White-Paper

DELPHIX™

ANFORDERUNGEN DER DATENSCHUTZ-GRUNDVERORDNUNG FÜR DATA MASKING

Was die IT wissen und tun muss

EINLEITUNG

Diebstahl von geistigem Eigentum, Einbrüche in Datenbanken und andere Verbrechen im Cyberspace sind heute so verbreitet, dass Unternehmen unter wachsendem Druck stehen, sensible Daten zu schützen. Angesichts der Bedenken von Verbrauchern wurden Gesetze erlassen, die von Unternehmen verlangen, beim Umgang mit personenbezogenen Daten besondere Sorgfalt walten zu lassen.

Viele Unternehmen sehen sich daher veranlasst, Technologielösungen zu nutzen, um die Herausforderungen zu bewältigen, die sich aus diesen neuen Vorschriften ergeben. Eine dieser Technologien ist Data Masking. Darunter versteht man den Austausch sensibler Daten durch ein nicht sensibles Äquivalent unter Beibehaltung der Qualität und Konsistenz, die erforderlich sind, damit die Daten für Analysten oder Softwareentwickler weiterhin verwendbar bleiben. Obwohl diese Technologie bereits seit einiger Zeit existiert, gewinnt sie im Zuge der Datenschutz-Grundverordnung der EU, die ab Frühjahr 2018 angewendet wird, an Relevanz und Bedeutung.

Die Datenschutz-Grundverordnung sieht strenge Einschränkungen für Unternehmen vor, die Daten europäischer Bürger erheben, benutzen und verarbeiten. Unternehmen – in der EU sowie auch außerhalb – stehen vor neuen Anforderungen, die sie dazu veranlassen, ihre Ansätze für die Privatsphäre ihrer Kunden zu überdenken und neue Schutzmaßnahmen umzusetzen. In der Tat wurde als neuer Begriff die „Pseudonymisierung" eingeführt, um eine gesetzliche Definition im Zusammenhang mit dem Schutz personenbezogener Daten hinzuzufügen. Pseudonymisierung ist ein Oberbegriff für Ansätze wie Data Masking, die für den Schutz von vertraulichen Daten verwendet werden, aus denen direkt oder indirekt die Identität einer Person abgeleitet werden kann. Die Datenschutz-Grundverordnung bestraft Unternehmen, die im Rahmen ihrer Sicherheitsstrategie keine geeigneten Schutzmaßnahmen treffen, wie beispielsweise durch Pseudonymisierungstechnologien. Die Strafe für eine Nichtbeachtung dieser Vorschrift kann Unternehmen hart treffen: Sie kann bis zu 4 % des weltweiten Umsatzes betragen – genug, um die laufenden europäischen Geschäfte von Unternehmen zu gefährden, die in der Europäischen Union tätig sind.

In diesem White-Paper werden die zu erwartenden Änderungen in der Datenschutz-Grundverordnung untersucht und die wichtigsten Anforderungen dargestellt, die Unternehmen kennen und in ihre Umsetzung einbeziehen müssen. Danach gehen wir darauf ein, wie jüngste Innovationen des Data Maskings die Einhaltung behördlicher Auflagen gewährleisten und dabei gleichzeitig die Komplexität reduzieren, die ein Hindernis für geschäftliche Agilität bildet.

DIE AUTOREN

Phil Lee ist Partner in der Privacy, Security and Information Group bei Fieldfisher und leitet den US-Standort im Silicon Valley in Kalifornien. Er hat CIPP(E)- und CIPM-Status und ist Mitglied der Privacy Faculty von IAPP.

Phil Lee ist insbesondere spezialisiert auf Profiling des Nutzerverhaltens und die Cookie-Reglementierung, E-Marketing und internationale Datenübertragungsstrategien (einschließlich verbindliche Unternehmensregelungen). Er hat an zahlreichen grenzüberschreitenden Datenschutzprojekten für mehr als 80 Länder mitgewirkt. Phil Lee ist nicht nur im Datenschutz- und Informationsrecht sondern auch in einer Vielzahl Technologie-, Social Media- und E-Commerce-Projekte beratend tätig. Who's Who Legal nennt Phil Lee „einen der profiliertesten Rechtsexperten" für Datenschutz und Online-Regelungen.

Jes Breslaw ist derzeit EMEA Director of Strategy bei Delphix. Er ist seit 19 Jahren in führenden Positionen bei Technologielieferanten und Systemintegratoren in Europa tätig. Jes Breslaw begann seine Karriere als Produktmanager für IBM-Hardware und war dann acht Jahre lang im Bereich Sicherheitslösungen tätig, unter anderem bei CheckPoint Software und Cisco. Bevor er zu Delphix kam, arbeitete Jes Breslaw bei Unternehmen, die sichere Mobillösungen bereitstellen, zuerst Workshare und dann Accellion.

EINE VERÄNDERTE UMGEBUNG: DAS NEUE EUROPÄISCHE DATENSCHUTZRECHT

Im April 2016 beschloss die Europäische Union endgültig neue, weiterreichende Regelungen, die sowohl in der EU als auch darüber hinaus wesentliche Auswirkungen auf alle Unternehmen haben werden, die personenbezogene Daten über europäische Bürger erheben, nutzen und verarbeiten. Die nunmehr erreichte Regelung stellt den Höhepunkt jahrelanger harter Arbeit europäischer Politiker und Gesetzgeber dar. Die europäische Kommission, das EU-Parlament und der Europäische Rat einigten sich damit auf den Text der neuen europäischen „Datenschutz-Grundverordnung", die die Nachfolgeregelung der veralteten „Datenschutzrichtlinie" der EU ist.

