EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Neue EU-Datenschutz-Grundverordnung DSGVO / GDPR Übertragung in die Praxis

Fachartikel von Arne Vodegel, Sales Manager, IPG GmbH Deutschland

Die neue EU-Datenschutz-Grundverordnung (DSGVO) vereinheitlicht den Datenschutz personenbezogener Daten innerhalb der EU und ist in Kraft getreten. Dies löst bei vielen Unternehmen Handlungsbedarf aus. Denn in vielen Unternehmen mangelt es schon an den Grundvoraussetzungen für Datensicherheit. Es fehlt das umfassende und vollständige Wissen an welchen Stellen im Unternehmen sensitive Daten gehalten und von welchen Prozessen sie abgerufen werden. Eine granulare Differenzierung von Rollen und Berechtigungen für den Datenzugriff nach dem Need-to-know-Prinzip ist oft nicht durchgängig vorhanden. Diese Aufgabe ist bei Unternehmen mit vielen Niederlassungen, externen Mitarbeitenden oder Subunternehmern noch komplexer.

Lückenlose Datensicherheit und Transparenz in Bezug auf Datennutzung sind strikt einzuhalten. Auf die IT bezogen hat die DSGVO verschiedene Auswirkungen:

Haftung
Ihre Kunden haften für Datenpannen in Ihrem Unternehmen mit und wollen wissen, wie die anvertrauten Informationen kontrolliert werden. Ungenügender Datenschutz hat eine Ordnungsgeldbusse zur Folge.

Marktortprinzip
Die neuen Datenschutzgesetze auf Basis der DSGVO gelten für alle Datenverarbeiter auch ausserhalb der EU, wenn Daten von EU-Bürgern erhoben, verarbeitet oder gespeichert werden.

Datenschutz (Verlust)-Folgeabschätzungen
Ohne Risiko-Inventar geht nichts mehr. Die Rechenschaftspflicht besagt, dass Datenverarbeiter neu Folgeabschätzungen vor der Einführung einer Datenverarbeitung vorhalten müssen.

Datenschutz-Managementsystem (DSMS)
Ohne ein DSMS, ähnlich einem Informationsschutz-Managementsystem (ISMS), wird Datenschutz nur als lückenhaft in Einzelteilen vorhanden sein. Das reicht nicht. IPG kennt die Plan-Do-Check-Act (PDCA) Zyklen seit Jahren, jetzt ist es auch im Datenschutz «angekommen».

Ein sicheres Benutzer- und Zugriffsmanagement gewährleistet die Einhaltung der DSGVO
Fehlt Transparenz über Berechtigungen und Zugriffsmöglichkeiten auf Daten oder ist beispielsweise nicht bekannt, welche Anwender Daten verändern können, werden Risikominderungsmassnahmen in der Praxis nicht wirksam. Rechte müssen deshalb durchgängig in einer Identity Management und Identity Governance Lösung dynamisch verwaltbar und protokollierbar sein.

An dieser Stelle kann IPG, mit ihrer langjährigen Expertise und den speziellen Kompetenzen sowie dedizierten Partnerschaften, Unternehmen aller Branchen helfen. Die oben genannten Hinweise sind beispielsweise in jedem Identity Management System standardmäßig integriert. Herstellerabhängig bedarf es mehr oder weniger Konfigurationsaufwand.

Herausforderung Authentifizierung

Da die DSGVO Nachvollziehbarkeit im Umgang mit personenbezogenen Daten verlangt, besteht hoher Bedarf an einer zuverlässigen, durchgängigen Authentifizierung der Anwender. Zusätzlich müssen Anwender mit hohen Privilegien und Berechtigungen besonders geprüft werden. Eine Multi-Faktor- sowie Omni-Channel-Authentifizierung sollte genutzt werden, um den Zugriff auf die Zielsysteme auf Basis der Identität zu gewährleisten.

Multi-Faktor-Authentifizierung

Multi-Faktor-Authentifizierungen (MFA) kombinieren zwei oder mehr unabhängige Berechtigungsnachweise:

- Was der Anwender kennt (Passwort)
- Was der Anwender hat (Security Token)
- Was der Anwender ist (biometrische Verifizierung)

Das Ziel von MFA ist es, eine mehrschichtige Absicherung zu erschaffen. Unautorisierte Personen haben es so schwerer, auf ein Ziel, wie zum Beispiel einen physischen Standort, ein Computing-Gerät, ein Netzwerk oder eine Datenbank, Zugriff zu erlangen. Sollte ein Faktor kompromittiert oder kaputt sein, muss sich der Angreifer mit mindestens einer weiteren Barriere auseinandersetzen, um einen erfolgreichen Einbruch durchzuführen.

