMail-Adresse eines Anwenders verborgen bleiben kann und gegebenenfalls mit einer neuen Authentifizierung geändert werden kann. Jeder User gibt sich in Version 2.1 einen eindeutigen Benutzernamen.

In Version 1.4 wurden die Benutzer nur anhand der EMail-Adresse identifiziert. In Version 2.1 geschieht dies nun anhand des frei wählbaren Benutzernamens.

Auf dem „Reg Server“ des Herstellers wird zu jedem Benutzernamen eine authentifizierte EMail-Adresse gespeichert. Diese kann von dem Benutzer später mit neuer Authentifizierung geändert werden. Der Anwender kann bei der Registrierung entscheiden, ob seine EMail-Adresse anderen Anwendern offengelegt wird oder nicht. Es gibt in keinem Fall ein zentrales Directory welches neugierige Benutzer einsehen können. Anwender werden immer persönlich eingeladen, entweder über einen bekannten Benutzernamen oder über eine beliebige EMail-Adresse. Jeder eingeladene Benutzer erhält die Einladung per EMail. Im Falle das ein Benutzernamen eingeladen wurde oder falls zu einer EMail-Adresse ein Benutzer registriert ist so erhält der eingeladene Benutzer in seinen TeamDrive Clients ebenfalls die Einladung zum Space beitriff. Jede EMail-Adresse kann nur für einen Benutzernamen zur Authentifizierung verwendet werden.

Benutzerdaten wie Name, Telefonnummer, etc. werden nur lokal und innerhalb der jeweiligen Spaces gespeichert und ausgetauscht. Diese Daten sind unter ausschließlicher Kontrolle eines jeden Benutzers und sind nur in den jeweiligen Spaces sichtbar.

Die Mindestpasswortlänge der Anwender wurde auf 8 Stellen gesetzt.

III. Kosmetische Änderungen

- 10 Die Anwendung wurde schlanker, leichter und schneller gemacht.

IV. Cross Plattform Kompatibilität.

- 11 Der neue Client Code wird in identischer Weise mit nur geringen Anpassungen an die jeweils anderen Betriebssysteme für Windows XP, Vista, MacOS 10.5 und Linux zur Verfügung stehen. Gegenstand der Zertifizierung ist jedoch nur die Version für das Windows-Betriebssystem.

V. Aufteilung in kostenfreie Clients mit Werbung und kostenpflichtige Professional-Variante ohne Werbung.

- 12 Es gibt nur eine Version von TeamDrive die durch die Eingabe eines Lizenzschlüssels erweiterbar ist.
- 13 Es gibt eine kostenfreie Version die keinen Lizenzschlüssel erfordert. Diese Version arbeitet standardmäßig mit dem von TeamDrive gehosteten Serverangebot über eine TeamDrive interne abgesicherte HTTP Verbindung oder alternativ mit beliebigen WebDAV Servern, die von den Kunden schon heute genutzt werden. Diese Kunden, die heute unverschlüsselte Daten auf z.B. GMX im Media Center speichern, bekommen durch TeamDrive die zusätzliche Sicherheit durch eine automatische Verschlüsselung aller Daten, die auf dem externen Server abgelegt werden. Möchten diese Kunden den sicheren Backup- und Relay-Service nutzen, so stehen ihnen 100 MB kostenlos zur Verfügung. Dieser Service kann jederzeit erweitert werden.
- 14 In dieser kostenfreien Version wurden Werbebanner eingeführt, die an drei Stellen eingeblendet werden können. Hierfür gibt es einen separaten unabhängigen Werbeserver der die Clients mit Werbung versorgt. Ohne Kontakt zu dem Regserver oder irgendwelchen Hosting Services holen sich dort die TeamDrive Clients 1x am Tag Werbung ab und melden anonymisierte Laufzeit und Einblendedaten. Even-

tuelle Banner-Clicks gelangen über den TeamDrive Proxy Server auf die entsprechenden Webseiten der Werbepartner. Durch die Eingabe eines Lizenzschlüssels lässt sich die Banner-Einblendung abschalten.

TeamDrive speichert keine IP Adressen und verhindert durch einen eigenen Proxy Server eine Weitergabe an Dritte. TeamDrive betreibt einen eigenen Werbe-Proxy Server. Jeder kostenfreie Client kontaktiert diesen Server 1 mal täglich. Anhand von Echtzeit-IP-Adressen Analyse und des übermittelten Distributionsschlüssels lädt sich der Client bei diesem Zugriff die relevanten Banneranzeigen herunter. Es werden keine IP Adressen gespeichert, sondern nur die Anzahl der Zugriffe aus den verschiedenen Regionen erfasst. Mit dem einmaligen Zugriff pro Tag liefert der Client eine kurz Statistik mit der Zeit die die Banner im TeamDrive Explorer sichtbar waren. Auch diese Information wird ausschließlich anonymisiert ohne Client Bezug gespeichert. Klickt ein User auf einen Banner, so wird der Click über den TeamDrive Proxy Server weitergeleitet. Somit wird verhindert, dass eine Client IP-Adresse an den Zielrechner weitergeleitet wird.

