Kurzgutachten zur Erteilung eines Gütesiegels gemäß Datenschutzauditverordnung Schleswig-Holstein für das IT-Produkt „BackStor, Version 1.1“

im Auftrag der Sachsen DV Betriebs- und Servicegesellschaft mbH

datenschutz cert GmbH

12. Februar 2013

datenschutz cert

Inhaltsverzeichnis

1. Über die Auditierung von BackStor, Version 1.1

Mit diesem Kurzgutachten werden die Ergebnisse der datenschutzrechtlichen und IT-sicherheitstechnischen Auditierung von „BackStor“, Version 1.1, dokumentiert, mit welcher die datenschutz cert GmbH seitens der Sachsen DV Betriebs- und Servicegesellschaft mbH beauftragt wurde.

Die Prüfung wurde anhand des Standards des Datenschutz-Gütesiegels gemäß der Schleswig-Holsteinischen Landesverordnung über ein Datenschutzaudit (DSAVO)[1] durchgeführt. Grundlage für die Erstellung dieses Kurzgutachtens ist die Version 1.2 des Anforderungskatalogs für ein Datenschutz-Gütesiegel des ULD.

Im Ergebnis stellen die Auditoren fest, dass BackStor, Version 1.1, konform zu den gesetzlichen Anforderungen an den Datenschutz und die Datensicherheit eingesetzt werden kann und in besonderem Maße den Datenschutz beim Anwender fördert.

2. Antragstellerin

Antragstellerin dieses Gutachtens ist die

Sachsen DV Betriebs- und Servicegesellschaft mbH
Täubchenweg 26
04317 Leipzig

Gesamtverantwortlicher Projektleiter für BackStor ist Herr Peter.

3. Sachverständiger/Prüfstelle

Sachverständige dieses Gutachtens ist die Prüfstelle

datenschutz cert GmbH
Konsul-Smidt-Str. 88a
28217 Bremen

unter der Leitung von Herrn Dr. Sönke Maseberg (Technik) und Frau Irene Karper (Recht). Ansprechpartner für diese Begutachtung sind Frau Dr. Irene Karper (Recht) und Herr Ralf von Rahden (Technik).

4. Zeitraum der Prüfung und Prüfverfahren

Die Begutachtung erstreckte sich auf den Zeitraum von 06.07.2011 bis 04.01.2013 und beinhaltete eine konzeptionelle Analyse der zur Verfügung gestellten Unterlagen sowie die Durchführung von Plausibilitätstests anhand eines Testzugangs.

5. Kurzbezeichnung des IT-Produkts

Begutachtet wird das IT-Produkt „BackStor“, Version 1.1 („BackStor“).

6. Tools, die zur Herstellung des Produkts verwendet wurden

BackStor basiert auf der Software „Asigra Cloud Backup“, Version 11 der Asigra Inc. Die Version 11 wird durch jeweilige Patches auf aktuellem Stand gehalten, zum Auditzeitpunkt bei Version 11.2. Die Sachsen DV ist seitens der Asigra Inc. lizenziert.

---

[1] Landesverordnung über ein Datenschutzaudit (Datenschutzauditverordnung - DSAVO) v. 18.11.2009, *GVOBl.* Schl.-H. *2008, S. 562ff. / GVOBl.* Schl.-H. *2009, S. 742ff.*

7. Beschreibung des IT-Produkts

BackStor ist eine Remote-Backup-Lösung für die Sicherung, Archivierung oder Wiederherstellung von Daten für Unternehmen oder öffentliche Stellen (Anwender). Es basiert auf der Software „Asigra Cloud Backup“ und wird insbesondere von Stellen eingesetzt, die ein hohes IT-Sicherheitsniveau gewährleisten (z.B. Banken, Krankenhäuser, Behörden).

BackStor wird im Rechenzentrum der Sachsen DV in Leipzig gehostet. Zudem wartet die Sachsen DV Systemkomponenten und unterstützt den Anwender bei der Installation im Sinne einer „Software as a Service“ (SaaS). BackStor wird als Gesamtkonzept der Asigra Cloud Backup-Lizenzierung in Verbindung mit dem SaaS der Sachsen DV am Standort Leipzig angeboten.

Die Datensicherung erfolgt online über eine Internet-Verbindung im Hintergrund, so dass der laufende Geschäftsbetrieb beim Anwender nicht beeinträchtigt wird. Der Anwender bestimmt, welche Teile seiner Daten verfügbar sein bzw. gesichert werden müssen und legt die Sicherungszyklen und Aufbewahrungsfristen individuell fest.

Zur Wahrung der Vertraulichkeit werden alle Daten verschlüsselt übertragen und verschlüsselt im Rechenzentrum der Sachsen DV gespeichert. Dem Anwender obliegt dabei die Hoheit über den Schlüssel, so dass ein Zugriff auf Daten ohne sein Mitwirken nicht möglich ist.

