SHARDSECURE

Gewährleisten Sie die Compliance für die DSGVO und Schrems II

Datenschutz für grenzüberschreitende Datenübertragungen

Nicole Beranek Zanon, Managing Partner, HÄRTING Attorneys-at-Law Ltd.
Hans-Peter Erlingsson, CEO, Lex Legem Advisory and Consulting
Jesper Tohmo, CTO and Co-Founder, ShardSecure

Einführung

Das Urteil des Gerichtshofs der Europäischen Union in der Rechtssache Schrems II erschwert Organisationen in der EU und im Europäischen Wirtschaftsraum (EWR) den Datentransfer zu globalen Cloud-Service-Providern erheblich. Dies gilt auch für Datenübermittlungen aus der Schweiz in Drittstaaten mit einem unzureichenden Datenschutzniveau. Dabei handelt es sich um Länder, die in der Liste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) aufgeführt sind.

Dieses Whitepaper zeigt, wie der patentierte Ansatz von ShardSecure für den Datenschutz Unternehmen dabei unterstützt, die spezifischen Anforderungen für grenzüberschreitende Datenübertragungen und für die DSGVO-konforme Verarbeitung personenbezogener Daten in Cloud-Services gemäß den Empfehlungen des Europäischen Datenschutzausschusses (European Data Protection Board, EDPB) zu erfüllen. Dieser Ansatz von ShardSecure deckt die Use Case 5-Anforderungen des EDPBs für gespeicherte Daten (Data-at-Rest) umfassend ab.

Das Schrems-II-Urteil und seine Auswirkungen auf die Cloud-Nutzung

Am 16. Juli 2020 erklärte der Gerichtshof der Europäischen Union („der Gerichtshof“) den Angemessenheitsbeschluss des EU-US Privacy Shield (EU-US-Datenschutzschild) in der Rechtssache C-311/18 –Data Protection Commissioner gegen Facebook Ireland Limited und Maximillian Schrems (genannt „Fall Schrems II“) – für ungültig. Der Gerichtshof äußerte auch Zweifel daran, inwieweit Datenübermittlungen aus der EU und dem EWR in die USA (sowie in andere Gerichtsbarkeiten mit Datenschutzgesetzen, die nicht dem EU-Niveau entsprechen) durch die Standardvertragsklauseln (Standard Contractual Clauses, SCCs) der Europäischen Kommission legitimiert werden können. Der Gerichtshof bestätigte die allgemeine Gültigkeit der SCCs als Transferinstrument, betonte jedoch, dass die SCCs durch technische oder organisatorische Sicherheitsmaßnahmen ergänzt werden müssen, wenn die Gesetze oder Praktiken des Drittlandes die Wirksamkeit dieser SCCs beeinträchtigen. Der Grund dafür ist, dass eine Vereinbarung zwischen den Parteien – wie die SCCs – keinen ausreichenden Schutz sowohl vor einer behördlichen Überprüfung auf Basis des Foreign Intelligence Act (FISA), Absatz 702, als auch vor einer Verletzung des Grundrechts auf freie Rechtsausübung auf Grundlage der Charta der Grundrechte der Europäischen Union für europäische Betroffene bieten kann.

Die Auswirkungen des Schrems-II-Urteils auf die Cloud-Nutzung waren bahnbrechend. Da der Gerichtshof die Angemessenheit des EU-US Privacy Shield (EU-US-Datenschutzschilds) aufgehoben hat, war die gesamte Rechtsgrundlage für den freien Datenverkehr mit den USA außer Kraft gesetzt. Darüber hinaus waren die SCCs und andere von der DSGVO genehmigte Transferinstrumente ohne die Umsetzung ergänzender Maßnahmen nicht immer rechtsgültig. Über Nacht befanden sich viele Unternehmen in der Schwebe und hatten damit zu kämpfen, die operative Effizienz und Informationssicherheit mit dem Datenschutz und der Einhaltung gesetzlicher Vorschriften in Einklang zu bringen.

Die Auswirkungen dieses Urteils für die Schweiz waren weniger gravierend. Grundsätzlich gilt, dass im Sinne des schweizerischen Bundesgesetzes über den Datenschutz (Swiss Federal Act on Data Protection, FADP) ein „angemessener“ und auch in Zukunft „geeigneter“ Schutz, der einem risikobasierten Ansatz entspricht, ausreichend ist. Gemäß Art. 6 Abs. 2 FADP erfordert die Weitergabe von Daten an unsichere Drittstaaten nur einen „angemessenen“ Schutz, nicht aber den Ausschluss jeglichen Risikos. Im Sinne dieses Ansatzes genügt nach dem Willen des Gesetzgebers ein Vertrag als Schutz, auch wenn Verträge bekanntlich nicht vor dem Zugriff ausländischer Behörden schützen. Ein Ausschluss jedes theoretischen Risikos ist demnach nicht erforderlich. Allerdings gilt es dabei zu beachten, dass das mit Cloud-Projekten verbundene Risiko in jedem konkreten Einzelfall zu prüfen ist.

