ZfK ZEITUNG FÜR KOMMUNALE WIRTSCHAFT
VKU Verlag München/Berlin
Redaktion: Neumarkter Str. 87
81673 München
Ausgabe 01/19, Seite 10

Anonym im Testsystem

DSGVO Wie lassen sich Kundendaten in Testsystemen datenschutzkonform verwenden? Cronos hat dazu eine eigene Lösung entwickelt

Volker Schwalm, Münster

Der Umgang mit produktiven Kundendaten in SAP »Testsystemen« steht bei vielen Unternehmen bislang nicht im Vordergrund. Jetzt kommt das Thema mit der Datenschutzgrundverordnung (DSGVO) neu auf den Tisch und wirft die Frage auf, warum sich die Energiewirtschaft damit bisher so schwer tut und welche Lösungen es gibt.

Betroffenenrechte | Für den Umgang mit Kundendaten in Testsystemen gibt es zwei datenschutzrechtliche Anforderungen: zum einen die Wahrung der konkreten Betroffenenrechte, zum anderen eine etwas abstraktere Anforderung, die neudeutsch als Privacy by Design bezeichnet wird.

In Bezug auf die Betroffenenrechte ist die rechtliche Lage schnell umrissen: Mit Abschluss eines Vertrages, der Erteilung eines Opt-ins oder einer anderen expliziten Zustimmung des Kunden hat dieser der produktiven Nutzung seiner Daten zugestimmt.

Ob damit auch implizit die Nutzung der Daten für Testzwecke abgedeckt ist, wird unterschiedlich beurteilt. Für die einen Betrachter ergibt sich die Zustimmung zur Nutzung für IT-Tests aus der Sache heraus, weil ohne Systemtests keine zuverlässige Datenverarbeitung möglich ist. Kritischere Stimmen verweisen auf die fehlende explizite Zustimmung, die rechtlich eigentlich einzufordern wäre. Daher bauen viele Versorger entsprechende Ergänzungsklauseln in ihre Standardvertragsbedingungen ein, die dann auch für Bestandskunden zur Zustimmung gebracht werden müssen.

Privacy by Design | Wenn nun ausschließlich die eigenen produktiven Mitarbeiter auf die Testsysteme (oder Konsolidierungs-/Qualitätssicherungssysteme – je nach Namensgebung) Zugriff hätten, wäre damit den Anforderungen der DSGVO Genüge getan. Allerdings tummeln sich auf den nicht-produktiven Systemen auch Berater oder andere Systemnutzer, die möglicherweise auch am Berechtigungswesen vorbei auf Daten zugreifen können – beispielsweise über die Programmierung. Hier greift ergänzend die Verpflichtung zum Privacy by Design: Unternehmen müssen von sich aus ihre IT-Systeme so auslegen, dass Datenschutzverletzungen schon per Systemdesign möglichst erschwert oder sogar verhindert werden.

Durcheinandergewürfelt: *Aus Christian Meier kann mit dem Cronos-Verfahren ein Thomas Schmidt werden, dessen Identität sich nicht mehr zurückverfolgen lässt.*

Schutz von Daten auf Testsystemen | Für die Umsetzung dieser Anforderungen gibt es in der SAP-Welt auch etablierte Verfahren:

- Einsatz von Datenextrakten: Es werden nur selektiv Daten von den Produktionssystemen auf die Qualitätssicherungssysteme gespiegelt.
- Einsatz künstlicher Daten.

Trotzdem haben bisher nur wenige Unternehmen wirklich konsequent versucht, ihre Testsysteme, den datenschutzrechtlichen Vorgaben entsprechend, zu schützen. Wesentlicher Grund ist – neben bislang fehlendem Handlungsdruck – die mangelnde Praxistauglichkeit der etablierten Standardverfahren im speziellen Kontext der Energiewirtschaft.

Der Einsatz eines Teildatenbestandes auf den Qualitätssicherungssystemen hat sich schon deswegen bei Versorgern nicht durchgesetzt, weil es sehr schwierig ist, einen repräsentativen Datenbestand für die Tests zu definieren. Aufgrund der sich ändernden regulatorischen Anforderungen müsste die Bestimmung eines Satzes von aussagefähigen Testdaten für jeden Prozesstest erneut erfolgen.

Der Einsatz künstlicher Daten konnte sich wiederum – wenn überhaupt – nur über Entwicklungstests durchsetzen. Für prozesshafte Abnahmetests seitens der Fachbereiche ist es jedoch unabdingbar, echte Konstrukte zu Tests heranzuziehen,

weil sich nur anhand realer Konstellationen das Soll-Verhalten im Produktivsystem mit hinreichender Genauigkeit im Testsystem nachbilden und prüfen lässt.