7.1 Komponenten

Zu BackStor gehören folgende, auf Asigra Cloud Backup basierende Komponenten:

- DS-System (Hauptkomponente im Rechenzentrum der Sachsen DV)
- DS-System Replication (optional Replizierung der Daten in einem weiteren Rechenzentrum der Sachsen DV in Leipzig zur Erhöhung der Verfügbarkeit)
- DS Client (Komponente beim Anwender)
- Backup Lifecycle Management – BML (optional zur Langzeitarchivierung)
- DS-Billing (Abrechnungssystem)
- DS-NOC - Network Operation Control (Monitoring und Administration)
- DS-Licence (Hilfsprogramm zum Lizenzmanagement).

In der folgenden Abbildung wird die technische Infrastruktur bezogen auf die Komponenten verdeutlicht:

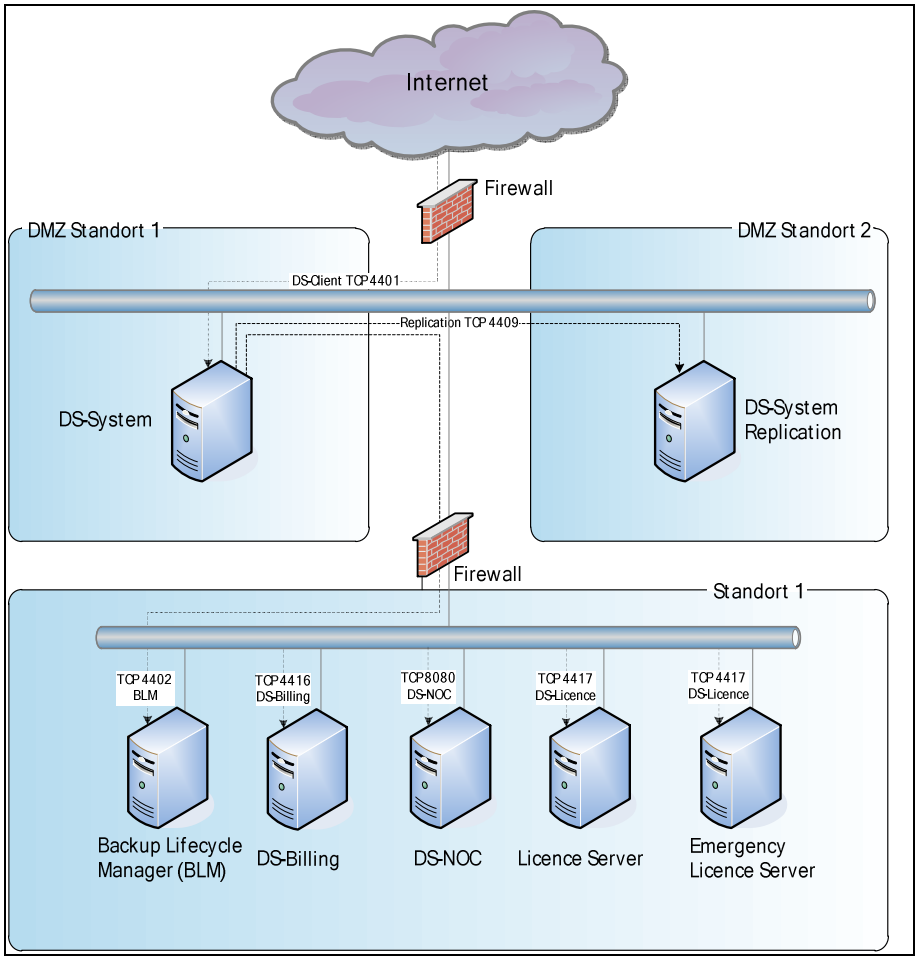

Abbildung1: Infrastruktur und Komponenten

DS-System

Im DS-System wird für den Anwender ein Account eingerichtet. Zur Identifikation werden eine Accountnummer und DS-Client-IDs erzeugt und zusammen mit den IP-Adressen der DS-Clients hinterlegt, um bei jeder Kommunikation die Authentizität des anfragenden DS-Clients überprüfen zu können.

In einer Client-Bibliothek liegen die Daten eines DS-Clients, verschlüsselt mit einem individuellen (privaten) Client-Schlüssel. Der DS-Client sendet für jede Datei die Dateigröße und einen eindeutigen Hash-Wert mit, der vor der Verschlüsselung erzeugt wurde. Erkennt das DS-System anhand dieser beiden Werte, dass es dieselbe Datei von mindestens drei Clients erhält, so erfragt das DS-System von dem letzten Client, der die Sicherung angestoßen hat, die jeweilige Datei erneut zu senden, allerdings nun verschlüsselt mit dem Account-Schlüssel. Die mit dem Account-Schlüssel verschlüsselte Datei wird in der Account Bibliothek gespeichert. Die identischen Kopien der anderen Clients werden auf diese Datei verlinkt und gelöscht.