Split- oder Multi-Party-Processing – eine vom EDPB empfohlene, ergänzende Maßnahme (Use Case 5)[1]

Am 18. Juni 2021 nahm der Europäische Datenschutzausschuss (European Data Protection Board, EDPB) Empfehlungen zu den Maßnahmen an, die die Transferinstrumente ergänzen, um die Einhaltung des Datenschutzes auf EU-Ebene zu gewährleisten.

Diese Empfehlungen, die in Form von allgemeinen Regeln und Anwendungsfällen (Use Cases) formuliert sind, verdeutlichten die Pflichten von Datenexporteuren bei internationalen Datenübermittlungen und erläuterten, welche Maßnahmen zur Ergänzung der Transferinstrumente, einschließlich der SCCs, ausreichen und welche nicht. Im Folgenden werden wir diese allgemeinen Regelungen für die Übermittlung untersuchen, damit deutlich wird, wie Microsharding die vom EDPB definierten Anforderungen des Use Case 5 abdecken kann.

Der Use Case 5 bezieht sich ausdrücklich auf „Split- oder Multi-Party-Processing“ als allgemein vertretbare Zusatzmaßnahme – es sei denn, einer der Verarbeiter benötigt Zugang zu den Daten im Klartext. Die Aufteilung von Informationen in kleinere Bestandteile vor der Übertragung sowie die Verteilung dieser Komponenten auf mehrere Auftragsverarbeiter, Standorte und Gerichtsbarkeiten auf eine Art und Weise, sodass kein Bestandteil der Daten von einem einzelnen Verarbeiter rekonstruiert werden kann, wird das Risiko, dass die Gesetze und Praktiken von Drittländern die Sicherheitsvorkehrungen der SCCs und anderer anerkannter Transferinstrumente beeinträchtigen, wirkungsvoll eliminieren.

Die allgemeinen Regeln des EDPBs sowie des EDÖBs für grenzüberschreitende Datenübermittlungen:

1. Abbildung der Übertragungen

Zunächst müssen die Unternehmen „über ihre Datenübertragungen Bescheid wissen“ und abbilden, wohin ihre Daten übermittelt werden. Die Aufteilung der Daten in einzelne Bestandteile im Microsharding-Prozess sowie deren Verteilung über mehrere Standorte hinweg mag für eine gründliche Zuordnung der Datenübertragungen anfänglich nicht eingängig erscheinen. Der Vorteil ist jedoch: Mithilfe des Microsharding-Prozesses können die Informationen nicht mit einer betroffenen Person in Verbindung gebracht werden.

2. Überprüfung des Transferinstruments

Ob das Transferinstrument für das Bestimmungsland geeignet ist, muss von Fall zu Fall geprüft werden.

3. Bewertung des Übertragungsziels

Die Leitlinien des EDPB empfehlen, die Gesetze und Praktiken im Zielland der Übermittlung zu bewerten, um sicherzustellen, dass diese die Rechte des Einzelnen nicht verletzen, insbesondere im Hinblick auf den Zugriff von Behörden auf personenbezogene Daten.

Unter Berücksichtigung der Anforderungen von Use Case 6 des EDPB – wonach es keine technischen Mechanismen gibt, um das mit einem Zugriff auf Daten im Klartext verbundene Risiko zu vermeiden – empfehlen wir, ein ausführliches Gespräch über den Umfang Ihrer Datenübertragungen und Ihre Szenarien zu führen, den Microsharding abdecken soll.

4. Identifizierung ergänzender Maßnahmen

In der Liste der Use Cases führt das EDPB Beispiele für ergänzende Maßnahmen auf, die im Rahmen von Schritt 4 zu berücksichtigen sind. Das EDPB betont, dass jede ergänzende Maßnahme nur dann als wirksam im Sinne des Schrems II-Urteils angesehen werden kann, wenn und soweit diese – allein oder in Kombination mit anderen – die spezifischen Mängel behebt, die Sie bei Ihrer Bewertung der für Ihre Übermittlung geltenden Gesetze und Praktiken des Drittlandes festgestellt haben.

---

[1] Use Case 5, S.33, Nr. 92, Absatz 1
(https://edpb.europa.eu/system/files/2021- 06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf)

Soweit das EDPB und der EDÖB empfehlen, gegebenenfalls ergänzende Maßnahmen zu identifizieren und zu ergreifen, um das Sicherheitsniveau für die übermittelten Daten auf den EU-Standard der wesentlichen Gleichwertigkeit anzuheben, können Microsharding sowie Split- oder Multi-Party-Processing die jeweilige Übermittlung und Verarbeitung sicherer gestalten.

5. Formale Verfahrensschritte

Das EDPB empfiehlt, alle formalen Verfahrensschritte umzusetzen, die der Erlass der ergänzenden Maßnahmen erfordern kann – je nach dem von Ihnen gewählten Transferinstrument gemäß Artikel 46 DSGVO. Diese Schritte können beispielsweise die Genehmigung von verbindlichen, internen Datenschutz-Richtlinien (Binding Corporate Rules, BCR) als Grundlage für die Übermittlung umfassen.

6. Neubewertung und Überwachung

Bewerten Sie in angemessenen Abständen das Sicherheitsniveau der personenbezogenen Daten, die Sie in Drittländer übermitteln, neu und überwachen Sie, ob es Entwicklungen gemäß Klausel 5 gegeben hat oder geben wird, die sich darauf auswirken könnten.

