imprivata OGITIX

RATGEBER

USER- UND RECHTE-MANAGEMENT IM KONTEXT DER EU-DSGVO

Die Datenschutz-Grundverordnung (EU-DSGVO) betrifft auch das sensible Umfeld der Verwaltung von Benutzerkonten und Zugriffsrechten. Wir erläutern für Sie die Handlungsfelder, deren Risiken und Lösungsansätze.

Inhaltsverzeichnis

1 Einleitung zur EU-DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Die Datenschutz-Grundverordnung gilt unmittelbar und einheitlich in allen EU-Mitgliedstaaten bereits seit dem 25. Mai 2016, am 25.05.2018 endet die Umsetzungsfrist.
Private Unternehmen und öffentliche Stellen sind somit verpflichtet, die Anforderungen der DSGVO bis spätestens zum 25. Mai 2018 umgesetzt zu haben.

Die EU-DSGVO findet Anwendung auf alle Rechtspersonen, unabhängig von ihrer Größe, Branche oder Rechtsform, sofern die Organisation personenbezogene Daten von Personen verarbeitet, die sich in der EU aufhalten. Somit betrifft die EU-DSGVO

- **Alle privaten und öffentlichen Organisationen in der EU, die personenbezogene Daten von Personen in der EU verarbeiten.**
- **Alle privaten und öffentlichen Organisationen außerhalb der EU, die personenbezogene Daten von Personen in der EU verarbeiten.**

2 Anforderungen der EU-DSGVO an das User- & Rechte-Management

Aber welche Auswirkungen hat die DSGVO konkret auf die Verwaltung von Benutzerkonten und Zugriffsrechten? **Um diese Frage zu beantworten, sind speziell die folgenden Artikelauszüge der DSGVO relevant, die wir im hier näher beleuchten:**

Art. 5 Abs. 1 Grundsätze für die Verarbeitung personenbezogener Daten

*...Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich **Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust**, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit")...*

Im Kontext des User- & Rechte Managements müssen Unternehmen und öffentliche Organisationen somit sicherstellen, dass nur befugte Personen Zugriff auf personenbezogene Daten haben und somit **nur befugte Personen über die entsprechenden Zugriffsrechte verfügen**.

Erfahrungsgemäß lässt sich diese Anforderung durch organisatorische Maßnahmen oder Insellösungen nicht ausreichend umsetzen. Die Komplexität entsteht durch häufige personelle und organisatorische Veränderungen sowie durch die Anzahl an Systemen und Applikationen. Diese Komplexität lässt sich nur über geeignete technische Lösungen zur Verwaltung von Benutzerkonten und Zugriffsrechten wie OGiTiX unimate beherrschen.

Art. 25 Abs. 2 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Security by Design)

*Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die **sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden**.*

Der Artikel 25 Absatz 2 wird für den Kontext des Managements von Zugriffsrechten konkreter und schreibt vor, dass der Zugriff auf personenbezogene Daten nicht dauerhaft bestimmten Personen gewährt oder verwehrt werden darf. Es muss vielmehr sichergestellt werden, dass der Zugriff für den jeweiligen Arbeitskontext erforderlich ist.

Eine prozesskonforme Verwaltung der Zugriffsrechte lässt sich durch die Umsetzung des Need-to-Know-Prinzips und des Least-Privilege-Prinzips umsetzen. Eine Durchsetzung dieser Prinzipien wird durch eine Identity & Access Management Lösung wie OGiTiX unimate ermöglicht.

Art. 5 Abs. 2 Rechenschaftspflicht

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Die Rechenschaftspflicht bedeutet generell nachweisen zu können, dass geeignete technische und organisatorische Maßnahmen umgesetzt wurden. Eine Dokumentation der Prozesse & Richtlinien dient als Grundlage, reicht aber als Nachweis nicht aus. Vielmehr muss nachgewiesen werden, dass die Prozesse und Richtlinien bspw. für die Vergabe von Zugriffsrechten auch tatsächlich in der Praxis eingehalten werden.

Jeder einzelne Vorgang muss lückenlos nachvollziehbar sein. Die Fragen: „Wer hatte wann welche Rechte?“ und „Von wem wurden diese beantragt, vergeben und genehmigt?“ müssen jederzeit beantwortet werden können. Auch an dieser Stelle lässt sich festhalten, dass nur eine technisch übergreifende Lösung mit lückenloser Protokollierung die Rechenschaftspflicht mit vertretbarem Aufwand bewerkstelligen lässt.