Sollte dieselbe Datei von verschiedenen Anwendern gesichert werden (z.B. Betriebssystem-Dateien), erkennt das DS-System dies auf dieselbe Weise. Es kann dann davon ausgegangen werden, dass es sich nicht um eine vertrauliche Datei

handelt, da sie sonst nicht identisch auf drei oder mehr unterschiedlichen Anwendersystemen vorliegen würde. Daher erfragt das DS-System diese Datei unverschlüsselt, um sie in der öffentlichen Bibliothek zu sichern und entsprechend die übrigen Kopien auf diese zu verlinken und zu löschen. Um die Wahrscheinlichkeit von zufälligen Hashwert-Kollisionen, und in Folge dessen fälschlicher Speicherung in der öffentlichen Bibliothek, zu verhindern, muss der Anwender Backup-Sets anlegen, zum einen für unsensible Daten wie die des Betriebssystems und für sensible Daten. Für Letztere ist die Funktion „Common File Elimination" vom Anwender zu deaktivieren. Auf diese Weise können nur die als unsensibel eingestuften Daten in der öffentlichen Bibliothek gespeichert werden. Der Anwender wird zudem in § 4 Abs. 2 der „*Vereinbarung zum Datenschutz und der Datensicherheit in Auftragsverhältnissen nach § 11 BDSG*" auf diesen Umstand hingewiesen und vertraglich aufgefordert, das System entsprechend zu konfigurieren.

Über die GUI „DS Operator" ist es möglich, nach gesicherten Dokumenten zu suchen und diese zu löschen. Bei der Löschung eines Backups durch den Anwender besteht keine Möglichkeit zum Restore. Die Daten verbleiben aber bis zur nächsten Ausführung von „clean libraries" im Speicher.

DS-System Replication

Für eine redundante Datenhaltung kann das „DS-System Replication" verwendet werden, das eine kontinuierliche Replikation der Datenbestände des DS-Systems auf einen weiteren Datenspeicher vornimmt. Um eine Hochverfügbarkeit zu erreichen, kann das DS-System darüber hinaus als N+1-Konfiguration (mehrere parallel arbeitende DS-Systeme) aufgesetzt werden. Die Nutzung ist optional und kann vom Anwender zusätzlich beauftragt werden.

DS-Client

Der DS-Client wird beim Anwender installiert und sammelt die zu sichernden Daten im Hintergrund ein, ohne dass hierfür weitere Software installiert werden muss. Für mobile Endgeräte gibt es spezielle Mobile- bzw. Consumer-Clients.

Für bereits gesicherte Dokumente werden Änderungen gespeichert, im Sinne eines inkrementellen Backups. Anschließend erstellt der DS-Client per Hashwert eine Signatur und komprimiert und verschlüsselt jede Datei. Über die Signatur sind verschlüsselte Dateien im Backup-System identifizierbar. Der individuelle (private) Schlüssel, sowie ein Account-Schlüssel bei der Nutzung mehrerer DS-Clients werden bei der Installation des DS-Client erzeugt und hierbei verschlüsselt und hardcodiert in der Anwendung gespeichert. Sie liegen unter alleiniger Kontrolle des Anwenders.

Als Algorithmen stehen DES (56 bit) oder AES (128,192 oder 256 bit) zur Verfügung. Im Dokument „*Enterprise/Service Provider Product Overview and Implementation Guide*" wird der Anwender deutlich darauf hingewiesen, dass DES relativ langsam und unsicher sei, und die Verwendung von AES dringend empfohlen. Diese Empfehlung wird zudem nochmals im Dokument „*Hinweise zum Datenschutz bei BackStor*" aufgenommen.

Der Anwender ist für die Sicherung der Schlüssel verantwortlich. Die Möglichkeit, die Schlüssel zur Sachsen DV zu übertragen, ist durch eine systemweite Einstellung

unterbunden. Somit ist ein unbefugter Zugriff auf die gesicherten Anwenderdaten ausgeschlossen. Im Falle des Verlustes des Schlüssels kann allerdings auch nicht mehr auf den gespeicherten Datenbestand zugegriffen werden. Im Dokument „*Hinweise zum Datenschutz bei BackStor*“ wird der Anwender auf diese Aspekte hingewiesen.

Der DS-Client verbindet sich mit dem DS-System zur Übertragung der zu sichernden Daten. Diese werden zuvor vom DS-Client verschlüsselt. Die Verbindung wird stets vom DS-Client aufgebaut, so dass das DS-System sich nicht selbstständig mit den von ihm verwalteten DS-Clients verbinden kann, und ebenfalls mit einem zufälligen 256 bit-Schlüssel verschlüsselt. Der DS-Client wird bei jeder Verbindung zunächst anhand seiner Accountnummer, DS-Client-ID und optional zusätzlich mit seiner IP-Adresse authentifiziert.

Backup Lifecycle Management - BLM

Dateien können auch in ein Langzeitspeichersystem (Backup Lifecycle Management, sog. BLM-Archiver) verschoben oder dort mit der GUI gesucht oder gelöscht werden. Dieser Dienst ist vom Anwender ebenfalls optional buchbar.