Adressieren Sie den Use Case 5 mit der Microshard™ Technology

Die Microshard-Technologie von ShardSecure ist eine Split-Processing-Technologie, die ohne Weiteres in einer Multi-Party-Processing-Umgebung genutzt werden kann. Mit dem Einsatz der Microshard-Technologie kann jede Organisation alle Arten von Daten überall verarbeiten und speichern und gleichzeitig die Bestimmungen der DSGVO und des Schrems-II-Urteils einhalten.

Im Folgenden erläutern wir, wie Sie Microsharding nutzen können, um die Anforderungen von Use Case 5 zu erfüllen.

Das Use Case 5-Szenario[2] – die Anforderungen

1

Sie erfüllen die Anforderungen des EDPBs, wenn Sie als Datenexporteur personenbezogene Daten so verarbeiten, dass diese in zwei oder mehr Bestandteile aufgeteilt werden, von denen jeder – ohne die Verwendung zusätzlicher Informationen – nicht mehr interpretiert oder einer bestimmten betroffenen Person zugeordnet werden kann.

Wie ShardSecure Sie dabei unterstützen kann

Microsharding wurde für den ausdrücklichen Zweck entwickelt, unbefugte Benutzer oder Organisationen daran zu hindern, die ursprünglichen Daten aus den Microsharded-Daten zu rekonstruieren oder zu identifizieren. Die Funktion von Microsharding besteht darin, Daten in sehr kleine Bestandteile (Microshards) zu zerlegen, diese Microshards in mehreren logischen Containern neu anzuordnen und zu mischen und diese Container an verschiedenen kundeneigenen Standorten zu speichern.

Nutzer können die Speicherorte und deren Anzahl und frei konfigurieren. Wir empfehlen mindestens vier Speicherorte. Theoretisch gibt es keine Obergrenze für die Anzahl der Speicherorte, die verwendet werden können, wir befürworten jedoch maximal zehn.

---

[2] Use Case 5, S.33, Nr. 92, Absatz 1 (https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf)

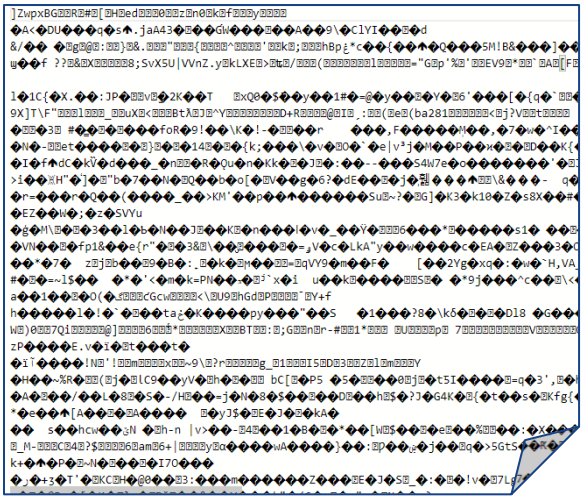


Abbildung 1: Beispiel eines Containers mit Microsharded-Daten

Für den unwahrscheinlichen Fall, dass ein Unbefugter Zugriff auf die Microsharded-Daten jedes Speicherorts (für einen bestimmten Datenbestand) erlangen kann, reichen diese Daten allein nicht aus, um die Microsharded-Daten zu rekonstruieren. Hierfür gibt es mehrere Gründe:

1. Der Microsharding-Prozess entfernt Dateinamen, Dateierweiterungen und alle anderen Daten oder Metadaten, die Aufschluss darüber geben könnten, wie die Microsharded-Daten rekonstruiert werden. Jedem Microshard-Container wird zudem ein zufälliger alphanumerischer Name zugewiesen. Daher ist es nicht möglich zu erkennen, welche Container von welchen Originaldaten abgeleitet wurden.

2. Die Originaldaten können in Microshards mit einer Größe von nur vier Bytes zerlegt werden, von denen jeder nur ein bis vier Zeichen enthalten würde (Shredding). Der Anwender kann die Größe der Microshards frei konfigurieren, sodass ein unbefugter Benutzer nicht wissen kann, wie viele Zeichen ein Bestandteil der Originaldaten umfasst.

3. Der Microsharding-Prozess kann auch Decoys oder Daten zur Täuschung verwenden, um die Wiederzusammensetzung der Daten für Unbefugte zusätzlich zu erschweren. Ob Decoy-Daten verwendet werden sollen und – wenn ja – in welchem Umfang, kann der Anwender ebenfalls konfigurieren.

4. Die ShardSecure-Lösung umfasst eine Policy-Engine, die Benutzer ebenfalls konfigurieren können. Sie können die Größe der Microshards, die Menge der Decoy-Daten (falls gewünscht), die Anzahl der zu verwendenden Container und vieles mehr anpassen.

Die ShardSecure-Lösung umfasst mehrere Komponenten, die im Zusammenspiel und zusammen mit dem gesamten Datenbestand genutzt werden müssen, um die Microshard-Daten wieder zusammenzusetzen. Diese zusätzlichen Komponenten werden nicht zusammen mit den Microsharded-Daten gespeichert.

