iBite
Information-Bites by isacon AG

Rechtssicher testen mit personenbezogen Daten

- PyAno als Lösungsansatz -

Mit der am 25. Mai 2018 in Kraft getretenen EU-Datenschutz-Grundverordnung (EU-DSGVO), erhöhten sich die datenschutzrechtlichen Anforderungen im Umgang mit personenbezogenen Daten. Die Sanktion in Höhe einer Strafzahlung von 4% des Jahresumsatzes gibt umso mehr Anlass bei der Implementierung von IT-Systemen und Datenbanken den Datenschutz zu beachten. Wie verhält es sich allerdings, wenn das Unternehmen im Rahmen von Software-, Komponenten- oder Integrationstests auf Daten zurückgreifen muss, die einen Personenbezug zulassen?

Im Folgenden soll der rechtliche Rahmen, die Grundsätze sowie mögliche Lösungsansätze beleuchtet werden.

Testdaten im rechtlichen Kontext

Personenbezogene Daten dürfen nach dem Art. 5 EU-DSGVO grundsätzlich nur „...für festgelegte, eindeutige und legitime Zwecke erhoben werden.“ (Zweckbindung). Diese Zweckbindung folgt dem Leitsatz der Datenminimierung mit dem Ziel so wenig wie möglich personenbezogene Daten zu erheben, verarbeiten und zu nutzen.
Daraus folgt unmittelbar, dass die Verwendung personenbezogener Echtdaten ohne Beachtung des Datenschutzes rechtswidrig ist.

Demnach hat die EU-DSGVO in einer IT-Systemlandschaft sowohl im Produktiv- als auch im Testsystem Anwendung zu finden. Die Nutzung von Echtdaten zu Testzwecken stellt eine Zweckdurchbrechung dar, da diese grundsätzlich zunächst für den entsprechenden Geschäftsvorgang des Unternehmens erfasst wurden.

Eine Möglichkeit zur Verwendung von Echtdaten zu Testzwecken bedürfte also einer zweckgebundenen Einwilligung. Die Gesetzgebung nimmt die Unternehmen auch in die Pflicht zu gewährleisten, dass personenbezogene Daten bei der Nutzung, Verarbeitung und Speicherung nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle). Kontextbezogen problematisch ist, dass auf Test- und Entwicklungsumgebungen in der Regel mit Entwicklern, Testern oder externen Beratern wesentlich mehr Personen Zugriff haben als es im Livesystem der Fall ist.

Des Weiteren besteht je nach Testverfahren und –umgebung die Gefahr, dass durch einen Systemfehler sensitive Echtdaten wie Kreditkarten- oder Kontodaten an unbefugte Dritte übermittelt werden (Datensicherheit). Das Testen mit Echtdaten muss demnach auch unter dem Aspekt der Datensicherheit als unzulässig bewertet werden. Neben der in Artikel 33 der EU-DSGVO erwähnten innerhalb von 72h einzuhaltenden Meldepflicht gegenüber der Aufsichtsbehörde und dem Betroffenen, ist vielmehr auch das mit dem Reputationsschaden einhergehende Risiko für das Unternehmen nicht zu vernachlässigen.

Ausnahmeregelung

Die EU-DSGVO eröffnet mit Artikel 6 Abs. 6 eine Ausnahmeregelung für eine Datenverarbeitung im Falle einer nicht im Sinne dieses Zweckes vorliegenden Einwilligung zur Verarbeitung. Hierbei wird „…das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören“ gefordert.

Damit bietet die EU-DSGVO als Lösung für Softwaretests ausdrücklich die Pseudonymisierung an. Die sogenannten Erwägungsgründe – von dem Europäischen Parlament aufgestellten Ziele, die mit der DSGVO erreicht werden sollen - erwähnen im Rahmen pseudonymisierter Daten explizit auch anonymisierte. Auf Letztere findet die DSGVO explizit keine Anwendung.

Begriffsabgrenzung: Pseudonymisierung und Anonymisierung

Anonymisierung und Pseudonymisierung sind zunächst beides Verfahren, die es Dritten erschweren sollen Personenbezüge aus Daten abzuleiten.