DS-Billing

Das DS-Billing-System importiert und verarbeitet statistische Daten zu Abrechnungszwecken und stellt eine GUI für die Administration bestimmter Systemaktivitäts- und Verwaltungs-Tools, insbesondere ein Audit Trail, zur Verfügung.

DS-NOC und DS-Licence

DS-NOC (Network Operation Control) ist eine J2EE-Anwendung (Java), mit der Diensteanbieter, Verkaufsgruppen oder Endbenutzer auf DS-Systeme, BLM-Archiver, DS-License-Server und DS-Billing-Systeme SSL-verschlüsselt zugreifen und diese verwalten (z.B. Benutzer-Clients anlegen) oder Logs überwachen (Protokollauswertungen).

DS-Licence ist ein Hilfeprogramm zur Lizenzsteuerung der Software Asigra Cloud Backup.

Logging-Funktionen und Protokolle

In den Komponenten werden zudem Protokolle erzeugt, z.B. über vorgenommenen Änderungen (wer, wann, was geändert wurde), und zur Revisionskontrolle vorgehalten. Über Aktivitäts- und Ereignisprotokolle können Verbindungen, Aktivitäten oder Fehlermeldungen überprüft werden.

Diese Protokolle werden - je nach Aufzeichnungszweck - entweder sofort gelöscht oder 2, 4 oder 6 Monate aufbewahrt. Der Anbieter hat hierzu eine detaillierte Übersicht vorgelegt. Jedes Protokoll, das von der DS-System-Datenbank gelöscht wird, wird automatisch in eine Textdatei gesichert. Mit Ausnahme des Benutzernamens werden keine personenbezogenen Daten gespeichert. Es werden zwar z.T. IP-Adressen geloggt, diese sind aber nur bestimmten Systemen bzw. Clients zugeordnet und nicht einzelnen natürlichen Personen im Sinne des § 3 BDSG.

Auf dem DS-Client werden ebenfalls Protokolle erstellt, deren Speicherdauer allerdings vom Kunden selbst einzustellen ist.

8. Modellierung des Datenflusses

Der Datenfluss wird in der nachfolgenden Abbildung verdeutlicht:

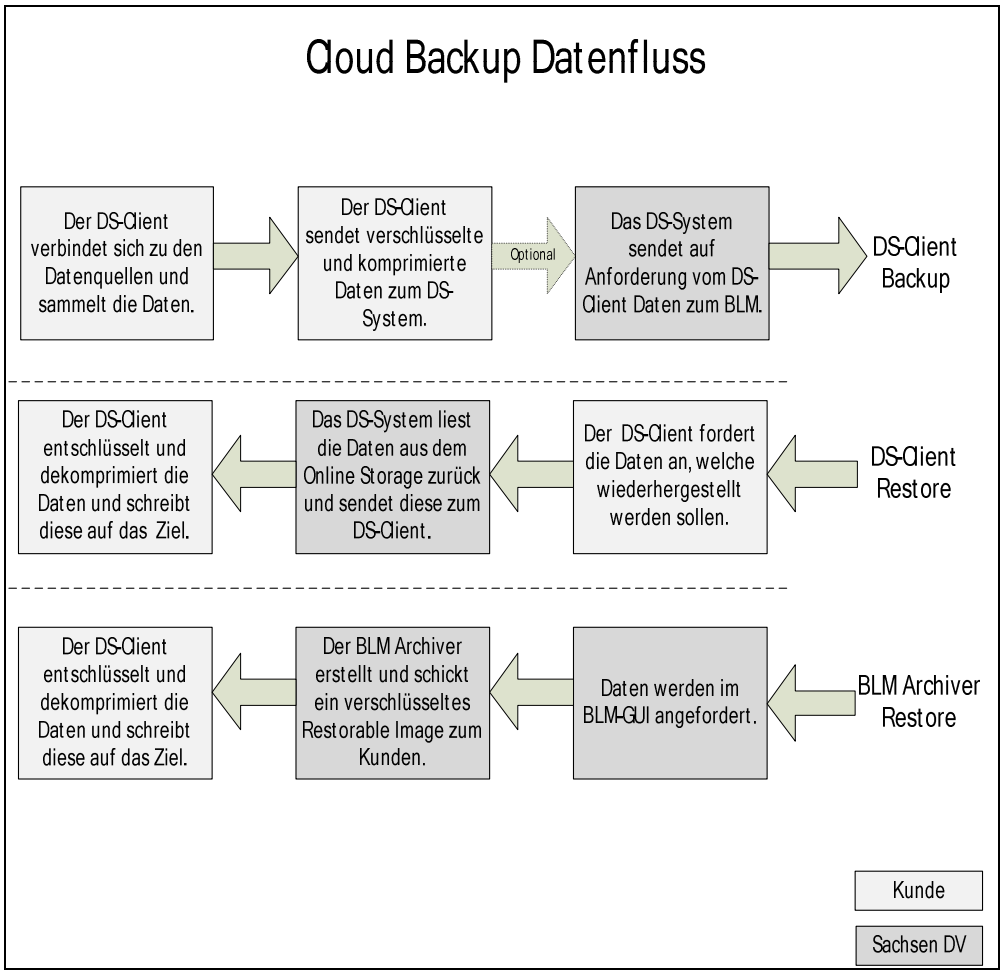

Abbildung 2 Datenfluss

Die Daten liegen auch im BLM Archiver nur verschlüsselt vor. Ein Restorable Image wird ohne Kenntnis des Klartextes erstellt und dem Anwender übergeben. Der Anwender kann dieses Image unter Verwendung seines DS-Client lesbar machen.