Zwar nimmt die DSGVO keinen direkten Bezug auf die Funktionen und die Notwendigkeit eines Identity & Access Management-Systems, aber die Notwendigkeit eines solchen Systems zur Sicherstellung der Konformität mit der EU-DSGVO erschließt sich letztendlich aus der Logik der einzelnen Anforderungen.

Im Folgenden geben wir Ihnen einen Überblick über die wichtigsten DSGVO Herausforderungen im der Berechtigungsverwaltung und zeigen Ihnen auf mit welchen Funktionen einer Identity & Access Management-Lösung am Beispiel von OGiTiX unimate Sie diese Herausforderungen lösen können.

3 Die wichtigsten Handlungsfelder und Lösungsansätze

OGiTiX unimate unterstützt als Identity & Access Management Lösung sowohl die IT, die Fachbereiche, als auch das Management bei der Einhaltung der DSGVO-Anforderungen.
Die wichtigsten Handlungsfelder sowie deren Lösungsmöglichkeiten zur Sicherstellung der DSGVO-Konformität:

3.1 Arbeitsintensive, fehleranfällige Konten- & Rechteverwaltung

In den meisten Unternehmen erfolgt die Administration von Benutzerkonten und Zugriffsrechten noch zu großen Teilen manuell. Die notwendigen Änderungen wie die Vergabe oder der Entzug von Gruppenberechtigungen, Rollen oder Profilen werden über die jeweiligen Verwaltungs-Werkzeuge von Microsoft, SAP und weiteren Herstellern durchgeführt. Diese manuelle Arbeit hat unterschiedliche Auswirkungen:

- Die Umsetzung der Zugriffsrechte in den Zielsystemen ist fehleranfällig. Korrekte Benutzerrechte können nicht sichergestellt werden.
- Es entsteht viel unnötiger Arbeitsaufwand für Umsetzung aber auch für die Koordination von bspw. Rückfragen oder Entscheidungen.
- Dies führt zu langen Laufzeiten der Prozesse und bei den betreffenden Mitarbeitern potentiell zu Wartezeiten und unproduktiven Zeiten.
- Um die Arbeiten sauber bewerkstelligen zu können, ist außerdem viel Know-how zum Prozess und dem Zielsystem bei den handelnden Personen erforderlich.

OGiTiX unimate sorgt für eine durchgängige Automation der Prozesse wie Eintritt, Austritt und Änderung sowie für die Nachversorgung mit Rechten. Die Provisionierung der Zielsysteme wie Active Directory, SAP, Office365 oder Exchange erfolgt dabei über Schnittstellen ebenfalls automatisiert. Manuelle Administrationstätigkeiten im User- & Rechte Management gehören damit der Vergangenheit an.

Die technische Umsetzung durch die Identity Management Software entlastet das IT Personal und eliminiert die Wartezeiten für den Anwender. Falsche Zugriffsrechte gehören der Vergangenheit an, da eine prozesskonforme Umsetzung durch die IAM Software sichergestellt ist. Vergaberichtlinien und die damit erzielte DSGVO-Konformität werden eingehalten – automatisch.

✓ **Automation der Konten- & Rechte-Administration**

- Bedarfsgerecht automatisierte Umsetzung in den Zielsystemen
- Erhebliche Reduktion des Aufwandes und der Wartezeiten
- Eliminierung von Fehlerquellen in der Rechtevergabe

3.2 Zu viele administrative Rechte zur Erfüllung der Aufgaben

Die manuelle Umsetzung von Zugriffsrechten erfordert i.d.R. umfangreiche administrative Berechtigungen bei den Mitarbeitern, die diese Änderungen im Zielsystem durchführen. Dabei werden häufig auch generische, nicht personengebundene Admin-Konten verwendet.Das Risiko des Missbrauchs dieser Administrationsrechte ist immanent. Die Gefahr, dass Personen Zugriff auf unbefugte Datenbereiche erhalten, kann nur organisatorisch gelöst werden. Hinzu kommt, dass ein erkannter Missbrauch durch den teilweise fehlenden Personenbezug bei administrativen Benutzerkonten nicht bis auf den Verursacher nachvollziehbar ist.

OGiTiX unimate automatisiert die Administration der Konten und Rechte und nutzt dafür entsprechende Schnittstellen. Damit wird der Großteil der Rechteadministration abgedeckt und die Notwendigkeit, dass Personen administrative Rechte in diesen Applikationen haben, reduziert sich auf ein einfacher kontrollierbares Mindestmaß.