Die Pseudonymisierung ordnet einem personenbezogenen Datum ein Pseudonym in Form eines Codes oder einer ID zu. Vergleichbar wäre dies mit der Matrikelnummer von Studierenden.
Eine Zuordnung von Pseudonym zu natürlichen Personen ist allerdings anhand einer Masterliste weiterhin möglich. Diese Masterliste sollte daher durch geeignete technische und organisatorische Maßnahmen geschützt werden. Denn wer Zugriff auf die Masterliste hat, kann den Personenbezug wiederherstellen.
Im Falle einer Datenpanne ist der Personenbezug für Dritte demnach nur mit erheblichem technischem und zeitlichem Aufwand zu ermitteln. Sie fallen demnach weiterhin in den Anwendungsbereich der EU-DSGVO. Jedoch wird das Datenschutzrisiko einhergehend mit einer Meldepflicht signifikant minimiert.

Bei der Anonymisierung existiert keine Masterliste und ein Rückschluss von anonymisierten Daten auf eine echte Person ist lediglich mit unverhältnismäßigem Aufwand hinsichtlich Zeit, Technik und Arbeitskraft möglich. Sie fallen demnach nicht mehr in den Anwendungsbereich der EU-DSGVO.
Der Begriff des unverhältnismäßigen Aufwands wird jedoch zukünftig vor dem Hintergrund technologischer Entwicklungen und zunehmender Rechnerleistungen stets aufs Neue zu bewerten sein.

Wie kann PyAno Sie dabei unterstützen DSGVO-konform zu testen ?

PyAno ermöglicht es sensible und personenbezogene Daten zu anonymisieren oder zu pseudonymisieren und damit – unabhängig ob in SAP oder einer anderen Umgebung – DSGVO-konform zu testen. Der Verfremdungsgrad kann individuell bestimmt werden. Anhand eines Regelwerks können Sie definieren, welche Daten auf welche Weise anonymisiert werden. Das Regelwerk kann kundenindividuell mittels Customizing und Erweiterungen angepasst werden. In einer SAP-Umgebung stehen Anonymisierungs-funktionen für Namen und Adressen der Geschäftspartner zur Verfügung.
Tabellenbeziehungen und die Feldbeziehungen können entsprechend gepflegt werden, damit die Datenkonsistenz gewahrt bleibt. Persönliche Daten sind vollständig geschützt, und der Datensatz wird den Anforderungen der EU-DSGVO gerecht. Mit den anonymisierten Daten können Entwickler oder Tester bedenkenlos auf Entwicklungs- oder Testsysteme zugreifen. Da die referentielle Integrität gewährleistet bleibt, können Analysen und Testszenarien durchgeführt werden.

Die Vorteile im Überblick:

- Datensicherheit und Datenschutz: Mit PyAno anonymisierte Daten schützen vor Datenmissbrauch auf Testumgebungen.
- „Sprechende Daten“: Die verfremdeten Daten sind realitätsgetreu und nicht kürzel- oder codebasiert und vermitteln so den Eindruck Echtdaten sein zu können.
- Realistische Tests: Die anonymisierten Daten sind logisch korrekt und widerspruchsfrei und somit konsistent.
- Plattformunabhängig: Funktioniert im SAP-Systemumfeld als auch auf allen gängigen Datenbanksystemen.
- Rechtemanagement: Komplexe Zugriffs- und Berechtigungsprüfungen auf den Testsystemen können für die Tester vereinfacht werden. Die Daten sind dank PyAno für alle einsehbar.

Unsere Experten helfen Ihnen weiter!

Sie haben weitergehende Fragen rund um das Thema Datenschutz und PyAno oder zum Service- und Produktangebot der isacon AG? Kontaktieren Sie gerne unseren Experten oder besuchen Sie uns auf www.isacon.com.

Milan Dosenovic

milan.dosenovic@isacon.com

+49 (6201) 256 650

isacon AG
Bergstraße 49 / 69469 Weinheim