Zusammengefasst werden folgende Datenarten mittels BackStor verarbeitet:

Primärdaten:

Dies sind alle Daten, die an BackStor übertragen werden. Welche Daten übertragen werden, hängt vom jeweiligen EDV-System des Anwenders ab; diese können personenbezogen oder personenbeziehbar sein, müssen es aber nicht. Aufgrund der individuellen Anwendung können die Primärdaten nicht abschließend aufgeführt werden. Beispielhaft wird allerdings davon ausgegangen, dass es sich um Gesundheitsdaten handelt, die einen höchsten Schutz genießen.

Sekundärdaten:

Logdaten, wie sie bei der oben unter 7.3 beschriebenen Protokollierung anfallen.

9. Abgrenzung des Auditgegenstands

Diese Auditierung des IT-Produkts BackStor umfasst demnach Folgendes:

- Asigra Cloud Backup, Version 11 mit den Teilkomponenten:
  - DS-System + DS-System Replication
    - DS-Operator
  - DS Client
    - DS-Mobile-Client
    - DS-Consumer-Client
  - Backup Lifecycle Management (BLM)
  - DS-Billing
  - DS-NOC
  - DS-Licence
- Service und Betrieb durch die Sachsen DV in den Ausprägungen
  - Backup, Restore und Hosting im Rechenzentrum der Sachsen DV
  - Pflege und Wartung
  - Unterstützung bei der Installation
- Logging-Funktionen.

Nicht zum Auditgegenstand gehören hingegen

- die Einsatzumgebung beim Anwender
- Hardware und Betriebssystem im Rechenzentrum der Sachsen DV
- die Lizenzierung und Vertriebsprozesse seitens der Sachsen DV oder der Asigra Inc. oder deren sonstige Dienstleistungen oder Darstellungen
- die ggf. beauftragte Fernwartung durch die Sachsen DV.

10. Zusammenfassung der Prüfergebnisse

Folgende herausragende Prüfergebnisse konnten festgestellt werden:

10.1 Umsetzung von rechtlichen Anforderungen

Für die Auditierung sind u.a. die Vorgaben der Datenschutzauditverordnung Schleswig-Holstein (DSAVO), des Landesdatenschutzgesetzes Schleswig-Holstein (LDSG S-H)[2], der Datenschutzverordnung (DSVO)[3], das Bundesdatenschutzgesetz

[2] Landesdatenschutzgesetz - LDSG - Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen v. 27.01.2012, GVBl. Schl.-H. 1/2012, S. 78 ff. u. 89 ff.
[3] Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten v. 09. 1 2008 , GVOBl Schl.-H. 2008, S. 841ff.

(BDSG)[4] sowie als *lex specialis* die Regelungen des Telemediengesetzes (TMG)[5] einschlägig.

Da mittels BackStor Datenarten aus verschiedenen Bereichen (z.B. aus dem Gesundheits-, Banken- oder Behördenbereich) verarbeitet werden, können weitere spezialgesetzliche Datenschutzregelungen einschlägig sein. Um ein möglichst vergleichbares datenschutzrechtliches Schutzniveau annehmen zu können, wird seitens der Auditoren davon ausgegangen, dass mittels BackStor auch besondere personenbezogene Daten verarbeitet werden können. Gemäß § 3 Abs. 9 BDSG sind besondere Arten personenbezogener Daten alle Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Diese Daten unterliegen einem besonderen, höchsten datenschutzrechtlichen Schutz, der den Prüfmaßstab bildet.

Die Prüfung erfolgt am Beispiel einer Archivierung von Patientendaten. Etwa besteht eine Pflicht zur Aufbewahrung von Patientendaten gemäß § 10 der Musterberufsordnung (MBO)[6] bzw. gemäß der gleichlautenden Berufsordnung für Ärzte des Landes Schleswig-Holstein. Im Vordergrund steht dabei die Wahrung des Patientendatenschutzes. Er wird durch § 203 Strafgesetzbuch[7] und § 9 MBO dargelegt und geschützt. Ferner ist ein Beschlagnahmeschutz gemäß § 97 der Strafprozessordnung[8] zu gewähren.

10.1.1 Zulässigkeit der Datenverarbeitung

BackStor trägt diesen Anforderungen in vollem Umfang Rechnung. Die ärztliche Schweigepflicht und das Beschlagnahmeverbot werden insbesondere dadurch umgesetzt, dass Daten verschlüsselt gespeichert werden.