Warum ist das für Sie für Bedeutung? Um darauf eine Antwort zu geben, treten wir erst einmal einen Schritt zurück und sehen uns an, wie sich die Technologie und die Rechtslage über die letzten 20 Jahre entwickelt haben. Die Geschichte beginnt 1995, als die EU ihre aktuelle Datenschutzrichtlinie (Richtlinie 95/46/EG, hier einfach „Richtlinie") beschloss, die für die gesamte EU festlegte, wie Unternehmen Daten von Personen erheben, nutzen und verarbeiten können. Die aktuelle Richtlinie stammt also aus einer Zeit, in der nur wenige Haushalte über Computer verfügten (an dieser Stelle sei daran erinnert, dass laut amerikanischer Statistikbehörde 1995 nur rund 30 % der US-Haushalte über einen Computer verfügten[1]) und fast niemand Internetzugang hatte. Damals gab es weder Social Media noch Online-Banking oder Cloud Computing. Genau diese Richtlinie regelt aber immer noch die rund um die Uhr verbundene und vernetzte Welt von Big Data, in der die Europäer heute leben.

Die Technologie hat sich weiterentwickelt, die Rechtsordnung aber nicht. Die Europäische Kommission erkannte, dass das europäische Datenschutzrecht an die neuen Technologien angepasst werden musste, und beschloss Anfang 2012, Vorschläge für ein neues Datenschutzrecht zu veröffentlichen – die „Datenschutz-Grundverordnung". Die Vorschläge waren umstritten und wurden von vielen Seiten kritisiert, die an Daten Interesse haben – Regierungen, multinationale Unternehmen, Organisationen zum Schutz bürgerlicher Freiheiten, Presse und andere. Die Argumente kamen dabei immer aus der jeweils eigenen Perspektive und daher wurden die Vorschläge entweder als zu eng oder zu locker, zu streng oder nicht streng genug beurteilt. Es war nicht einfach, hier einen Konsens herzustellen. Im Verlauf der folgenden vier Jahre wurde die Datenschutz-Grundverordnung zu einem der am heftigsten debattierten Gesetzgebungsvorhaben in der Europäischen Union. Während der Gesetzesvorbereitung gab es mehr als dreitausend Abänderungsanträge.

Trotz dieser Schwierigkeiten wurde die Datenschutz-Grundverordnung am 14. April 2016 zu europäischem Recht (mit einem spätesten Umsetzungstermin im Jahr 2018). Zu den umstrittenen neuen Anforderungen gehört die Bestimmung, dass die Datenschutz-Grundverordnung weltweit für alle Unternehmen gilt, die Waren und Dienstleistungen für europäische Bürger anbieten bzw. das Verhalten europäischer Bürger überwachen. Ebenso umstritten war die Tatsache, dass Unternehmen, die die Datenschutz-Grundverordnung verletzen, strenge Strafen in der Höhe von bis zu 4 % des weltweiten Jahresumsatzes riskieren. Aufgrund dieser bedeutenden Risiken für Unternehmen beherrschte der Datenschutz die Titelseiten der Presse und stand so hoch auf der Tagesordnung von Vorstandssitzungen wie nie zuvor. Unternehmen prüfen derzeit ihre aktuellen Datenschutzstrategien, um sich auf 2018 vorzubereiten, wenn die neuen gesetzlichen Regelungen in Kraft treten.

Vor diesem Hintergrund von Veränderungen in der Rechtslage und neuen Risiken untersuchen wir in diesem White-Paper, wie „Pseudonymisierungstechnologien" wie die Data Masking-Technologie von Delphix Unternehmen dabei unterstützen können, sich auf diese Änderungen vorzubereiten und die durch die neuen Rechtsvorschriften entstehenden Risiken zu mindern.

1http://www.census.gov/hhes/computer/

PSEUDONYMISIERUNG UND DATENSCHUTZ-GRUNDVERORDNUNG

WAS IST PSEUDONYMISIERUNG?

Europäische Datenschutzgesetze schützen „personenbezogene Daten", daher unterliegen Daten, die nicht „personenbezogen" sind, nicht den europäischen Datenschutzregelungen und können von Unternehmen genutzt und unbeschränkt geteilt werden. Gemäß der derzeitigen Rechtslage gilt eine breite Definition für „personenbezogene Daten". Sie ist auf „alle Informationen über eine bestimmte oder bestimmbare natürliche Person" anzuwenden, auch wenn eine „Person, … unmittelbar oder mittelbar identifiziert werden kann, insbesondere durch Verweis auf eine Identifikationsnummer oder die körperlichen, physiologischen, geistigen, wirtschaftlichen, kulturellen oder sozialen Merkmale der Person."[2]

Der Verweis auf „unmittelbare oder mittelbare" Identifizierung löste sehr lange Zeit Verwirrung bei Unternehmen aus. „Unmittelbare" erfasst eindeutig Informationen, die offensichtlich die Identität einer Person verraten, beispielsweise ihr Name oder ihre Kontaktdaten. Aber was war unter „mittelbarer" Identifizierung zu verstehen? Die europäischen Datenschutzbehörden sind der Ansicht, dass Daten, die durch das Entfernen mittelbar identifizierbarer Details scheinbar „anonymisiert" (verschleiert) wurden, weiterhin personenbezogenen Daten darstellen, wenn der sich daraus ergebende Datensatz eine „mittelbare" Identifizierung ermöglicht.[3]

Dies kann beispielsweise der Fall sein, wenn ein Unternehmen seine Daten nur unzureichend verschleiert und nur Kundennamen aus seinen Datenbanken entfernt, aber Daten über die Kontoaktivitäten des Kunden aufbewahrt (beispielsweise welche Dienste er benutzt, Zahlungsaufzeichnungen und IP-Adressen, Informationen über die Geräte, von denen der Zugriff auf das Online-Konto erfolgt). In diesem Fall kann die Sammlung dieser Daten ausreichen, um eine „mittelbare" Identifizierung des Kunden mit relativ wenig Aufwand zu ermöglichen.