Je nach Sicherheits-Anforderungen ist es möglich jegliche manuelle User- & Rechte Administration zu unterbinden. Über sogenannte Notfalluser-Prozesse in der IAM Software können dann für Ausnahmefälle administrative Rechte beantragt, im 2-, 4- oder auch 6-Augenprinzip entschieden werden und dann zeitlich befristet bestimmten Personen zugänglich gemacht werden.

✓ **Sicherheit der Konten- & Rechte-Administration**

- Granulare Rechtekonfiguration zur Automation
- Administrations-Rechte werden vom IAM System verwaltet
- Notwendigkeit von administrative Rechten reduziert auf ein Minimum

3.3 Manuelle Koordination und unklare Vergabeprozesse

Die Steuerung der Prozesse wie Eintritt, Austritt und Änderung sowie die Nachversorgung mit Rechten ist häufig durch manuelle Tätigkeiten geprägt. In Laufzetteln, Checklisten oder Tickets werden die notwendigen Tätigkeiten festgehalten.
Wer an welcher Stelle des Prozesses Aufgaben oder Entscheidungen zu erledigen hat, wird von Mitarbeitern „erkannt“ und manuell in die Wege geleitet. Hierzu werden E-Mails versendet, Telefonate geführt oder Tickets erstellt – eine Art Turnschuh-Prozesssteuerung. Medienbrüche und manuelle Tätigkeiten prägen den Alltag – mit unterschiedlichsten Konsequenzen:

- Bestenfalls fragmentierte Dokumentation des Prozessablaufs

- Vgl. Nachweißpflicht nach DSGVO
- Manuell koordinierter Prozessablauf im Unternehmen
  - Keine Sicherstellung der Laufzeiten
  - Häufige Rückfragen: „Wo ist mein Antrag?“
- Teils unklare Vergabeverfahren
  - Wer darf für welche Mitarbeiter und Rechte was entscheiden?
  - Viele Rückfragen, telefonische Einholung von Genehmigungen
- Die IT erhält häufig zu spät oder gar keine Information zu notwendigen Änderungen
  - Austritte werden zu spät oder gar nicht umgesetzt
  - Eintritte werden zu spät gemeldet -> Ad-hoc Administration

In OGiTiX unimate werden die relevanten Prozesse wie Mitarbeiter-Eintritt, -Austritt oder -Änderung sowie Anträge auf Zusatzberechtigungen von A bis Z hinterlegt. OGiTiX unimate steuert den gesamten Prozess und bindet erforderliche Stellen via E-Mail, Aufgabe oder Entscheidung bedarfsgerecht ein.

Organisationsdaten wie Abteilungen, Vorgesetzte, Stellvertreter oder auch Entscheider für bestimmte Rollen, Datenbereiche oder Gruppen sind entweder in der unimate Datenbank hinterlegt oder werden über die Anbindung an das AD oder bspw. das SAP Org.-Management abgefragt.

Die Prozesse können als Self-Service initiiert oder automatisch über eine Anbindung an das HR-System gestartet werden. Ein geführtes Arbeiten sorgt zudem für eine hohe Usability in den Formularen und Prozessen – jeder sieht nur die für ihn relevanten Informationen.
Damit werden eine ganze Reihe an Vorteilen und Ergebnissen erzielt:

✓ **Digitale Vergabe- & Life-Cycle-Prozesse (automatisch gesteuert)**

- Automatische Eintritts-, Austritts- und Veränderungsprozesse
- Entscheider-Zuordnung durch Anbindung an Organisationsdaten
- Einhaltung von Vergaberichtlinien | Prozesskonformität
- Eskalations- & Erinnerungsmanagement
- Delegations- & Ausnahmeverwaltung
- Systembedingte, lückenlose Protokollierung
- Kalkulierbare Laufzeiten und damit SLA-fähige Prozesse

3.4 Rechte-Entzug bei Mitarbeiter-Austritt unzureichend

Die Umsetzung von Mitarbeiter-Austrittsprozessen und damit die Deaktivierung von Benutzerkonten, remote Zugriff oder Extranet-Zugängen stellt für viele Unternehmen eine große Herausforderung dar. Häufig werden die relevanten IT-Bereiche viel zu spät, nicht ausreichend oder teilweise überhaupt nicht über notwendige Arbeiten informiert.