Die Speicherung einer Kopie der Schlüssel im DS-System würde es der Sachsen DV zwar *theoretisch* ermöglichen, auf einen gespeicherten Datenbestand zuzugreifen und dadurch Daten im Klartext einzusehen. Die Möglichkeit, die Schlüssel zur Sachsen DV zu übertragen, ist jedoch durch eine systemweite Einstellung unterbunden. Somit ist ein unbefugter Zugriff auf die gesicherten Anwenderdaten ausgeschlossen. Im Falle des Verlustes des Schlüssels kann dann allerdings auch nicht mehr auf den Datenbestand zugegriffen werden. Im Dokument „*Hinweise zum Datenschutz bei BackStor*“ sowie im Rahmen der Installation wird der Anwender auf diese Aspekte hingewiesen, so dass dieser angemessen sensibilisiert wird.

Im Rahmen des SaaS kann die Sachsen DV ferner die Adressliste der archivierten Daten einsehen, nicht aber dessen verschlüsselte Inhalte. Die Adressliste enthält die Datenmenge, die Versionsnummer sowie den Dateinamen. Je nach Konvention des Anwenders kann der Dateiname dabei ausnahmsweise Rückschlüsse auf

---

[4] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung v. 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes v. 14.08.2009 (BGBl. I S. 2814).
[5] Telemediengesetz v. 26.02.2007 (BGBl. I S. 179), zuletzt geändert durch Art. 1 des Gesetzes v. 31.05. (BGBl. I S. 692).
[6] MBO-Ä 1997 in der Fassung der Beschlüsse des 114. Deutschen Ärztetages 2011 in Kiel.
[7] Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 4 des Gesetzes v. 23.06. 2011 (BGBl. I S. 1266)
[8] Strafprozessordnung in der Fassung der Bekanntmachung v. 07.04.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 5 des Gesetzes v. 23.06.2011 (BGBl. I S. 1266).

personenbezogene Daten enthalten. Daher wird der Anwender im Dokument „*Hinweise zum Datenschutz bei BackStor*“ darauf hingewiesen, dass er im Falle des Supports durch die Sachsen DV die Einhaltung des Datenschutzes prüfen sollte und die zu archivierenden Dateien so benennt, dass ein Rückschluss auf natürliche Personen grundsätzlich ausgeschlossen werden kann. Der Anwender wird zudem in der „*Vereinbarung zum Datenschutz und der Datensicherheit in Auftragsverhältnissen nach § 11 BDSG*“ auf diesen Umstand hingewiesen und vertraglich verbindlich dazu aufgefordert, zu vermeiden, dass durch sprechende Dateinamen Rückschlüsse auf besondere oder sensible Personendaten möglich sind.

Die Verarbeitung der (Patienten-)Daten kann auf § 11 LDSG S-H bzw. § 28 Abs. BDSG gestützt werden. Die Verarbeitung von – hier angenommenen - Patientendaten durch BackStor kann auf dem jeweiligen Behandlungsverhältnis zwischen dem Arzt und dem Patienten beruhen und ist insofern vertraglich begründet. Ferner trägt die Archivierung von Patientendaten ggf. dazu bei, lebenswichtige Interessen zu wahren. Da die Zuordnungsfunktion verschlüsselt hinterlegt sind und die Sachsen DV keinen Zugang zum Schlüssel besitzt, bleibt der Anwender jederzeit Herr seiner verschlüsselten Daten.

Für die Zulässigkeit der Auftragsdatenverarbeitung ist zu gewährleisten, dass die ärztliche Schweigepflicht im Rahmen der Archivierung nicht durchbrochen wird. Aus der Zulässigkeit der Auftragsdatenverarbeitung ergibt sich nämlich nicht automatisch die Befugnis, medizinische Daten gegenüber dem Personal des Auftragsdatenverarbeiters zu offenbaren. Während Systemadministratoren, die Mitarbeiter eines Krankenhauses oder einer Arztpraxis sind, Erfüllungsgehilfen des Arztes darstellen, gilt dies nicht für externe Dienstleister. Folglich ist die Offenbarung von Patientendaten gegenüber eigenem EDV-Personal zulässig. Externen dürfen medizinische Daten jedoch grundsätzlich nicht offenbart werden.

Letzteres wird im Rahmen der Datenverarbeitung bei BackStor durch eine vollständige Verschlüsselung der archivierten Datensätze verhindert. Der Archivar (Sachsen DV) hat grundsätzlich keinerlei Zugangsmöglichkeit. In Einzelfällen kann es allerdings vorkommen, dass die Sachsen DV im Rahmen des Supports per Teamviewer bei einem Anwender auf dessen ausdrücklichen Wunsch bzw. mit dessen ausdrücklichen Einverständnis Einblick in vollständige bzw. de-pseudonymisierte Datensätze erhält. Die Offenbarung liegt dabei weiterhin in der Hand des jeweiligen Anwenders (bzw. Schweigepflichtigen). Die Sachsen DV hat für diesen Fall in dem Dokument „*Hinweise zum Datenschutz*“ das Verfahren mittels Teamviewer kurz beschrieben und weist darauf hin, dass hierbei Gesundheits- und Sozialdaten sowie generell besondere personenbezogene Daten nicht ohne Einwilligung des Betroffenen offenbart werden dürfen. Sowohl systemseitig als auch organisatorisch durch die Sensibilisierung des Anwenders in den Produktunterlagen ist damit eine unbefugte Offenbarung des Patientengeheimnisses weitestgehend ausgeschlossen.