Um mit diesem Sachverhalt umzugehen, trifft die Verordnung eine Unterscheidung. Daten, die vollständig anonymisiert sind (beispielsweise zusammengefasste, anonymisierte Statistiken, aus denen kein Datensatz extrahiert werden kann, der zu einer Person zuordenbar ist), werden vom Datenschutz ausgenommen. Hingegen werden Daten, die verborgen sind, aber bei denen die Möglichkeit besteht, eine Identität wie im oben genannten Beispiel herauszufinden, als pseudonymisiert klassifiziert.

Nach der aktuellen Rechtslage werden „pseudonymisierte Daten" nicht definiert, sie werden aber im Wesentlichen genauso behandelt wie andere Arten von unmittelbar identifizierbaren personenbezogenen Daten. Wenn also ein Unternehmen Maßnahmen getroffen hat, seine Daten durch Data Masking oder Streuspeicherung (Hashing) zur Einhaltung von Datenschutzbestimmungen zu verfremden, unterliegt der verfremdete Datensatz gegebenenfalls weiterhin der umfassenden Geltung der Compliance-Regelungen gemäß der Richtlinie.

Die aktuelle Rechtslage hat daher die unerwünschte Konsequenz, dass auch Unternehmen, die im Prinzip „rechtskonform" handeln, indem sie Datenverfremdungstechniken wie Data Masking oder Hashing einsetzen, für ihr richtiges Verhalten im rechtlichen Sinne nicht besser behandelt werden. Dies hält wiederum viele Unternehmen davon ab, Kosten und Aufwand auf sich zu nehmen, um diese Technologien einzusetzen, obwohl sie natürlich für den Datenschutz große Vorteile hätten.

Die Datenschutz-Grundverordnung hingegen erkennt an, dass die Pseudonymisierung gefördert werden muss, und enthält einige Bestimmungen zu diesem Zweck.

2) Art 2(a) Richtlinie

3) Siehe Artikel „Stellungnahme 5/2014 zu Anonymisierungstechniken" durch die EU

WIE KÖNNEN UNTERNEHMEN MIT DER PSEUDONYMISIERUNG DIE DATENSCHUTZ-GRUNDVERORDNUNG BESSER EINHALTEN?

Im Unterschied zur Richtlinie enthält die neue Datenschutz-Grundverordnung eine ausdrückliche gesetzliche Definition von Pseudonymisierung als „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden."[4]

Einfach gesagt, die Datenschutz-Grundverordnung erklärt, dass pseudonymisierte Daten in einem Format gespeichert werden, aus dem eine direkte Identifizierung einer bestimmten Person nur mit zusätzlichen Informationen, beispielsweise aus getrennt gespeicherten Zuordnungstabellen, möglich ist.

Beispiel: „Benutzer ABC12345" und nicht „Karl Mustermann". Um „Karl Mustermann" aus „Benutzer ABC12345" abzuleiten, ist eine Zuordnungstabelle erforderlich, die Benutzer-IDs den Benutzernamen zuordnet). Wenn solche Zuordnungsinformationen vorhanden sind, müssen sie getrennt gespeichert werden und Kontrollen unterliegen, die verhindern, dass sie mit den pseudonymisierten Daten kombiniert werden können, um eine Identifizierung vorzunehmen. Data Masking und Hashing sind Beispiele für Pseudonymisierungstechniken.[5]

Wie die Richtlinie stuft auch die Datenschutz-Grundverordnung pseudonymisierte Daten als personenbezogene Daten ein. Dies hat zur Folge, dass für die Nutzung und den Schutz von pseudonymisierten Daten das europäische Datenschutzrecht weiterhin gilt. Entscheidend ist aber, dass die Datenschutz-Grundverordnung im deutlichen Gegensatz zur Richtlinie Unternehmen dazu motiviert, ihre Datensätze aus verschiedenen Gründen zu pseudonymisieren. Diese werden nachstehend beschrieben.

PSEUDONYMISIERUNG ALS SICHERHEITSMASSNAHME

Art. 30 der Datenschutz-Grundverordnung legt die Sicherheitsanforderungen fest, die Unternehmen erfüllen müssen. Die Grundverordnung fordert, dass Unternehmen „geeignete" technische und organisatorische Maßnahmen treffen müssen, um personenbezogene Daten zu schützen, und dabei das Risiko berücksichtigen müssen, das für Personen entsteht, wenn die Sicherheit der Daten verletzt wird.

In diesem Zusammenhang erklärt die Datenschutz-Grundverordnung ausdrücklich, dass Unternehmen „unter anderem… die Pseudonymisierung und Verschlüsselung personenbezogener Daten" in Betracht ziehen sollten. Die Verordnung sagt zwar nicht ausdrücklich, dass Unternehmen die Pseudonymisierung implementieren müssen, der explizite Verweis auf die Pseudonymisierung unter den Sicherheitsbestimmungen der Datenschutz-Grundverordnung ist aber vielsagend – weil damit angezeigt wird, dass bei einer Sicherheitsverletzung die Aufsichtsbehörden auch die Tatsache berücksichtigen werden, ob ein Unternehmen Pseudonymisierungstechnologien implementiert hat. Unternehmen, die dies nicht getan haben, werden daher gegebenenfalls von Aufsichtsbehörden strenger behandelt.

Um diesen Punkt noch zu betonen, enthält die Präambel der Datenschutz-Grundverordnung die Formulierung „dass personenbezogene Daten so schnell wie möglich pseudonymisiert werden", um die Anforderungen des Datenschutzes „durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default)" zu erfüllen.[6] Einfacher formuliert: Die Datenschutz-Grundverordnung erkennt die Pseudonymisierung als wichtiges Instrument für die Einhaltung der von ihr gestellten Anforderungen an.

4) Artikel 4(5) Datenschutz-Grundverordnung

5) Ebenda 3 auf Seite 20.