Dies hat zur Folge, dass Benutzerzugriffe mehr oder weniger lang aktiv bleiben, auch wenn der Mitarbeiter bereits gar nicht mehr für das Unternehmen arbeitet. Damit steigt die Gefahr des Missbrauchs dieser Zugriffsmöglichkeiten exponentiell. Die Motivation von Ex-Mitarbeitern ist in dieser Hinsicht naturgemäß wesentlich höher als bei Angestellten. Nach einer veröffentlichten Sicherheitsumfrage „WIK/ASW Sicherheits-Enquete 2014/2015“ des deutschen Verfassungsschutzes erfolgten über 30% der öffentlich gewordenen Hackerangriffe durch sog. Innentäter. Die Dunkelziffer liegt dabei wie immer wesentlich höher.

Neben den Sicherheitsrisiken ergeben sich noch weitere Herausforderungen. Denn was geschieht mit den persönlichen Daten und E-Mails des Mitarbeiters? Wann erfolgt eine Archivierung oder Löschung der Daten? Und wie wird damit umgegangen, wenn Mitarbeiter wieder eintreten und erneut für das Unternehmen arbeiten (sog. Wiedereintritt)?

Mit OGiTiX unimate als Identity Management Lösung werden Austrittsprozesse in der Regel automatisch durch eine Anbindung an das HR-System gestartet. OGiTiX unimate sorgt dafür, dass alle Benutzerkonten des betreffenden Mitarbeiters stichtagsgetreu und automatisch deaktiviert werden. Alternativ und parallel zur direkten Anbindung an das HR-System kann der Austrittsprozess als Self-Service für die Personalabteilung oder Fachvorgesetzte bereitgestellt werden. Auch der zyklisch automatische Import von CSV- oder XML-Dateien mit den HR-Informationen ist möglich.

Damit wird sichergestellt, dass Mitarbeiter ab dem Tag des Austritts über keine aktiven Benutzerrechte mehr verfügen und alle Stellen informiert werden. Alle Folgeaufgaben wie bspw. Lizenzen freigeben, Postfach und Benutzerablagen sichern können dabei ebenfalls vom System gesteuert werden.

✓ **Automatische und Stichtagsgetreue Umsetzung von Austrittsprozessen**

- Automatische Erkennung von Austritten durch Anbindung an das HR-System
- Wahlweise auch Self-Services zum Start von Austrittsprozessen
- Sicherstellung, dass ab dem Tag des Austritts keine Benutzerkonten mehr aktiv sind
- Weitere Aufgaben im Zuge des Austritts werden ebenfalls verwaltet
- Lückenlose Protokollierung und aktives Monitoring

3.5 Rechte-Zuwachs bei organisatorischen Wechseln

Die Problematik bei organisatorischen Wechseln besteht heute darin, dass für die neue Stelle nicht mehr notwendige Zugriffsrechte i.d.R. bestehen bleiben. Häufig passiert dies, weil nicht transparent ist, welche Rechte entzogen werden dürfen. Oder weil schlicht und einfach die Entfernung nicht mehr erforderlicher Rechte vergessen wird.

Die Vergabe neuer Berechtigungen hingegen erfolgt quasi zwangsläufig, weil der Mitarbeiter ansonsten seiner Arbeitstätigkeit nicht nachkommen kann. Die Meldung über organisatorische Wechsel erreicht die IT zudem häufig zu spät oder erfolgt gar nicht. Fehlende Rechte werden dann auf Zuruf und im Ad-hoc Verfahren durch die IT vergeben. Die so entstehende Dringlichkeit führt neben Unzufriedenheit und Fehleranfälligkeit dazu, dass Dokumentationspflichten dieser Vorgänge vernachlässigt werden.

Mit OGiTiX unimate erfolgt ein Identity Lifecycle Management. Damit wird sichergestellt, dass Mitarbeiter vom Eintritt über die unterschiedlichsten Veränderungen im Unternehmen bis hin zum Austritt des Mitarbeiters immer nur die erforderlichen Benutzerrechte besitzt.

Automatische ablaufende Prozesse sorgen dafür, dass Change-Prozesse wie Abteilungs- und Positionswechsel, die Erweiterung des Aufgabenbereiches oder sogar der Wechsel zu einem anderen Konzerninternen Unternehmen stringent umgesetzt werden, kein Arbeitsschritt vergessen wird und alles vom System lückenlos dokumentiert wird.

