Data Redact

Das Recht auf Vergessenwerden

Im Mai 2018 trat die EU-Datenschutz-Grundverordnung (DSGVO/engl. GDPR) in Kraft. Artikel 17 schreibt vor, dass Personen das Recht auf Löschung („Recht auf Vergessenwerden“) haben. Gemeint ist das Recht auf Löschung personenbezogener Daten und die Untersagung der Verarbeitung in bestimmten Fällen, wenn beispielsweise einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für den Zweck, für den sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein, und es liegt kein vorrangiger berechtigter Grund für die weitere Verarbeitung vor.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet (d. h. es wurde anderweitig gegen die DSGVO verstoßen).

Unternehmen, die in ihren Systemen personenbezogene Daten speichern, haben nun verschiedene Möglichkeiten. So können sie beispielsweise:

- Das Recht auf Vergessenwerden verweigern (unter Verweis auf einen rechtlichen Standpunkt für diese Sichtweise)
- Daten auf Antrag löschen.
- Aufbewahrungszeiträume mit regelmäßiger Löschung definieren

Was ist Data Redact?

Mit Data Redact können Unternehmen sensible oder personenbezogene Daten verfremden, ohne ganze Datensätze zu löschen. Der Vorgang ist dadurch vereinfacht.

Bei aktuellen, am Markt verfügbaren Produkten wird der Zugriff zur Verarbeitung durch Berechtigungen blockiert oder dauerhaft archiviert. Dies sind allerdings keine effizienten Lösungen für Unternehmen, um die Compliance-Anforderungen der DSGVO zu erfüllen.

Data Redact ist eine Fiori-App, die das Produkt Data Disclose zum Suchen und Abrufen personenbezogener Daten ergänzt. Mit dieser komplementären Applikation lassen sich die abgerufenen Daten so verfremden, dass sie nicht mehr identifiziert werden können. Weil die Daten nicht mehr zu Identifikationszwecken verfügbar sind, erfüllen Sie die gesetzlichen Bestimmungen und das Recht auf Vergessenwerden. Die Informationen liegen aber weiterhin im System, und Sie können wie gewohnt Reports erstellen – auch wenn die entsprechenden Daten verfremdet wurden.

So funktioniert die Lösung:

1

Datensätze werden mit Data Disclose oder Data Retain ermittelt und für die Verfremdung freigegeben.

2

Durch eine separate Benutzerrolle werden die freigegebenen Datensätze nochmals geprüft und die Datenverfremdung wird in Echtzeit ausgeführt.

3

Die Daten werden für einem Monat in einem Audit-Protokoll vorgehalten, bis sie dann automatisch gelöscht werden.

vertrieb@epiuselabs.com | www.epiuselabs.com | T +49 6227 6 98 98 0