6) Erwägungsgründe 78 Datenschutz-Grundverordnung

PSEUDONYMISIERUNG ZUR REDUKTION DER BELASTUNG DURCH MELDEPFLICHTEN BEI VERLETZUNGEN DES SCHUTZES PERSONENBEZOGENER DATEN

Im Zusammenhang mit dem oben genannten Aspekt führt die Datenschutz-Grundverordnung neue Regeln für Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten ein. Unternehmen, bei denen ein Problem mit der Datensicherheit aufgetreten ist, müssen ihre Unternehmenskunden, ihre Aufsichtsbehörden und die Personen, deren Daten davon betroffen sind, möglicherweise verständigen. Das derzeitige Datenschutzrecht kennt solche Anforderungen nur in bestimmten regulierten Sektoren (beispielsweise Meldepflichten bei Datenverletzungen für Telekommunikationsunternehmen und Internet-Service-Provider).

Unternehmen, bei denen es zu Verletzungen des Schutzes personenbezogener Daten gekommen ist, wissen, dass dabei neben den Kosten für die Wiederherstellung des Schutzes der betroffenen Daten mit zusätzlichen Kosten finanzieller Art, Verlust von Reputation und Ressourcenaufwand zu rechnen ist. In den USA, wo Meldepflichten bei Verletzungen des Schutzes personenbezogener Daten bereits seit längerer Zeit eingeführt sind, sieht die Federal Trade Commission bedeutende Strafen für Zwischenfälle beim Datenschutz vor. Unternehmen, bei denen eine Verletzung personenbezogener Daten vorgekommen ist, müssen nicht nur mit schlechter Presse rechnen sondern auch mit Sammelklagen.[7] Viele Unternehmen machen sich daher Sorgen, ob die Einführung von Meldepflichten für Verletzungen des Schutzes personenbezogener Daten in der EU zu ähnlichen Problemen für Unternehmen führen wird wie jenseits des Atlantiks in den USA.

Die von der Datenschutz-Grundverordnung eingeführten Regeln enthalten die Erwartung, dass Unternehmen die für den Datenschutz zuständigen Aufsichtsbehörden innerhalb von 72 Stunden nach Entdeckung einer Verletzung des Schutzes personenbezogener Daten – eine sehr kurze Frist für jeden größeren Zwischenfall im Zusammenhang mit dem Datenschutz – und die betroffenen Personen „ohne unangemessene Verzögerung" verständigen müssen.[8] Die Datenschutz-Grundverordnung enthält die Klausel, dass Unternehmen die für den Datenschutz zuständige Aufsichtsbehörden nicht verständigen müssen, wenn „die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt". In diesem Sinne enthält sie auch die Bestimmung, dass Unternehmen betroffene Personen nur informieren müssen, wenn die Verletzung des Schutzes personenbezogener Daten zu einem „hohen Risiko" für ihre Privatsphäre werden könnte – und die Meldung ist nicht erforderlich, wenn das Unternehmen „geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat … solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden …"[9]

Verkürzt gesagt: Wenn eine Verletzung des Schutzes personenbezogener Daten ein geringes Risiko für die betroffenen Personen in sich trägt, werden die Meldepflichten der Datenschutz-Grundverordnung gemildert. Die Pseudonymisierung durch Data Masking, Hashing oder Verschlüsselung ist eindeutig eine Methode zur Reduktion der Risiken für Personen nach einer Verletzung des Schutzes personenbezogener Daten (beispielsweise durch Reduktion der Wahrscheinlichkeit eines Identitätsdiebstahls oder anderer Formen des Datenmissbrauchs) und wird von der Datenschutz-Grundverordnung als Sicherheitsmaßnahme wie oben bereits beschrieben akzeptiert.

Daraus ergibt sich, dass Unternehmen, die ihre Daten wirksam pseudonymisiert haben, die Ausnahmeregelungen für die Meldepflicht an Aufsichtsbehörden und die betroffenen Personen bei einer Verletzung des Datenschutzes in Anspruch nehmen können. Angesichts der zunehmenden Häufung und der Kosten von Datenschutzverletzungen[10] ist dies ein wichtiger Anreiz für Unternehmen, ihre Datensätze zu pseudonymisieren.

PSEUDONYMISIERUNG ZUR VERRINGERUNG DER BELASTUNG DURCH DATENHERAUSGABEPFLICHTEN

Eine der größten Herausforderungen für die Einhaltung der Vorschriften der aktuellen Richtlinie betrifft das „Auskunftsrecht", das Einzelpersonen das Recht gibt, von einem Unternehmen die Herausgabe einer Kopie aller personenbezogenen Daten zu verlangen, die über sie verarbeitet werden.[11] Das Unternehmen muss diese Anforderung innerhalb einer sehr kurzen Frist (in der Regel nur

7) Siehe als Beispiel http://www.wired.com/2015/08/court-says-ftc-can-slap-companies-getting-hacked/.

8) Art. 31 und 32 Datenschutz-Grundverordnung

9) Art. 33(1), 34(1) und 34(3)(a) Datenschutz-Grundverordnung

10) Siehe „Global State of Information Security Survey 2015" von PWC unter http://www.pwc.com/us/en/press-releases/2014/global-state-of-information-security-survey-2015.html

11) Art 12 Richtlinie

40 Tage) erfüllen und in dieser Zeitspanne aufwendige und kostenintensive Anstrengungen unternehmen, um seine Systeme zu durchsuchen und personenbezogene Daten zu ermitteln, die mit dieser E-Mail-Adresse verbunden sind, eventuelle personenbezogene Daten von Dritten aus den für die Herausgabe ermittelten Daten zu entfernen (beispielsweise Verweise auf Dritte in E-Mails), Rücksprache mit der Rechtsabteilung zu halten, um die herauszugebenden Unterlagen im Hinblick auf Compliance und Risikomanagement zu überprüfen, und dann die Daten an die Person zu übermitteln. Die Ausübung des Auskunftsrechts erfolgt häufig im Zusammenhang mit Rechtsstreitigkeiten durch Personen, die mehr Informationen erhalten möchten als sie im normalen Verfahrensverlauf zu erhalten berechtigt sind.