Die „*Vereinbarung zum Datenschutz und der Datensicherheit in Auftragsverhältnissen nach § 11 BDSG*“ sowie die dazugehörige Anlage „Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG“ enthalten zudem alle in § 11 BDSG bzw. § 17 LDSG S-H geforderten Aspekte.

10.1.2 Cloud Computing

Für BackStor waren auch die „*Orientierungshilfe – Cloud Computing*“ der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[9] zu beachten. Im Audit wurde festgestellt, dass BackStor diese Anforderungen erfüllt. Alle Dokumente bieten offene, transparente und detaillierte Informationen über die technischen, organisatorischen und rechtlichen Rahmenbedingungen des SaaS einschließlich der Sicherheitskonzeption.

Da es sich bei BackStor um eine Private Cloud in einem den Vertragsparteien bekannten, abgegrenzten und räumlich definierten IT-System handelt, besitzen die Aspekte zum Ortswechsel, zur Portabilität und zur Interoperabilität im Sinne der Orientierungshilfe keine Relevanz.

Durch die schriftliche Regelung technisch-organisatorischer Sicherheitsmaßnahmen (z.B. § 3 des Mustervertrags zur Auftragsdatenverarbeitung) wird die Umsetzung von Sicherheitsmaßnahmen zwischen den Parteien definiert. Die Sachsen DV erfüllt die Anforderungen an aktuelle und aussagekräftige Nachweise über die IT-Infrastruktur, insbesondere durch ein zum Auditzeitpunkt gültiges Zertifikat „Trusted Site Infrastructure TSI V2.0 Level 3 (erweitert)“ der TÜV Informationstechnik GmbH.

10.1.3 Telemedienrechtliche Vorgaben

Auch die Webseiten zu dem IT-Produkt BackStor unter www.oxportal.net und http://www.sachsendv.de/Content/Projekte/BackStor/index.html (beide mit Stand von 02/2013) entsprechen den Anforderungen des TMG und weisen Impressum, Datenschutzerklärung sowie einen rechtskonformen Umgang mit Nutzerdaten auf.

10.2 Datensparsamkeit und Datenvermeidung

BackStor ermöglicht dem Anwender, nur Daten zu archivieren, die für ihn zwingend erforderlich sind. Die Archivierung mehrfach vorhandener Daten wird durch die Selektionsfunktion begrenzt. Die Verschlüsselung sorgt dafür, dass Dateien, die nicht als öffentlich eingestuft worden sind, vor unberechtigtem Zugriff geschützt sind. Der Anwender wird zudem im Dokument „*Hinweise zum Datenschutz bei BackStor*“ auf die Datenlöschung und den datensparsamen Umgang sensibilisiert.

10.3 Löschung, Anonymisierung, Pseudonymisierung

Aspekte der frühzeitigen Löschung, des Anonymisierens und Pseudonymisierens der Daten obliegen dem Anwender. BackStor unterstützt diese Aspekte mittelbar, indem der Anwender in den „*Hinweisen zum Datenschutz bei BackStor*“ auf entsprechende Maßnahmen hingewiesen wird. Löschprozesse werden zudem anhand des „BLM Archiver“ unterstützt, indem dieser eine Suchfunktion der archivierten und zu löschenden Dokumente ermöglicht.

10.4 Transparenz

Die von der Sachsen DV zur Verfügung gestellten Produktdokumentationen sind verständlich und aussagekräftig. Datenfluss, Zugriffsmöglichkeiten und die

[9] Z.B. abrufbar unter http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf (Stand 02/2013).

Verarbeitung von personenbezogenen Daten werden transparent dargelegt. Der Anwender wird ferner im Dokument „*Hinweise zum Datenschutz bei BackStor*“ auf den Datenschutz insgesamt hingewiesen und sensibilisiert.

10.5 Technisch-organisatorische Maßnahmen zum Datenschutz

In beiden Rechenzentren ist ein angemessener Zugangsschutz etabliert. Dies wird für das eine Rechenzentrum durch ein im Auditzeitpunkt gültiges Trusted-Site-Zertifikat (Level3) des TüV IT nachgewiesen. Für das andere Rechenzentrum ist auf hohem Niveau ein Zugangskontrollsystem etabliert (u.a. mit Alarmanlage, Wachdienst, Videoüberwachung und Zugangscodes.