2

Sie erfüllen die Anforderungen des EDPBs, wenn die einzelnen Bestandteile der Daten an separate Verarbeiter in verschiedenen Gerichtsbarkeiten übermittelt werden.

Wie ShardSecure Sie dabei unterstützen kann

Die Richtlinien der ShardSecure-Engine können so konfiguriert werden, dass die Microshard-Container in verschiedenen Gerichtsbarkeiten gespeichert werden. Diese Container können über die verschiedenen Regionen und Standorte eines einzelnen Cloud-Providers, über mehrere Cloud-Provider oder in einer hybriden Umgebung bestehend aus On-Premises-Speicher und einem oder mehreren Cloud-Providern verteilt werden. Damit ist sichergestellt, dass kein Speicherort alle Komponenten eines bestimmten Containers erhält.

3

Sie erfüllen die Anforderungen des EDPBs auch dann, wenn die Auftragsverarbeiter die Daten möglicherweise gemeinsam verarbeiten und hierbei beispielsweise Secure Multi-Party Computation zum Einsatz kommt. Dabei muss gewährleistet sein, dass keine der beteiligten Parteien Informationen erhält, die sie nicht schon vor der Verarbeitung besessen hat.

Wie ShardSecure Sie dabei unterstützen kann

Microsharding wurde entwickelt, damit der Eigentürmer der Daten die Kontrolle über diese behalten kann und die gespeicherten Daten (Data-at-Rest) umfassend geschützt sind. Das in diesem Dokument beschriebene Verfahren stellt sicher, dass der Datenzugriff durch unbefugte Nutzer unverständlich und für diese Nutzer wertlos ist. Handelt es sich – im Rahmen unserer Antworten – bei den Auftragsverarbeitern um Cloud-Provider, wird den Auftragsverarbeitern lediglich der Zugriff auf diejenigen Daten gewährt, die der Dateneigentümer ausdrücklich und auf die von ihm als angemessen erachtete Art und Weise gestattet.

4

Sie erfüllen die Anforderungen des EDPBs, wenn der für die gemeinsame Verarbeitung verwendete Algorithmus vor aktiven Angreifern sicher ist.

Wie ShardSecure Sie dabei unterstützen kann

Die Microsharding-Technologie verwendet keine mathematischen Berechnungen und kann daher nicht rückgängig gemacht oder dekodiert werden. Unser Quellcode ist ebenfalls durch Microsharding geschützt, um Supply-Chain-Attacken zu verhindern.

5

Darüber hinaus erfüllen Sie die Anforderungen des EDPBs, wenn der für die Verarbeitung Verantwortliche anhand einer gründliche Analyse der betreffenden Daten unter Berücksichtigung der fehlenden Informationen, die die Behörden der Empfängerländer möglicherweise besitzen und verwenden, nachgewiesen hat, dass die von ihm an die Auftragsverarbeiter übermittelten personenbezogenen Daten selbst bei einem Abgleich mit solchen Informationen keiner bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Wie ShardSecure Sie dabei unterstützen kann

Die verteilten Container wissen nicht, wo sich die anderen Container befinden, und sie enthalten auch keine Informationen über das ursprüngliche Datenobjekt, die bei der Wiederzusammensetzung helfen würden. Bei der Pseudonymisierung von Daten ist die Re-Identifizierung eines an einem bestimmten Ort gespeicherten Datenbestandes möglich, bei Microsharding nicht. Ein unbefugter Nutzer kann die Microsharded-Daten nicht erneut identifizieren, selbst wenn er auf ihren Speicherort zugreift.

6

Schließlich erfüllen Sie die Anforderungen des EDPBs, wenn es keinen Nachweis für eine Zusammenarbeit zwischen den Behörden in den jeweiligen Gerichtsbarkeiten gibt, in denen die einzelnen Auftragsverarbeiter ansässig sind, die ihnen den Zugang zu allen von den Auftragsverarbeitern gespeicherten personenbezogenen Daten ermöglichen würden und sie in die Lage versetzen würden, den Inhalt der personenbezogenen Daten in einer eindeutigen Form zu rekonstruieren und zu verwerten, wenn eine solche Verwertung den Wesensgehalt der Grundrechte und Grundfreiheiten der betroffenen Personen nicht respektieren würde. Ebenso sollten die Behörden der beiden Länder nicht befugt sein, auf personenbezogene Daten zuzugreifen, die sich im Besitz von Auftragsverarbeitern in allen betroffenen Gerichtsbarkeiten befinden.

Wie ShardSecure Sie dabei unterstützen kann

Der Nutzer kann sowohl die geografischen Speicherorte als auch deren Anzahl für die Microsharded-Daten konfigurieren. Sie unterliegen damit der Kontrolle des Dateneigentümers, der die Microsharded-Daten nach eigenem Ermessen oder Bedarf verteilen kann. Zudem können Dateneigentümer ihre Microsharded-Daten problemlos von einem Speicherort auf eine anderen verschieben – sei es zwischen Regionen eines einzigen Cloud-Providers, zwischen verschiedenen Cloud-Providern oder von einem Cloud-Provider auf einen On-Premises-Speicher.