Einzelpersonen haben auch in der Datenschutz-Grundverordnung das Auskunftsrecht. Allerdings scheint die Datenschutz-Grundverordnung die Herausgabeanforderungen bei einer Ausübung des Auskunftsrechts abzumildern, wenn Daten pseudonymisiert wurden. Sie zeigt sich damit konsistent zu ihrem Ansatz zu Pseudonymisierung im Fall von Datenschutzverletzungen. Die Klausel lautet: „Kann [das Unternehmen] nachweisen, dass es nicht in der Lage ist, die betroffene Person zu identifizieren, … finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen."

Das bedeutet, dass ein Unternehmen nicht verpflichtet werden kann, Daten herauszugeben, die effektiv pseudonymisiert wurden, wenn eine Person ihr Auskunftsrecht ausübt. Dies ist ein besonders wichtiger Vorteil für Unternehmen mit einem großen Kundenkreis, bei denen jederzeit Auskunftsanfragen von Verbrauchern eintreffen können.[12]

PSEUDONYMISIERUNG ALS UNTERSTÜTZUNG FÜR DAS PROFILING

Eine weitere wichtige Weiterentwicklung in der Datenschutz-Grundverordnung ist die Einführung des Profiling-Konzepts, das wie folgt definiert wird: „[Profiling ist] jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen."[13] Die Datenschutz-Grundverordnung verfügt weiterhin, dass Unternehmen Personen nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung – einschließlich Profiling – unterwerfen dürfen, sofern nicht bestimmte rechtliche Kriterien erfüllt sind und die Person nicht ihre ausdrückliche Einwilligung gegeben hat.[14]

Die Regel gilt aber nur, wenn das Profiling „rechtliche Wirkung" entfaltet „oder sie in ähnlicher Weise erheblich beeinträchtigt". Die Datenschutz-Grundverordnung erwähnt ausdrücklich die Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren als zwei Beispiele für eine solche automatisierte Entscheidungsfindung.[15] Die Frage, ob das Online-Profiling für Zwecke der Datenanalyse oder gezielte Werbung von dieser Regel erfasst wird, bleibt aber offen.

Die Datenschutz-Grundverordnung ist zwar in diesem Punkt nicht vollkommen klar, aber Daten-Profiling in Fällen, in denen die unmittelbar identifizierenden Daten einer Person durch Pseudonymisierung entfernt wurden, reduziert wesentlich die Datenschutzauswirkungen auf die Person, insbesondere wenn die übergreifende Unterstützung der Datenschutz-Grundverordnung für Pseudonymisierung in die Betrachtung einbezogen wird. Angesichts dessen ist es nicht wahrscheinlich, dass die Online-Datenanalyse oder gezielte Werbung, die auf pseudonymisierten Daten basieren, „rechtliche Wirkungen" für Personen nach sich ziehen oder „sie in ähnlicher Weise erheblich beeinträchtigen". Sie erfordern daher wahrscheinlich nicht die ausdrückliche Einwilligung für eine automatisierte Entscheidungsfindung, die von der Datenschutz-Grundverordnung sonst vorgeschrieben wird.

12) Siehe beispielsweise die ZDNet-Meldung „Reddit users overwhelm Facebook with data requests" unter http://www.zdnet.com/article/reddit-users-overwhelm-facebook-with-data-requests/

13) Art. 4(4) Datenschutz-Grundverordnung

14) Art. 22(1) und 22(2) Datenschutz-Grundverordnung

15) Erwägungsgründe 71 Datenschutz-Grundverordnung

RISIKEN DER NICHTEINHALTUNG DER DATENSCHUTZ-GRUNDVERORDNUNG

Die Datenschutz-Grundverordnung wird nach ihrem Inkrafttreten schwere Strafen für Unternehmen vorschreiben, die sie nicht einhalten.[16] Die Datenschutz-Grundverordnung richtet ein zweistufiges Geldstrafensystem ein, nach dem bestimmte Verstöße gegen die Datenschutz-Grundverordnung mit Geldstrafen von bis zu 10 Millionen Euro oder 2 % des weltweiten Umsatzes (also der Gesamteinnahmen eines Unternehmens) geahndet werden, während schwerwiegendere Verstöße Gesamtstrafen von bis zu 20 Millionen Euro oder 4 % des weltweiten Gesamtumsatzes – in beiden Fällen der jeweils höhere Betrag – nach sich ziehen können. Bei der Festlegung der Höhe der Geldstrafe können die Datenschutzbehörden die „technischen und organisatorischen Maßnahmen" berücksichtigen, die von Unternehmen eingesetzt wurden – und[17] die Verwendung von Pseudonymisierungstechnologien wird in diesem Fall sicherlich einen gewichtigen Faktor darstellen.

Neben den Geldstrafen räumt die Datenschutz-Grundverordnung den Datenschutzbehörden auch weitere Befugnisse ein, beispielsweise verpflichtende Überprüfungen. [18]Außerdem haben Einzelpersonen die Möglichkeit, Gerichtsverfahren gegen Unternehmen anzustrengen, die die Verordnung nicht einhalten (bzw. solche Verfahren durch Datenschutzorganisationen in ihrem Namen einbringen zu lassen).

Die Datenschutz-Grundverordnung folgt daher einem Ansatz nach dem Prinzip „Fordern und Fördern", um Unternehmen zu motivieren, ihre Daten zu pseudonymisieren – wobei das „Fördern" darin besteht, an verschiedenen Stellen der Datenschutz-Grundverordnung ausdrücklich die Pseudonymisierung zu empfehlen und bestimmte Pflichten für Unternehmen zu reduzieren, die ihre Daten pseudonymisieren. Das „Fordern" umfasst Strafandrohungen für Unternehmen, die die Vorschriften nicht einhalten.