Das Berechtigungskonzept sieht eine technische und administrative Rollenteilung vor, die einen missbräuchlicher Datenzugriff erheblich erschwert. Unterstützt wird dies durch eine revisionssichere Zugriffsprotokollierung.

Durch die Protokolldaten werden in Verbindung mit der Nutzerautorisierung die Nachprüfbarkeit von Verarbeitungsvorgängen und die Nichtabstreitbarkeit von Datenverarbeitungsschritten gewährleistet.

Die Integrität, Vertraulichkeit und Authentizität der Daten ist u.a. über die Identifizierung des DS-Client, der Verwendung eines SSL-Serverzertifikats, sowie über die Verschlüsselung angemessen gewährleistet.

Die Verfügbarkeit des Systems ist als besonders hoch zu bewerten. Für die Level 3 Trusted Site Zertifizierung ist der Hauptstandort über zwei getrennte Strom- und Datenleitungen angeschlossen und verfügt über eine leistungsfähige USV. Durch die (optionale) Nutzung des Replication System an zwei räumlich getrennten Standorten ist selbst bei einem Totalausfall der Betrieb gewährleistet.

10.6 Umsetzung von Betroffenenrechten

BackStor fördert die Rechte des Betroffenen, indem die dem Anwender ausgehändigten Dokumentationen die Datenverarbeitungsvorgänge und Verantwortlichkeiten in leicht verständlicher Form beschreiben und eine Vorabkontrolle oder die Erstellung des Verfahrensregisters erleichtern. Dadurch wird die Tätigkeit des Datenschutzbeauftragten bei Auskunftsersuchen oder Beschwerden unterstützt. Auch wird der Anwender auf den Datenschutz in BackStor sensibilisiert, insbesondere durch die „*Hinweise zum Datenschutz bei BackStor“.*

11. Gesamtbewertung

Für BackStor, Version 1.1 ergibt sich danach folgende Gesamtbewertung:

Nr.	Anforderungsprofil	Bewertung
Datenart A (Primärdaten):		
A1	Datensparsamkeit	angemessen
A2	Löschen, Anonymisieren, Pseudonymisieren	angemessen
A3	Transparenz	vorbildlich
A4	Sonstige Anforderungen	Nicht anwendbar

A5	Zulässigkeit	angemessen
A6	Datenschutzgrundsätze	angemessen
A7	Auftragsdatenverarbeitung	angemessen
A8	Besondere technischer Verfahren	Nicht anwendbar
A9	Sonstige Anforderungen	Nicht anwendbar
A10	Zugangskontrolle	vorbildlich
A11	Zutritts- und Zugriffskontrolle	angemessen
A12	Protokollierung	angemessen
A13	Weitere technisch-organisatorische Maßnahmen	vorbildlich
A14	Vorabkontrolle, Verfahrensverzeichnis, Datenschutzbeauftragter	vorbildlich
A15	Spezifische Pflichten	Nicht anwendbar
A16	Pflichten nach DSVO	angemessen
A17	Sonstige spezifische Anforderungen	Nicht anwendbar
A18	Betroffenenrechte	angemessen
A19	Sonstige Anforderungen	angemessen
Datenart B (Sekundärdaten):		
B1	Datensparsamkeit	angemessen
B2	Löschen, Anonymisieren, Pseudonymisieren	angemessen
B3	Transparenz	angemessen
B4	Sonstige Anforderungen	Nicht anwendbar
B5	Zulässigkeit	angemessen
B6	Datenschutzgrundsätze	angemessen
B7	Auftragsdatenverarbeitung	angemessen
B8	Besondere technischer Verfahren	Nicht anwendbar
B9	Sonstige Anforderungen	Nicht anwendbar
B10	Zugangskontrolle	vorbildlich
B11	Zutritts- und Zugriffskontrolle	angemessen
B12	Protokollierung	angemessen
B13	Weitere technisch-organisatorische Maßnahmen	angemessen
B14	Vorabkontrolle, Verfahrensverzeichnis, Datenschutzbeauftragter	vorbildlich

B15	Spezifische Pflichten	Nicht anwendbar
B16	Pflichten nach DSVO	angemessen
B17	Sonstige spezifische Anforderungen	Nicht anwendbar
B18	Betroffenenrechte	angemessen
B19	Sonstige Anforderungen	angemessen

12. Förderung des Datenschutzes

Das IT-Produkt BackStor, Version 1.1, fördert den Datenschutz auf vielfältige Weise, insbesondere durch:

--- die Transparenz der Datenverarbeitung

--- das Verschlüsselungskonzept

--- den Zutrittsschutz

--- eine hohe Verfügbarkeit der Daten.

13. Votum der Auditoren

Das IT-Produkt BackStor, Version 1.1, setzt insgesamt die Anforderungen an den Datenschutz angemessen um. Die Auditoren empfehlen die Gütesiegelvergabe.

Bremen, den 12. Februar 2013

Dr. Irene Karper LL.M.Eur.
datenschutz cert GmbH

Ralf von Rahden
datenschutz cert GmbH