Unified Communications und die EU-DSGVO

UC-Software unterstützt Unternehmen beim Schutz der personenbezogenen Daten

Transparenz und Rechenschaftspflicht, Löschung und Anonymisierung, Datenminimierung, Integrität und Vertraulichkeit – das sind Schlagworte, die derzeit nahezu alle Unternehmen beschäftigen. Bis spätestens 25. Mai 2018 müssen Firmen die Richtlinien der EU-DSGVO umgesetzt haben, ansonsten drohen empfindliche Strafen. Eingesetzte Softwareprodukte wie Unified Communications Bausteine sollten die Betriebe bei der Einhaltung der DSGVO unterstützten.

Personenbezogene Daten in einer UC-Software

Grundsätzliches Ziel der EU-DSGVO ist der Schutz personenbezogener Daten. Personenbezogene Daten sind alle Daten, die sich direkt oder indirekt auf eine natürliche Person beziehen oder Rückschlüsse auf diese zulassen. Eine Unified Communications (UC) und CTI Software führt unterschiedlichste Kommunikationswege zusammen. Ziel ist es, die interne und externe Unternehmenskommunikation sowie Arbeitsprozesse zu optimieren, zu vereinfachen und effektiver zu gestalten. Messaging Funktionen wie E-Mail, Fax, Anrufbeantworter und SMS sowie Computer Telefonie (CTI) und Collaboration mit Anruferidentifikation, Instant Messaging, Präsenzmanagement, Screen Sharing und Audio/Video-Kommunikation werden unter einer Anwenderoberfläche zur Verfügung gestellt. Hier werden Personenbezogene Daten in unterschiedlichster Art und Weise verarbeitet und gegebenenfalls gespeichert. So wird beispielsweise eine Faxnachricht mit einer Absenderinformation ausgestattet, CTI benötigt zur Bereitstellung der Telefoniefunktionen mindestens eine Telefonnummer und Anrufer können nur dann identifiziert werden, wenn deren Kontakt anhand der eingehenden Telefonnummer aus einer unternehmensinternen oder externen Datenquelle ermittelt wird. Gespeichert werden personenbezogene Daten beispielsweise im Journal oder in den Logfiles.

Grundsätze und Pflichten der EU-DSGVO

Die wesentlichen Grundsätze und Pflichten der DSGVO zum Schutz der Personenbezogenen Daten, die für eine UC-Software relevant sind, lauten: Zweckbindung, Datenminimierung, Transparenz und Rechenschaftspflicht, Richtigkeit der Daten, Löschung und Anonymisierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit. Personenbezogene Daten dürfen für einen bestimmten Zweck genutzt, verarbeitet oder gespeichert werden. Sie müssen auf das für den Zweck nötige Maß

beschränkt sein. Auf Wunsch muss ein Unternehmen der betroffenen Person Auskunft darüber geben, wie deren Daten erhoben und in welcher Form sie gespeichert oder weiterverarbeitet werden. Sollten Daten falsch gespeichert sein, müssen diese korrigiert werden. Auf Wunsch müssen die Daten einer Person gelöscht oder anonymisiert werden, so dass keine Rückschlüsse mehr auf diese Person möglich sind. Personenbezogene Daten dürfen nur so lange wie nötig und nur so wenige wie möglich im Unternehmen vorgehalten werden. Darüber hinaus muss ein Unternehmen angemessene technisch-organisatorische Maßnahmen treffen, damit die personenbezogenen Daten nicht unrechtmäßig in die Hände von Dritten fallen. Sollte dies doch der Fall sein, müssen die Aufsichtsbehörde und die betroffenen Personen, mit wenigen Ausnahmen, unverzüglich informiert werden.

Zweckbindung und Datenminimierung

Zweckbindung wird von einer UC-Software automatisch erfüllt. Die personenbezogenen Daten werden im Hinblick auf bestimmte Funktionen verarbeitet oder gespeichert: Im UC-Client werden die Daten beispielsweise im Journal vorgehalten, so dass der Benutzer sieht, wer wann angerufen hat und welche Anrufe ihm entgangen sind. In den Favoriten speichert der Benutzer ausgewählte Kontakte, so dass er diese ohne Suchaufwand anrufen, via Instant Messaging anchatten oder per Audio/Video Chat kontakten kann. Der UC-Server wiederum greift auf die unternehmensinternen oder externen Datenquellen lediglich dann zu, wenn der Benutzer eine Suche gestartet hat oder ein Anruf eingeht. Der Benutzer erhält das Ergebnis entweder im UC-Client oder im Gesprächsfenster am Bildschirm. Die Informationen in Fax-, Sprach- oder Kurznachrichten werden zur Absenderkennung genutzt. Die in den Logfiles gespeicherten Daten dienen dem Administrator zur Fehlererkennung und -behebung. Darüber hinaus bietet eine UC-Software wie estos ProCall Enterprise eine Reihe von Möglichkeiten, die Verarbeitung personenbezogener Daten im Sinne der Datenminimierung von vorne herein soweit möglich einzuschränken: Je nach Information und Zweck dürfen nur bestimmte Personen auf bestimmte Daten zugreifen. Lediglich der Administrator darf auf Logfiles zugreifen. Die Benutzer vergeben ihren Kolleginnen und Kollegen und weiteren Kontakten Berechtigungen und bestimmen somit selbst, in wie weit ihre Daten minimiert werden. Sie ordnen diese vorkonfigurierten Gruppen zu, die jeweils unterschiedlich detaillierte Informationen sehen. Auch können sie individuelle Berechtigungen vergeben. Im UC-Monitor beispielsweise sehen die Kontakte gegenseitig Daten wie Telefon- oder Mobilnummer, E-Mail Adresse, Termine und Präsenzstatus. Hier kann der Einzelne Mitgliedern seiner Abteilung erlauben, zu sehen, mit wem er telefoniert, während die anderen lediglich erfahren, dass er im Gespräch ist. Kennzeichnet er private Telefonate, werden diese grundsätzlich nicht angezeigt.