PSEUDONYMISIERUNG UND DATA MASKING-TECHNOLOGIE

Data Masking ist der faktische Standard für die Pseudonymisierung, insbesondere in sogenannten Nicht-Produktionsdatenumgebungen, die für Softwareentwicklung, Tests, Schulungen und Analysen eingesetzt werden. Indem sensible Daten durch fiktive, aber realistische Daten ersetzt werden, neutralisieren Data Masking-Lösungen das Datenrisiko und bewahren den Wert der Daten für den Einsatz in Nicht-Produktionsumgebungen.

Alternative Ansätze wie die Verschlüsselung können diesen Anspruch in wichtigen Bereichen nicht erfüllen. Ihr größter Nachteil ist die Schwachstelle für Identitätsdiebstahl, Insider-Bedrohungen oder andere Szenarios, bei denen sich Eindringlinge Chiffrierschlüssel besorgen können: Wer den richtigen Chiffrierschlüssel hat, kann alle Verteidigungslinien der Verschlüsselung überwinden und hat Zugang zu den sensiblen Daten. Data Masking verwandelt hingegen die sensiblen Daten unwiederbringlich und eliminiert damit das Risiko durch Insider- und Outsider-Bedrohungen gleichermaßen.

PSEUDONYMISIERUNG ERFORDERT EINEN „DATEN ZUERST"-ANSATZ

Data Masking bietet einem Unternehmen zwar ein Instrument, mit dem die wichtigsten Herausforderungen der Datenschutz-Grundverordnung bewältigt werden können, dafür ist allerdings ein „Daten zuerst"-Ansatz erforderlich, der eine höhere Aufmerksamkeit für die Art und Weise erforderlich macht, wie Daten sich im Zeitverlauf verändern und bewegen bzw. wie sie besser kontrolliert werden können. Unternehmen können Pseudonymisierung durch Data Masking wirksam realisieren, wenn sie sich die folgenden Fragen stellen:

WO SIND IHRE DATEN?

Unternehmen stellen viele Kopien ihrer Produktionsumgebung für Softwareentwicklung, Tests, Backup und das Berichtswesen her. In diesen Umgebungen werden rund 90 % aller Daten gespeichert und sie sind oft über mehrere Repositorys und Standorte verteilt. Unternehmen, die wissen, wo sich ihre Daten befinden – einschließlich sensibler Daten in verschiedenen Nicht-Produktionsumgebungen – sind besser vorbereitet, um Schutzmaßnahmen gezielt einzurichten.

16) Art. 79 Datenschutz-Grundverordnung
17) Art 79(2a)(e) Datenschutz-Grundverordnung
18) Art. 53 Datenschutz-Grundverordnung

WIE SIEHT IHRE DATEN-GOVERNANCE AUS?

Nur sehr wenige Organisationen verfügen über einen Datenvorstand (Chief Date Officer) oder Leiter für Datenschutz. Selbst wenn diese Position in einem Unternehmen besetzt ist, besteht dennoch möglicherweise keine adäquate Kontrolle über die Bewegung und Verarbeitung von Daten, weil die einzelnen Geschäftsbereiche – jeder mit eigenen Administratoren, IT-Architekten und Entwicklern – oft datenbezogene Prozesse auf Projektebene definieren und dabei wenige oder gar keine unternehmensweiten Richtlinien umsetzen oder überhaupt zur Verfügung haben. Unternehmen, die sich mit der Datenschutz-Grundverordnung beschäftigen, müssen die Kontrolle über ihre Daten wiedererlangen. Sie müssen Instrumente einführen, die eine mehr Transparenz und Standardisierung für Prozesse wie Data Masking fördern.

WIE STELLEN SIE DATEN BEREIT?

Viele vorhandene Ansätze für die Bereitstellung von Daten sind stark auf manuelle Aktivitäten angewiesen, weisen eine hohe Ressourcennutzung auf und benötigen eine aufwendige Koordination mehrerer Teams. Wenn die Pseudonymisierung auf komplizierten Datenbereitstellungsprozessen aufbaut, wird die Last noch größer und Unternehmen geben ihre Versuche mit Technologien wie Data Masking häufig wieder auf. Um eine Technologie wie Data Masking erfolgreich umsetzen zu können, muss ein Unternehmen nicht nur die Datenbereitstellung optimieren, sondern auch sicherstellen, dass Data Masking ein wiederholbarer und integrierter Teil des Bereitstellungsprozesses ist.

DIE DATENSCHUTZ-GRUNDVERORDNUNG: DYNAMIK FÜR POSITIVE VERÄNDERUNGEN

Für viele Unternehmen schafft die Datenschutz-Grundverordnung die Notwendigkeit, ihre Prozesse für Speicherung, Verwaltung und Schutz ihrer Daten zu überdenken und neu aufzustellen. Ein wesentlicher Aspekt ist auch, dass die neue Verordnung zu einer Welle der IT-Innovation führen wird und damit das Potenzial hat, nicht nur die Compliance sicherzustellen und das Risiko von Verletzungen des Schutzes personenbezogener Daten zu reduzieren, sondern auch wesentliche Geschäftsinitiativen zu beschleunigen.

DATA MASKING MIT VIRTUELLEN DATEN

Innovationen, die virtuelle Daten und Data Masking kombinieren, werden beispielsweise nicht nur den Prozess der Verfremdung von Daten vereinfachen, sondern auch die Bereitstellung der verfremdeten Daten. Diese Lösungen erzeugen und liefern schlanke Datenkopien in einem Bruchteil der Zeit und für einen Bruchteil des für normale physische Kopien erforderlichen Speicherplatzes. Das Speichern, Verwalten und Bereitstellen virtueller Kopien erfolgt von einer einzelnen Kontrollstelle aus, um die Kontrolle über die Daten zu optimieren.