Praxistauglichkeit | Vor diesem Hintergrund hat Cronos ein neues Verfahren zur Anonymisierung von Testdaten in SAP-Systemen entwickelt. Das Vorgehen beruht auf einer klassischen vollständigen Kopie der Produktionsdaten (Systemspiegelung), mit dem Unterschied, dass die darin enthaltenen personenbezogenen Daten (Echtkundendaten) nach erfolgter Systemspiegelung verfremdet werden. Dazu wurde ein spezielles Verwürfelungsverfahren konzipiert und implementiert.

Verwürfelung als Lösung | Der wesentliche Vorteil ist hier, dass auf Basis der im SAP-System vorhandenen Daten nicht auf die Identität des Echtkunden geschlossen werden kann – die Anonymisierung ist daher DSGVO-konform. Der Clou: Aus Sicht der testenden Fachbereiche und Entwickler fühlen sich die verfremdeten Daten echt an. Die Daten sehen aus wie die von echten Kunden und verhalten sich auch so. Da es sich um originär echte Datenobjekte handelt, sind diese für Tests genauso repräsentativ wie die unverfälschten Originaldaten.

Funktionsweise im Detail | Das Verfahren ist einfach: Aus den Quellsystemen wird der Satz der existierenden Vor- und Nachnamen ermittelt und dann durch andere Namen ausgetauscht. Im Detail wird sichergestellt, dass gleiche Namen auf gleiche Namen abgebildet werden und insofern auch Dubletten als solche erhalten bleiben. Integrierte statistische Analysen stellen sicher, dass häufige Namen durch andere häufige Namen ersetzt werden, um den Datenbestand in der Gesamtheit repräsentativ zu halten. Auch werden juristische Personen standardmäßig von der Verfremdung ausgeschlossen, da sie nicht von der DSGVO betroffen sind – in der Folge sind spezielle, oftmals in komplexer Form abgebildete Vertragspartner wie Stadtverwaltungen von der Verwürfelung ausgenommen.

Abgedeckt werden die typischen schützenswerten personenbezogenen Daten: Name, E-Mail-Adressen und andere Kontaktinformationen wie Telefonnummern oder Bankverbindungen. Die Beziehungen zu verknüpften Dokumenten wie Rechnungsdrucke werden gekappt. Darüber hinaus erfolgt die Verwürfelung vollhistorisch auch unter Berücksichtigung von Zeitscheiben und Änderungsbelegen, sodass weder für einen kundigen Anwender, noch für ein Software-Programm die ursprünglichen Daten rekonstruierbar wären.

Einsatz in Systemlandschaften | Im Rahmen eines isolierten SAP-IS-U-Systems lässt sich eine solche Verfremdung ohne große weitere Überlegungen einfach ausrollen. In komplexeren Systemlandschaften ist zusätzlich das Zusammenspiel der verschiedenen IT-Systeme zu berücksichtigen. In der Cronos-Lösung wurde hier vorgedacht: So kann das Verwürfelungsverfahren auf mehreren SAP-Systemen parallel und synchron zum Einsatz kommen. Das führt in Verbindung mit SAP-Standardmechanismen dazu, dass ein Originalname SAP-übergreifend sowohl im IS-U-Vertriebssystem, in dem über die Marktkommunikation angebundenen IS-U-Netzsystem sowie in angeflanschten CRM-Systemen und im nachgelagerten BW-System, überall durch den gleichen anonymisierten Zielnamen ausgetauscht wird.

Kundeneigene Testverfahren | Diese SAP-systemübergreifende Konsistenz ist eine zentrale Vorbedingung für funktionierende Prozesstests. Im Rahmen eines Kundenprojektes müssen gegebenenfalls aber auch noch dritte angebundene IT-Systeme betrachtet werden, was jedoch individuell im Rahmen eines Projektes erfolgen muss. Übergeordnetes Ziel von Cronos in der Konzeptionsphase ist es immer, die bestehenden Testverfahren der Kunden möglichst unangetastet zu lassen, denn diese sind der wichtigste Garant für stabile Prozesse im laufenden Betrieb. Den Werkzeugen kommt dann die Aufgabe zu, im Hintergrund möglichst unauffällig für eine DSGVO-konforme Datengrundlage auf den Testsystemen zu sorgen.

Volker Schwalm ist Bereichsleiter bei der Cronos Unternehmensberatung GmbH.