Rechenschaftspflicht, Richtigkeit, Löschung und Speicherbegrenzung

Herauszufinden, welche Daten einer Person wo gespeichert, wie erhoben und in welcher Form weiterverarbeitet werden, also der Transparenz und Rechenschaftspflicht nachzukommen, stellt eine weitere Herausforderung dar. Eine UC-Software liefert in den Suchergebnissen im UC-Client oder im Gesprächsfenster die Datenquelle mit, in der die Informationen gespeichert sind. Allerdings ist es mühselig, sich diese einzeln auf diese Art zusammen zu suchen. Eine UC-Software wie ProCall Enterprise von estos liefert hier ein praktisches Tool mit: Alle in der Software verarbeiteten und gespeicherten Daten inklusive Datenquellen werden übersichtlich dargestellt. Auf dieser Grundlage kann ein Unternehmen weitere Recherchen betreiben und qualifiziert Auskunft über Erhebung, Verarbeitung und Speicherung der Daten geben. Stellt die Person fest, dass ihre Daten nicht korrekt sind, muss das Unternehmen diese bereinigen. Je zentraler die Datenhaltung ist, desto einfacher ist es, die Richtigkeit der Daten zu gewährleisten. Verfügt die Software über eine zentrale Verwaltung, genügt es, die Daten an einer Stelle zu verbessern. Die Änderungen wirken sich in der gesamten Software aus. Daten, die nicht in der UC-Software gespeichert sind, müssen entsprechend in der externen Datenquelle, beispielsweise einer Telefonbuch-CD oder der Datenbank des Unternehmens, berichtigt werden. Nur so kann gewährleistet werden, dass die falschen Informationen nicht an weiteren oder unvorhergesehenen Stellen auftauchen Gleiches gilt für den Grundsatz der Löschung und Anonymisierung: Fordert eine Person die Löschung ihrer Daten, dürfen diese nicht mehr in Zusammenhang mit ihr auftauchen oder in Verbindung gebracht werden. Die zentrale Verwaltung einer UC-Software sorgt dafür, dass die Änderungen wie Löschung oder Anonymisierung einmal vorgenommen in der gesamten Software wirken. Personenbezogene Daten, die die UC-Software aus externen Quellen bezieht, müssen hier bereinigt werden. Erstellt eine UC-Software einen Report über verarbeitete und gespeicherte Daten inklusive Angaben der Quellen, sieht das Unternehmen den jeweiligen originalen Speicherort und kann entsprechend handeln. Zusätzlich hilfreich ist es, wenn gespeicherte Daten automatisch dann gelöscht werden, wenn sie nicht mehr benötigt werden. In den Logfiles oder im Journal werden beispielsweise personenbezogene Daten zur Fehlerbehebung gespeichert. Hat der Administrator das Problem gelöst, gibt es keinen Grund mehr, die Daten vorzuhalten. Um dem Grundsatz der Speicherbegrenzung Rechnung zu tragen, ist in einer UC-Software ein angemessener Zeitraum voreingestellt, nachdem die Daten automatisch gelöscht oder anonymisiert werden Der Administrator kann diesen Zeitraum bei Installation oder jederzeit den Bedürfnissen eines Unternehmens gemäß den eigenen Möglichkeiten anpassen.

Integrität und Vertraulichkeit

Sicherheitskonzepte in Unternehmen mit Firewall, Verschlüsselung, Authentifizierung und Berechtigungsvergaben schützen vor Datenklau und Datenpannen. Damit der Grundsatz der Integrität und Vertraulichkeit auch im Hinblick auf die UC-Software eingehalten wird, muss diese in das jeweilige Konzept eingebunden werden. Eine Firewall schützt das interne Firmennetzwerk vor externen Angriffen und prüft anhand bestimmter Regeln, welche Daten durchgelassen werden. Können die Komponenten einer UC-Software wie die des ixi-UMS Unified Messaging Servers von estos sinnvoll entkoppelt werden, sind die UM-Komponenten, über die der Zugriff in das externe Netzwerk erfolgt, auf der einen, und diejenigen, die intern für die Integration in die IT sorgen, auf der anderen Seite der Firewall installiert. Für die Audio/Video-Kommunikation und den Chat mit Kunden oder Lieferanten bietet TLS-Verschlüsselung Sicherheit: Peer-to-Peer Verbindungen sowie Instant Messages werden so geschützt. Darüber hinaus empfiehlt es sich, ein Complianceverfahren im Sinne von Authentifizierung einzusetzen: Mittels Challenge Response beispielsweise kann der UC-Benutzer Kontaktanfragen annehmen oder ablehnen. Unterschiedliche Berechtigungsstufen ermöglichen es unter anderem, den Zugriff externer Mitarbeiter auf Kontakte im Firmennetzwerk auf die Beruflichen zu beschränken.

Fazit

Unified Communications Software verbessert die Kommunikation und Zusammenarbeit im Unternehmen und über Unternehmensgrenzen hinweg. Als ein Baustein in der ITK-Struktur des Unternehmens ist sie ebenfalls ein Baustein auf dem Weg zur EU-DSGVO Konformität. Erfüllt die UC-Software die Grundsätze und Richtlinien und bietet praktische Tools zur Recherche von personenbezogenen Daten, erleichtert sie dem Unternehmen den Weg zur Umsetzung der Kriterien der Europäischen Datenschutzgrundverordnung.