EU-DSGVO ist mehr als Double-Opt-In Lösungsansätze für weitere kritische Handlungsfelder

Die EU-DSGVO greift in wenigen Wochen, wirklich vorbereitet ist laut einer aktuellen DSAG-Studie allerdings nur ein einstelliger Prozentsatz der befragten Unternehmen*.

Viele offensichtliche Themen wie Double-Opt-In oder das Recht auf Auskunft sind x-fach in unterschiedlichsten Veröffentlichungen thematisiert, mit unterschiedlichsten Ansätzen, wie darauf reagiert werden sollte oder könnte.

Doch es gibt weitere – jedoch weniger beachtete – kritische Handlungsfelder. Zu diesen zählen unter anderem das **Recht auf Vergessenwerden (Art. 17)** und die **Sicherheit der Verarbeitung (Art. 32),** die sich wiederum auf die **Sicherstellung der Schutzziele** wie etwa Vertraulichkeit, Integrität und Verfügbarkeit auffächert.

Jede Person hat also das Recht, in einem angemessenen zeitlichen Rahmen zu erfahren, welche Daten zu welchem Zweck in Unternehmensdatenbanken gespeichert sind. Mit einem ordentlichen Datenmodell und geeigneten Abfragen oder Tools lässt sich dies auch wunderbar beantworten. So weit, so gut.

Jederzeit auskunftsbereit – Verfügbarkeit personenbezogener Daten

Doch wie kommen Sie an die Daten, wenn das System zu einem denkbar ungünstigen Zeitpunkt nicht verfügbar ist? Was, wenn aufgrund eines erzwungenen Restore eines Einzelsystems Daten plötzlich inkonsistent zu anderen Systemen sind?

Im Falle eines Falles greift Libelle **Business***Shadow,* eine Lösung, die Verfügbarkeits- und Disaster-Szenarien auf logischer Ebene abbildet. Der Vorteil: Nicht nur RPO und RTO, sondern speziell auch die RCO (Recovery Consistency Objective) sorgen dafür, dass Unternehmen sehr schnell mit konsistenten Datenbeständen wieder umfassend aussagefähig sind.

Löschen/Sperren personenbezogener Daten – Recht auf Vergessenwerden

Was, wenn Personen darüber hinaus von ihrem Recht auf Vergessenwerden Gebrauch machen möchten?

Besteht keine laufende Geschäftsbeziehung mehr, dürfen personenbezogene Daten auch nicht mehr im System gespeichert sein. Dem gegenüber stehen die gesetzlichen Aufbewahrungspflichten, für die auch abgeschlossene Geschäftsbeziehungen nachverfolgbar vorgehalten werden müssen. Ein Dilemma.

Abhilfe kann ein spezieller **Datentresor** schaffen, der im Libelle Toolset **Master Data Services Suite (MDSS)** enthalten ist. In diesem werden solche Stammdaten gelagert, deren Lebenszyklus aus DSGVO-Sicht beendet ist, sowohl regelmäßig automatisch ermittelt als auch explizit getriggert. In den Produktivdaten wird lediglich ein Lösch-/Sperrhinweis zu sehen sein, während die Echtdaten im Datentresor nur noch für Personen mit darüber hinausgehendem berechtigten Interesse verfügbar sind.

Testdaten anonymisieren – Vertraulichkeit personenbezogener Daten

Neben dem Recht auf Vergessenwerden ist auch das Thema Zweckgebundenheit personenbezogener Daten im Fokus. Es dürfen nur solche Daten verarbeitet werden, die für den konkreten geschäftlichen Zweck benötigt werden, und auch nur von einem berechtigten Personenkreis. Für Produktivumgebungen ist dies eine prozessuale/organisatorische Frage und Thema des Berechtigungswesens. Doch wie sieht es mit nicht-produktiven Umgebungen aus?

In der Praxis werden Q-/Projekt-/Schulungssysteme oft mit Systemkopien aktualisiert. Ergo: Echtdaten landen in nicht-produktiven Umgebungen. Somit hat eine Vielzahl nicht-berechtigter Personen (Entwickler, Berater, Admins) Zugriff auf diese. Vielleicht nicht tagesaktuell, aber doch ganz klar personenbezogen. Möglichkeiten, den unberechtigten Zugriff einzuschränken: entweder ein umfassendes Berechtigungskonzept analog der Produktivumgebungen, das häufig dem Einsatzzweck nicht-produktiver Umgebungen widerspricht. Oder dafür sorgen, dass personenbezogene Echtdaten zu dem werden, was diese Systeme tatsächlich brauchen: Testdaten.

Das Mittel der Wahl ist hierfür die **Anonymisierung der Echtdaten,** so dass diese keinen konkreten Personenbezug mehr besitzen, trotzdem realistisch und vor allem nicht mehr rückführbar sind.

Ein pragmatisch und schnell umsetzbarer Ansatz im Sinne der EU-DSGVO gelingt mit Libelle **Data***Masking* (LDM), einem Tool, das Daten auf nicht-produktiven Systemen und Systemlandschaften logisch konsistent anonymisiert. Somit können Geschäftsprozesse mit sinnvollen Testdaten nach Herzenslust Ende-zu-Ende durchgetestet werden.

www.libelle.com/dsgvo

Libelle AG
Gewerbestraße 42
70565 Stuttgart
Telefon: +49 711 78335-0
sales@libelle.com
www.libelle.com

* DSAG (2018, 7. Februar): Artikel „Die Zeit drängt". URL: https://www.dsag.de/dossier-datenschutz [17. April 2018].