Diese Funktionen geben den Dateneigentümern die Möglichkeit, ihre Microsharded-Daten über alle Gerichtsbarkeiten hinweg zu verteilen, die sie für angemessen halten.

Dabei gilt es zu beachten, dass Microsharded-Daten, wie in diesem Dokument beschrieben, unverständlich und für unbefugte Nutzer wertlos sind. Der bloße Zugriff auf alle Microsharded-Daten einer bestimmten Organisation reicht nicht aus, um die ursprünglichen Daten zu rekonstruieren. Zudem ist es nicht möglich, dass ein nicht autorisierter Benutzer seine eigene ShardSecure-Instanz nutzt, um die Microsharded-Daten eines Dritten wieder zusammenzusetzen (siehe auch „Integrität und Verfügbarkeit von Microsharded-Daten“).

Microshard™ Technology – ein kompakter Überblick

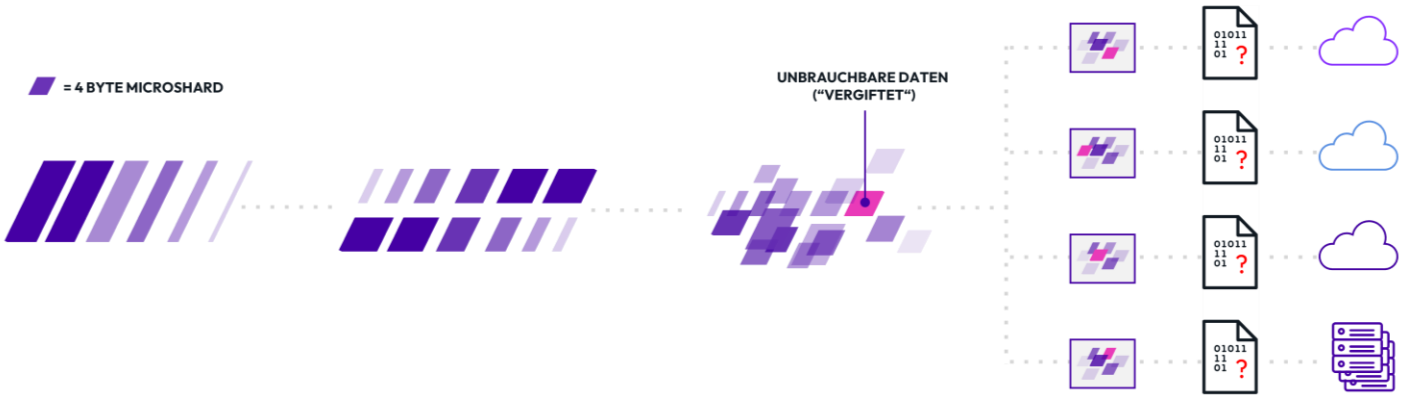
Die Microshard-Technologie von ShardSecure trägt dazu bei, den Datenschutz, die Sicherheit sowie die Resilienz für gespeicherte Daten (Data-at-Rest) in hybriden Infrastrukturen und Multi-Cloud-Umgebungen zu gewährleisten. Der Microsharding-Prozess, der im Folgenden detailliert beschrieben wird, trägt dazu bei, dass Microsharded-Daten unverständlich sind und für unbefugte Nutzer keinen Wert haben.

Die Lösung ist ein softwarebasierter, virtueller Cluster, den Kunden On-Premises, in ihrer Private Cloud und/oder in der Public Cloud betreiben können. Die Lösung fungiert als Abstraktionsschicht zwischen den Anwendungsservern eines Kunden und dem Hybrid-Cloud- oder Multi-Cloud-Speicher eines Kunden. Zu keinem Zeitpunkt werden Kundendaten in der ShardSecure-Lösung gespeichert oder von dieser abgerufen („gelesen“).

Das Frontend erscheint als einfacher Cloud-Speicher über eine API und als Netzwerk-Speicher über ein iSCSI-Modul. Die Anwendungen legen die Daten einfach wie gewohnt im Speicher ab. Die Daten werden jedoch vor der Speicherung an die nachfolgend beschriebene Microsharding-Engine geleitet. Das Backend verteilt die Microsharded-Daten an mehrere kundeneigene Speicherorte.

Der Microsharding-Prozess selbst besteht aus drei Hauptschritten: **Aufteilung (Shred). Mischung (Mix). Verteilung (Distribute)**.

AUFTEILUNG (SHRED)	MISCHUNG (MIX)	VERTEILUNG (DISTRIBUTE)
Die sensiblen Daten werden in ihre einzelnen Bestandteile zerlegt, die zu klein sind, um vertrauliche Informationen zu enthalten.	**Die Microshard-Daten** werden zu neuen Dateien gemischt, die unverständlich, nicht zu identifizieren und damit wertlos sind.	**Dies stellt sicher**, dass die Daten unvollständig sind, da sie an mehrere, segmentierte Speicherorte weitergeleitet werden.
Die Komprimierung und die Microshard-Größen lassen sich konfigurieren.	Dieser Prozess gewährleistet Trennung zusammengehöriger Microshard-Daten.	Räumliche Herausforderung für Angreifer, gleichzeitige Separation der Daten von Administratoren und Cloud-Providern.