Omni-Channel-Authentifizierung

Durch die zunehmende Verbreitung von mobilen Endgeräten wurde der Begriff „Omni-Channel“ geschaffen. Kunden bekommen die Möglichkeit, egal auf welchem Gerät beispielsweise ein und dasselbe Angebot einer Marke über einen beliebigen Kanal (online, Social Media) zu verfolgen. Im Sinne der Authentifizierung geht es somit über den Multi-Faktor hinaus auf integrierte Infrastrukturen mit einheitlicher Sicht auf alle Angebote sowie Daten.

Die Akzeptanz für die eingesetzten Lösungen zur Authentifizierung steigt, wenn jederzeit berücksichtigt wird, dass Sicherheitsmechanismen von Kunden und Anwendern nicht oder kaum wahrgenommen werden sollen. Ziel ist daher neben der Verwaltung von Identitäten und dem Management von Zugriffen auch die Überwachung der Performance von Systemen und Applikationen und des gesamten Geschäftsprozesses.

Identity & Access Management als solide Basis

Identity & Access Management (IAM) findet, unter anderem aus oben genannten Gründen, immer grössere Verwendung. Zeitgleich wachsen auch die Anforderungen an die Funktionalität, die inzwischen mehr leisten muss als die blosse Absicherung. Eine erfolgreiche Lösung muss auch Kundenzufriedenheit garantieren (intern wie extern) und gleich mehrere Stufen und Plattformen entsprechend bedienen, ohne dabei den Endnutzer übermässig zu beanspruchen oder zu verschrecken. Dennoch sollten Unternehmen die Realisierung einer passenden IAM-Lösung als Top-Priorität ansehen.

Identity & Access Management unterstützt in der Einhaltung der DSGVO überall dort wo:

- Ein Risiko-Inventar erstellt wird und Schutzniveaus eine Rolle spielen (Art. 35/36)
- Zugriff und Verarbeitung auf schützenswerte Daten gesteuert und belegt werden müssen (Art. 5/32)
- Verarbeitungstätigkeiten geschützt und nachvollzogen werden müssen (Art. 30)
- Auftragsverarbeiter ihnen anvertraute Daten DSGVO-konform beherrschen und dies auch belegen müssen (Art. 28)

EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Wie unterstützt IPG?

Um IAM als solide Basis für die DSGVO / GDPR zu nutzen, unterstützt IPG mit verschiedenen Leistungen:

Advisory

Unser Advisory erarbeitet gemeinsam mit den Kunden die schrittweisen Herangehensweisen, so dass am Ende ein unternehminternes IAM-Handbuch vorliegt. Dieses kann wiederum mit dem Datenschutz zu einem Notfallhandbuch erweitert/umformuliert werden.

Integration

Wir unterstützen bei der Erarbeitung und Integration der IAM-Lösung und schaffen mit dem individuellen Betriebshandbuch die Grundlage für den erfolgreichen IAM-Betrieb. Gerade bei der weiter oben beschriebenen Omni-Channel-Authentifizierung spielt die Integration der Lösung eine wichtige Rolle. Welche Applikationen müssen mit welchen Kanälen verbunden werden? Welche Daten müssen wo abgespeichert werden? Wer darf am Ende über welche Kanäle mit welcher Authentifizierung auf welche Daten und/oder Applikationen zugreifen? Die Expertise der IPG zeigt sich jetzt im Zusammenspiel mit den unterschiedlichen Disziplinen – Advisory, Integration, Fachbereich, Datenschutz.

Operations

Operations hilft sofort bei Incidents, die meldepflichtig sind - ITSM ist auch hier als Standard bereits implementiert und fundamental.

Education

Education sensibilisiert gerne gemeinsam mit externen Datenschützern die Mitarbeitenden, so dass jeder genau weiss, warum Datenschutz für jedes Unternehmen überlebensnotwendig ist. Jeder Mitarbeitende kann und muss dazu beitragen.

Kontaktieren Sie uns und erfahren Sie mehr über IAM-Lösungen für die DSGVO / GDPR.

Markus Blaha: Sales Manager Austria
markus.blaha@ipg-group.com; Telefon +43 676 734 23 00

Christian Rückert: Sales Manager Germany
christian.rueckert@ipg-group.com; Telefon +49 170 908 03 53

Arne Vodegel: Sales Manager Germany
arne.vodegel@ipg-group.com; Telefon +49 170 908 04 32

Marcel Weber: Sales Manager Switzerland
marcel.weber@ipg-group.com; Telefon +41 79 907 84 47