Data Masking kann zudem direkt in den Datenbereitstellungsprozess integriert werden, um virtuelle Kopien automatisch zu verfremden. Als Endergebnis werden verfremdete Daten viel schneller erstellt und bereitgestellt, sodass die Einhaltung der Datenschutz-Grundverordnung gewährleistet wird und von sicheren Daten abhängige Prozesse beschleunigt werden. Zu diesen Prozessen gehören vor allem Softwareentwicklung, Tests und Analyseprojekte, die – heute mehr denn je zuvor – bestimmen, wie Unternehmen aus allen Branchen im Wettbewerb bestehen und Erfolg haben.

Data Masking-Technologien gibt es schon seit längerer Zeit. Wie kommt es daher, dass zu viele Unternehmen damit schlechte Erfahrungen gemacht haben oder einfach entscheiden, sie nicht zu verwenden? Grund dafür ist, dass diese Technologien bisher stark auf die manuelle Verarbeitung in komplexen Abläufen ausgelegt waren. Eigens geschulte Personen oder Teams führen sie durch und jede Anwendung muss unabhängig bearbeitet werden. Unternehmen sehen sich daher gezwungen, Prioritäten festzulegen, welche Datensätze verfremdet werden und welche ungeschützt bleiben. Im neuesten Bloor Data Masking-Bericht wird das Beispiel des Data Masking von Oracle zitiert, bei dem „die Nutzung einer Oracle-Datenbank erforderlich ist (umfassende IT-Kenntnisse sind ebenfalls notwendig)“. Das Problem beim Data Masking liegt nicht in den Data Masking-Regeln, sondern in der Bereitstellung der dadurch verfremdeten Daten. Der Bloor-Bericht führt im Übrigen aus, wie einige der eigenständigen Methoden zum Massenprodukt wurden:

„... viele angebotene Lösungen werden auch für ihre ergänzenden Funktionen ausgewählt und nicht nur für die reinen Data Masking-Funktionen des Produkts."

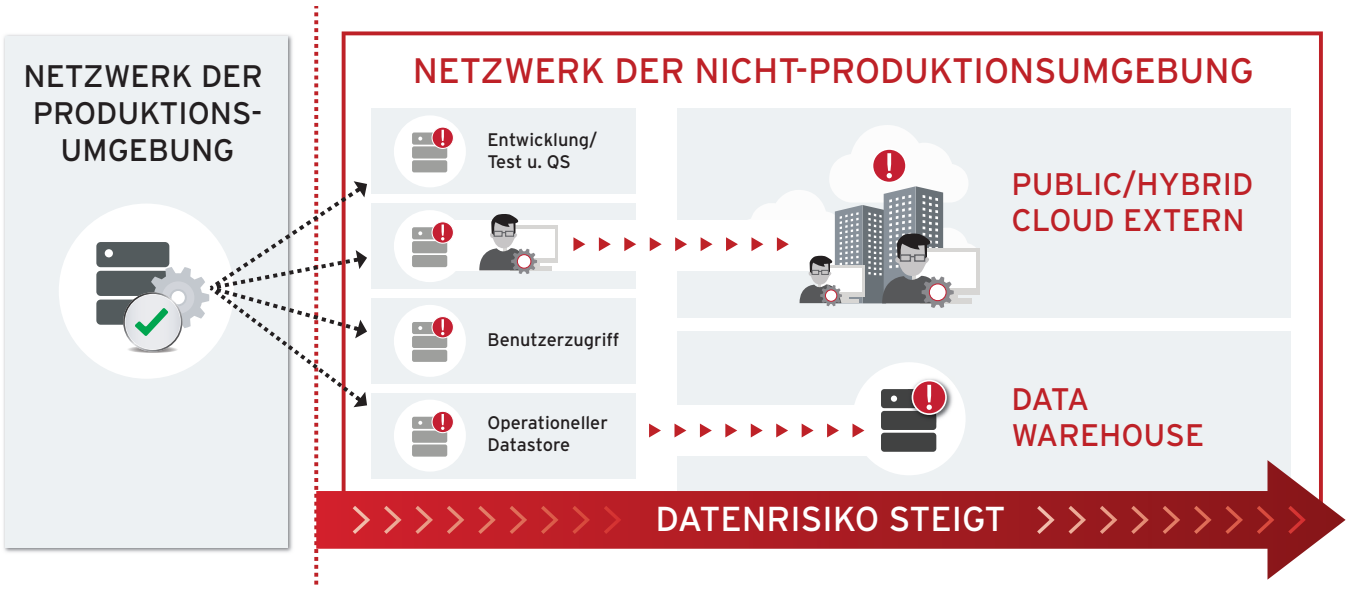
Der Gartner-Report aus Dezember 2015, „Magic Quadrant for Data Masking Technology, Worldwide", bietet ein Beispiel dafür, wie Data Masking in Verbindung mit Delphix Data Virtualization zusätzliche Vorteile mit sich bringt:

„Die Kombination von Data Masking mit Datenvirtualisierung spart Zeit und Speicher. Die Daten werden nur einmal in virtualisierten (gemeinsam genutzten) Daten sowie in geänderten Daten verfremdet, während die Einsparungen beim Storage bewahrt bleiben. Mit der Datenvirtualisierungstechnologie kann auch Zeit gespart werden, indem Kopien der verfremdeten Daten gespeichert und auf Anforderung bereitgestellt werden."

Was hat es also mit Delphix auf sich und wie wird ein „Daten zuerst"-Ansatz umgesetzt, um einen Prozess, der bisher langsam, unvernetzt, aufwendig und teuer war, in ein automatisches, zentralisiertes, schnelles und effizientes Verfahren zu verwandeln?