Aufteilung (Shred)

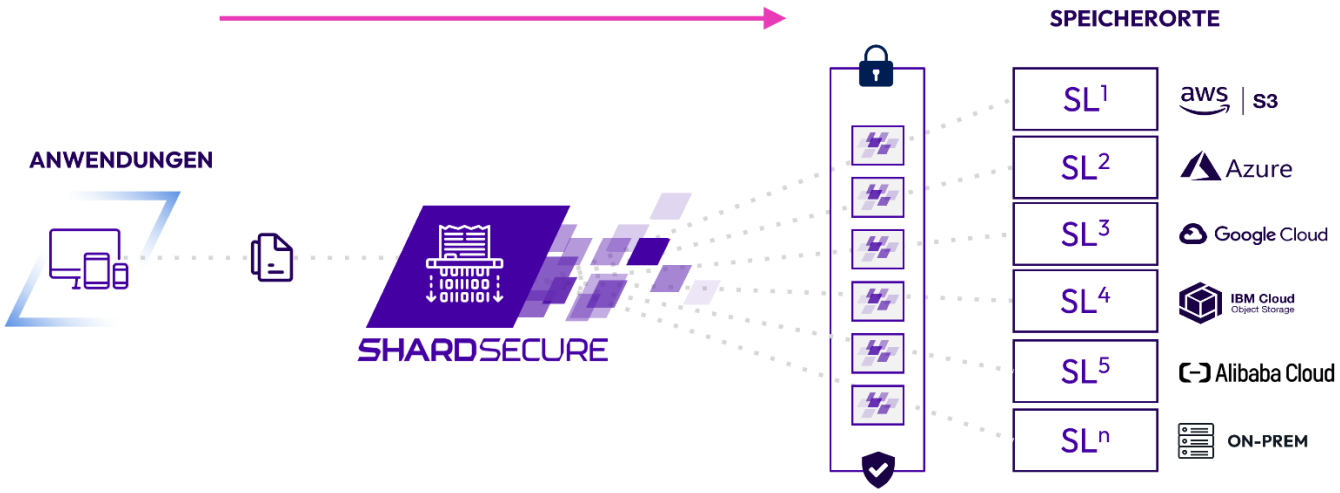
Die Technologie komprimiert die Daten und zerlegt diese dann digital in kleine Fragmente, so genannte Microshards. Der Benutzer kann die Größe der Microshards frei konfigurieren, wobei eine Größe bis zu vier Bytes möglich ist. Damit sind die Microshards zu klein, um personenbezogene Daten (Personal Identifiable Information, PII) oder andere sensible Daten zu enthalten.

Mischung (Mix)

Als nächstes werden die Microshards in mehrere logische Container gemischt, die als Microshard-Container bezeichnet werden. Dabei handelt es sich um Dateien, die eine Teilmenge der Microshards enthalten. Zudem kann der Benutzer definieren, ob und in welchem Umfang zusätzliche Decoy-Daten hinzugefügt werden, um Unbefugten eine erneute Zusammensetzung der Daten zusätzlich zu erschweren. Dateinamen, Dateierweiterungen und Metadaten werden entfernt.

Verteilung (Distribute)

Die Microshard-Container werden dann auf mehrere kundeneigene Speicherorte verteilt. Diese Speicherorte können über mehrere Cloud-Provider, mehrere Regionen eines einzelnen Cloud-Providers und/oder hybride Umgebungen hinweg verteilt sein.



Ein Beispiel für Microsharding

Nehmen wir eine 1 MB große Textdatei, die in Microshards mit einer Größe von vier Bytes aufgeteilt wird. Abhängig von dem für die Datei verwendeten Codierungsstandard ergeben sich daraus mehr als 262.000 Microshards mit einem bis zu vier Zeichen. Die Nutzung von Decoy-Daten erhöht diese Zahl zusätzlich. Die Microsharded-Daten werden in mehrere logische Container gemischt und auf mehrere Speicherorte verteilt. Aufeinanderfolgenden Komponenten der Daten werden nicht am selben Ort gespeichert.

Auch wenn ein nicht autorisierter Benutzer in der Lage wäre, alle Microsharded-Daten von ihren verschiedenen Speicherorten für diese eine Datei zu sammeln, gäbe es Billionen von möglichen Kombinationen, die für eine Rekonstruktion der Daten getestet werden müssten – und dies ist praktisch unmöglich.

Erneute Zusammensetzung von Microsharded-Daten

Die Wiederzusammenführung von Microsharded-Daten ist im Wesentlichen eine Umkehrung des Microsharding-Prozesses. Die Lösung kennt alle Speicherorte sowie die Reihenfolge der Microshards für alle Microsharded-Daten. Dabei ist wichtig zu verstehen, dass die für die Zusammensetzung der Daten verwendeten Anweisungen sicher an mehreren Orten gespeichert sind und alle Anweisungen in Kombination verwendet werden müssen, um die Microsharded-Daten wieder zusammenzuführen (weitere Informationen finden Sie im nachfolgenden Abschnitt „Integrität und Verfügbarkeit von Microsharded-Daten“).