- 15** Auf dem Werbe-Proxy Server wird folgende Statistik gespeichert:
- Anzahl von Clients die Werbung anzeigen (Separiert nach Land, Distributor)
 - Angezeigte Werbebanner (Anzahl Clients, Anzahl Einblendungen, Dauer der Einblendungen)
 - Ausgeführte Clicks (Ziel URL mit Anzahl der Clicks)
- 16** Auf die Funktionsweise der Bannereinbindung wird im Rahmen der EULA eingegangen. Diese Darstellung wird laut Zusage des Herstellers bis zum 13.03.2009 noch erweitert und dem Nutzer an prägnanter Stelle angezeigt.
- 17** FTP Server werden von der Version 2.1 nicht unterstützt.
- 18** Weiterhin ist in der Version 2.1 eine kostenpflichtige HTTPS Unterstützung verfügbar. Sollte der Anwender die kostenfreie Version mit einem WebDAV Server über HTTP ohne "S" verwenden so werden nur seine Server Zugangsdaten unverschlüsselt übertragen (Username und Passwort). Der Hersteller hat hier einen entsprechenden Hinweis in der Dokumentation eingeführt, die diesen Punkt deutlich hervorhebt. TeamDrive versendet diese Zugangsdaten bei der Einladung eines anderen Benutzers in verschlüsselter Form und speichert diese auch nur verschlüsselt auf allen eingeladenen Clientrechnern ab. Sollte ein kundiger Anwender allerdings das HTTP Protokoll analysieren so kann er dabei die Zugangsdaten aus spähen. Das betrifft aber nur eigene Server des Kunden und in keinem Fall eine Komponente des TeamDrive Netzwerkes.
Die Dateien selbst werden nur verschlüsselt übertragen und gespeichert.
- 19** In beiden Versionen, der kostenlosen und der kostenpflichtigen Version finden alle Übertragungen als Voreinstellung (per Default) sicher und verschlüsselt statt. In jedem TeamDrive Client ist die TeamDrive interne abgesicherte HTTP Verbindung voreingestellt. Anwender haben dann unter dem Menü "Einstellungen" die Möglichkeit eigene Relay- und Backup Server hinzuzufügen. In der kostenfreien Variante können an dieser Stelle nur HTTP Verbindungen über Port 80 eingegeben werden. Erst nach Erwerb und Eingabe eines Lizenzschlüssels kann eine HTTPS basierende Servereinstellung vorgenommen werden. Das betrifft aber nur diejenigen Anwender die neue SharedSpaces auf einem eigenen Server einrichten möchten.

- 20 Jeder TeamDrive Client beherrscht das HTTPS Protokoll und kann deswegen in jedem Fall mit sicheren Servern kommunizieren und Einladungen in Shared-Spaces annehmen. Ausschließlich das Anlegen eigener sicherer Server für TeamDrive ist der kommerziellen Version vorbehalten.
- 21 Die professionelle Version ist werbefrei und beinhaltet die HTTPS Unterstützung von WebDAV. Darüber hinaus beinhaltet sie höhere Service Level im Support, z.B. Telefonsupport.

D. Datenschutzrechtliche Bewertung

- 22 Sowohl die kosmetischen Änderungen, als auch die Cross Plattform Kompatibilität haben keinen Einfluss auf die datenschutzrechtlichen Aspekte.
- 23 Die Änderungen zum Verhalten der des Clients hinsichtlich der Einführung einer lokalen Datenbank ist positiv zu bewerten, da hierdurch der schnellere Zugriff auf seine aktuellen Dokumente gewährleistet ist.
- 24 Die Änderung, die aus datenschutzrechtlicher Sicht am meisten Beachtung findet ist die Vergabe und freie Wahl von Benutzernamen, statt einer Identifizierung via EMail-Adresse. Hierdurch ist ein anonymes Arbeiten möglich.
- 25 Die Aufteilung in eine Werbebanner-abhängige Variante und eine kostenpflichtige Variante birgt evtl. Risiken, die durch Maßnahmen vom Hersteller unterbunden sind. Aus den EULA ergibt sich, dass sich der Hersteller vorbehält die Unterstützung der (kostenlosen) Software und die Dienste jederzeit zu beenden. Für den Einsatz in der öffentlichen Verwaltung bedeutet dies eine Einschränkung in der Verfügbarkeit. Somit kann der Einsatz der kostenlosen Variante in einer öffentlichen Verwaltung nur zu Testzwecken erfolgen und empfohlen werden.

E. Zusammenfassung

- 26 Zusammenfassend kann dem Produkt TeamDrive in der Version 2.1 nach wie vor eine adäquate Umsetzung der Belange des Datenschutzes bescheinigt werden. Das mitgelieferte Handbuch enthält viele praktische Hinweise im Bezug auf Datenschutz und Datensicherheit.

Hiermit bestätige ich, dass das oben genannte IT-Produkt den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht.

Kellinghusen, den _____

Flensburg, den _____

Andreas Bethke
Dipl. Inf. (FH)
Beim Unabhängigen Landeszentrum für
Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für
IT-Produkte (technisch)

Stephan Hansen-Oest
Rechtsanwalt
Beim Unabhängigen Landeszentrum für
Datenschutz Schleswig-Holstein
anerkannter Sachverständiger für
IT-Produkte (rechtlich)