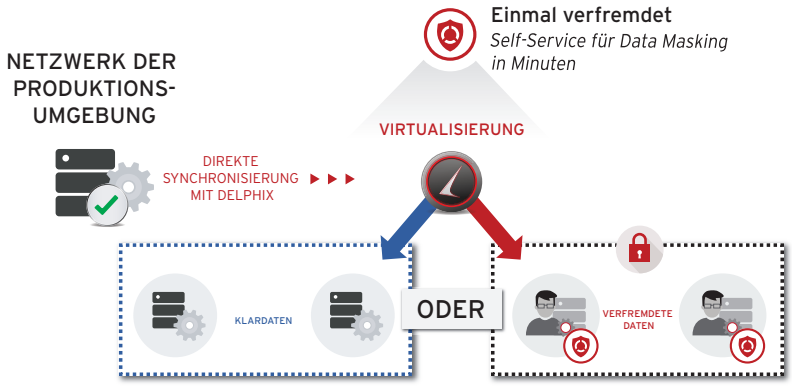
Eine jüngst von Delphix in Auftrag gegebene Studie zeigte, dass 90 % der Nicht-Produktionsdaten im Unternehmen nicht verfremdet sind. Grund dafür ist, dass das Kopieren der Daten von der Produktion in den Nicht-Produktionsbereich Wochen oder sogar Monate dauern kann. Das Verfremden dieser Daten kann weitere Wochen in Anspruch nehmen und danach müssen die Daten gegebenenfalls mehrere Male in Projekten aktualisiert werden, wobei der Prozess immer wieder von neuem beginnt.

WENN DATEN IN DEN NICHT-PRODUKTIONSBEREICH ODER WENIGER SICHERE NETZWERKE WANDERN, INSBESONDERE AN EXTERNE STANDORTE BEI DRITTANBIETERN ODER IN PUBLIC BZW. HYBRID CLOUDS, VERÄNDERN SIE SICH LAUFEND UND DIE ANGRIFFSFLÄCHE FÜR RISIKEN NIMMT ZU.



Delphix sammelt Produktionsdaten und bleibt danach für immer mit der Produktion synchronisiert. Dadurch wird eine fast zeitgleiche Kopie der Produktionsdaten erstellt. Aus dieser Kopie erstellt Delphix komplette und aktuelle virtuelle Kopien der Daten über Self-Service binnen Minuten. Sie behalten die vollständige Kontrolle über alle Ihre Produktionsdaten. Da sie nur mit einer einzigen realen Kopie und nicht mit mehreren Hundert arbeiten, reduzieren Sie die Angriffsfläche für Eindringlinge. Sie wissen auch genau, wo virtuelle Kopien gespeichert sind, und wer darauf Zugriff hat. Damit erhalten Sie die so wichtige Kontrolle und Steuerung.

Gleichzeitig kann eine Data Masking-Richtlinie vorbereitet werden, sodass bei einer Anforderung virtueller Kopien eine sofortige Verfremdung eingeleitet wird. Data Masking wird damit einfach Teil des automatischen Datenbereitstellungsprozesses.



- Delphix stellt eine direkte Verknüpfung mit der Produktion her.
- Von Delphix bereitgestellte Daten können verfremdete oder Klardaten sein.
- Verschiedene Daten werden je nach Anwendungsfall oder Benutzerrolle bereitgestellt.

Der Datenschutz wird damit in den gesamten Lebenszyklus der Technologie eingebettet, von der frühen Entwurfsphase bis zur endgültigen Bereitstellung, Nutzung und endgültigen Vernichtung.

ZUSAMMENFASSUNG

Die Datenschutz-Grundverordnung der EU motiviert Unternehmen, alle personenbezogenen Daten zu pseudonymisieren. Um dafür bereit zu sein, benötigen Unternehmen mehr Transparenz und Kontrolle über ihre Daten in Verbindung mit Tools, die nicht nur Daten verfremden, sondern auch diesen Prozess verschlanken und automatisieren. Der Ansatz bietet folgende Vorteile für Unternehmen:

- Maßnahmen für den Schutz personenbezogener Daten in Übereinstimmung mit den Anforderungen der Datenschutz-Grundverordnung
- Vermeidung der Meldepflichten bei einer Verletzung des Schutzes personenbezogener Daten
- Bereitstellung von Tools, die es der Rechtsabteilung ermöglichen, Daten zu identifizieren, zu überprüfen und darüber Bericht zu erstatten
- Reduktion oder Eliminierung des Erfordernisses zur Einholung von Einwilligungen für das Daten-Profiling
- Beschleunigung der IT- und Geschäftsprozesse, die vom Zugang zu sicheren Daten abhängen

ÜBER DELPHIX

Daten sind der Treibstoff für Anwendungsprojekte und Delphix transformiert die Art, wie Unternehmen Daten für ihre Anwendungsprojekte verwalten. Delphix Masking integriert virtuelle Daten mit Data Masking nahtlos, um folgende Ergebnisse für Kunden zu bewirken:

- Verfremden von sensiblen Daten schneller als jemals zuvor
- Bereitstellung von sicheren Daten in Minuten anstelle von Tagen oder Wochen
- Sicherstellung der Einhaltung von Regelungen, einschließlich der Datenschutz-Grundverordnung

Weitere Informationen darüber, wie Delphix Sie dabei unterstützen kann, die Anforderungen der Datenschutz-Grundverordnung einzuhalten, finden Sie unter delphix.com/solutions/data-masking.

Anforderungen der Datenschutz-Grundverordnung für Data Masking Was die IT wissen und tun muss – März 2016

Weitere Informationen finden Sie unter www.delphix.com.

Auf der Delphix-Website finden Sie auch die neuesten Produkt-Updates.
Wenn Sie Kommentare zu dieser Dokumentation haben, senden Sie Ihr Feedback bitte an:
help@delphix.com

Delphix Corp.
275 Middlefield Road, Suite 210
Menlo Park, CA 94025