Öffnet ein Benutzer eine Datei, ruft die Microsharding-Engine die Microshard-Container für diese Datei aus dem Speicher ab, setzt die Microshards wieder in der richtigen Reihenfolge zusammen, wobei alle Decoy-Daten ignoriert werden, und gibt die vollständige Datei an die anfordernde Anwendung für den Benutzer zurück. Dies geschieht in Echtzeit und parallel, sodass keine nennenswerte Latenzzeit entsteht.

Erwähnenswert hierbei ist, dass sich die Reihenfolge der Microshards und deren Verteilung jedes Mal ändern, wenn eine Datei gespeichert und in Microshards umgewandelt wird. Dies verhindert, dass ein unbefugter Nutzer geringfügige Änderungen in den Microsharded-Daten erkennen kann, die beispielsweise auf häufig aktualisierte Datenfelder hinweisen könnten. Wird eine vollständige Datei im Microsharding-Verfahren gespeichert und ändert sich die Reihenfolge und Verteilung der Microshards bei jeder Speicherung der Datei, ist es unmöglich, bestimmte Fragmente der Daten zu identifizieren.

Integrität und Verfügbarkeit von Microsharded-Daten

Die Lösung führt mehrere Prüfungen der Datenintegrität durch und rekonstruiert die Microsharded-Daten in Echtzeit, falls bestimmte Microsharded-Daten eine dieser Überprüfungen nicht bestehen sollten. Diese Funktion trägt dazu bei, dass jegliche Manipulation an den gespeicherten Daten (Data-at-Rest), einschließlich der Verschlüsselung durch Ransomware, rückgängig gemacht wird und der Geschäftsbetrieb unbeeinträchtigt fortgeführt werden kann.

Microsharded-Daten können auch Ausfällen von Storage-Services und unbefugten Löschungen standhalten. In beiden Fällen ist die Microsharding-Engine in der Lage, die fehlenden Daten in Echtzeit zu rekonstruieren und so die Business Continuity zu gewährleisten.

Eine häufig gestellte Frage ist, ob ein unbefugter Dritter seine eigene ShardSecure-Instanz installieren könnte, um die Microsharded-Daten einer angegriffenen Organisation wieder zusammenzusetzen. Die Antwort lautet: Nein.

Es sind drei Komponenten erforderlich, um Microsharded-Daten wieder zusammenzusetzen: die Speicherorte der Microshard-Container, die richtige Reihenfolge der Microshards für alle Daten sowie der Zugriff auf alle Speicherorte der Daten. Diese Komponenten, die die Speicherorte und die Reihenfolge der Microshards kennen, sind verschlüsselt und verfügen über zusätzliche Sicherheitsvorkehrungen.

Zusammen bilden diese Komponenten eine Kombination, die für jede Installation einzigartig ist. Daher ist es nicht möglich, eine neue ShardSecure-Instanz einzusetzen, um die von einer anderen Instanz mit Microsharding umgewandelten Daten wieder zusammenzusetzen. Gelangt beispielsweise ein unbefugter Nutzer in den Besitz aller Microsharded-Daten von Kunde A, könnte er keine neue ShardSecure-Instanz einrichten, um die Daten von Kunde A wieder zusammenzusetzen.

Nicole Beranek Zanon, Managing Partner, HÄRTING Attorneys-at-Law Ltd., Zug.
Nicole Beranek Zanon ist zugelassene Rechtsanwältin und hat an der Universität Freiburg Rechtswissenschaften (mit Spezialisierung auf Europarecht und zweisprachigem Abschluss in DE/FR) sowie an der Universität St. Gallen Wirtschaftswissenschaften (Exec. MBA HSG) studiert. Sie ist CIRCA Lead Auditor ISO 27001/2 und besitzt ein CIPPE/E-Zertifikat der IAPP. Sie konzentriert sich auf die Beratung von Mandanten im Informations-, Technologie- und Kommunikationsrecht und verfügt über mehr als 25 Jahre Erfahrung in den Bereichen Datenschutz und IT-Sicherheit als interne und externe Rechtsanwältin.

Hans-Peter Erlingsson, CEO and Founder, Lex Legem Advisory & Consulting.
Hans-Peter Erlingsson hält einen Master of Laws-Abschluss der Universität Uppsala und des University College Dublin und wurde im Jahr 2020 als GDPR Privacy Professional zertifiziert. Er hat sich auf IT-Recht, einschließlich Datenschutzrecht, spezialisiert und verfügt über mehr als 20 Jahre Erfahrung im Datenschutz-Management und Security-Risk-Management in verschiedenen Branchen. Neben verschiedenen kurz- und langfristigen Aufgaben spielte Hans-Peter Erlingsson beispielsweise eine Schlüsselrolle bei dem Aufbau und dem Management des globalen Compliance-Programms für den Datenschutz bei H&M Hennes & Mauritz.

Jesper Tohmo, CTO and Co-Founder, ShardSecure.
Als langjähriger Sicherheitsexperte verfügt Jesper Tohmo über mehr als 15 Jahre Erfahrung in den Bereichen Cybersicherheit und Cloud Computing. Zuvor war er Mitbegründer des Sicherheitsunternehmens 2 face commit, arbeitete als Cloud Automation Engineer bei Scania Sverige und war als Director of Business Development bei McAfee tätig. Jesper Tohmo war zudem Mitbegründer von NordicEdge, einem führenden Unternehmen für Identitätsmanagement, das von Intel McAfee übernommen wurde.

Bitte beachten Sie:

Dieses Dokument dient ausschließlich zu Informationszwecken und stellt keine Rechtsberatung, Verpflichtungen oder Zusicherungen seitens ShardSecure, verbundener Unternehmen oder seitens der Lizenzgeber in Bezug auf Produkte oder Dienstleistungen dar. Kunden sind in vollem Umfang für ihre eigenen, unabhängigen Bewertungen der hier dargestellten Informationen und für ihre Handlungen verantwortlich.

Referenzdokumente:

ShardSecure Whitepaper:

https://shardsecure.com/hubfs/resources/white-papers/ShardSecure__White-Paper--Microsharding-Mar-2021.pdf

ShardSecure Microsharding – Informationen zum Patent:

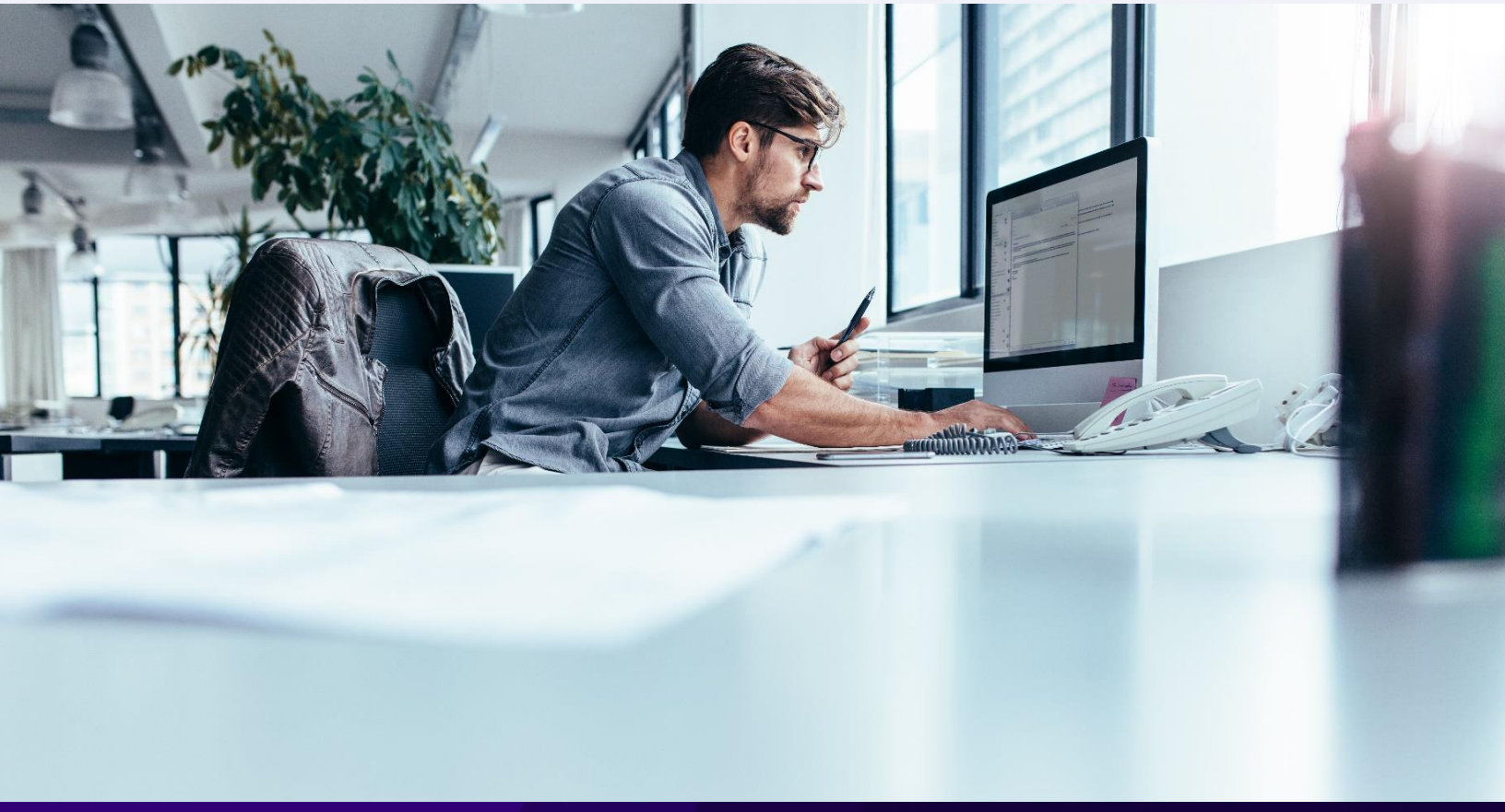
https://patents.justia.com/patent/20200143074

ShardSecure Web site:

https://shardsecure.com/

EU GDPR:

https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf



@ShardSecure
@ShardSecure
@ShardSecure
info@shardsecure.com