Um die Vergabe und den Entzug von Zugriffsrechten zu automatisieren, werden in OGiTiX unimate Rollen definiert. Diese definieren ein Standard-Set an Applikationen & Rechten (Applikationen, Funktionen, Gruppen, Rollen und Profile) die dem Mitarbeiter für eine bestimmte Abteilung, eine bestimmte Position und/oder eine definierte Business Rolle zustehen.

✓ **Identity Lifecycle Management mit OGiTiX unimate**

- Automatische Initiierung der Change-Prozesse
  - durch Anbindung an das HR-System
  - durch Self-Service-basierten Prozessstart
- Automatischer Entzug nicht notwendiger Rechte/Benutzerkonten
- Automatischer Vergabe erforderlicher Rechte/Benutzerkonten
- Standardkonten und -rechte werden im IAM System definiert
  - nach Abteilung, Position oder Rolle
- Diese werden bei einem Eintritt/Wechsel automatisch entzogen und vergeben
  - Least Privilege Prinzip
- Festlegung und autom. Verwaltung von Standardrechten für bestimmte Arbeitskontexte
  - beispielsweise bestimmte Projekte
  - Need-To-Know Prinzip
- Regelmäßige Überprüfung: Rechte und Rollen werden regelmäßig auf ihre Notwendigkeit geprüft. Dazu läuft ein automatischer Re-Zertifizierungsprozess

Need-to-Know-Prinzip

Auch wenn eine Person grundsätzlich Zugriff auf Daten einer Sicherheitsebene hat, verbietet das Need-to-know-Prinzip den Zugriff, wenn die Informationen nicht unmittelbar für die Erfüllung einer konkreten Aufgabe von dieser Person benötigt werden.

Personen, die nicht dauerhaft bestimmte Zugriffe benötigen, müssen somit in der Praxis mit entsprechenden Verfahren wie bspw. Ad-hoc Zugriffsanträgen temporär Zugriff erhalten. Diese Zugriffe müssen nach Erledigung der Aufgabe wieder (automatisch) entzogen werden.

Least-Privilege-Prinzip

Das Least-Privilege-Prinzip schreibt vor, dass einem Benutzer, einer Softwarekomponente oder einer anderen Entität nur die absolut notwendigen Rechte eingeräumt werden dürfen, damit diese, die ihr zugeteilten Aufgaben erledigen kann. Somit gilt es sicherzustellen, dass bei organisatorischen Wechseln der Position, Abteilung oder des Mandanten nicht mehr benötigte Berechtigungen automatisch entzogen werden und neue Zugriffsrechte entsprechend der neuen Rolle vergeben werden.

3.6 Inkonsistente, redundante Datenhaushalte

Alle Berechtigungs- und Identitätsrelevanten Informationen sind heute in unterschiedlichen Datenhaushalten wie dem HR System, Telefonanlage, Active Directory, Messaging, vielen Geschäftsapplikationen und einer Organisationsdatenbank (sofern vorhanden) verteilt. Häufig erfolgt die Übertragung der relevanten Informationen zur Identität wie bspw. Telefonnummer, Büronummern, eMail-Adressen oder Personalnummern in die verteilten Datenbanken gar nicht. Bestenfalls wird es partiell und durch manuelle Arbeit realisiert und ist damit fehlerbehaftet.

Dadurch ist eine Zuordnung der unterschiedlichen Nutzerkonten und Zugriffsrechte zu einer natürlichen Person, also einer Identität, gar nicht oder nur mit viel Aufwand möglich. Durch diese vielen Medienbrüche entstehen unterschiedliche Risiken:

- Eine Person/Identität erhält uneinheitliche/falsche Rechte
- Eine Person/Identität erhält doppelte Konten
- Austritte werden für alle Anwendungen verarbeitet
- Eine Übersicht pro Person/Identität existiert meist nicht

Über Identity & Access Management-Lösungen wie OGiTiX unimate werden diese heute verteilten und nicht verbundenen Datenbanken durch Schnittstellen angebunden. Diese Schnittstellen zu bspw. dem HR-System, Org.-Management, Active Directory und weitere Geschäftsapplikationen synchronisieren diese Informationen in die IAM Datenbank und verteilen diese an die relevanten Applikationen. So wird bspw. die E-Mail-Adresse im SAP HCM eingetragen, sobald diese verfügbar ist.

Im Zuge der Anbindung werden darüber hinaus alle Berechtigungsstrukturen wie Benutzerkonten, Gruppen, Rechten, Rollen, Profilen und Organisationsstrukturen wie OUs, Firmen, Abteilungen, Standorte und Genehmiger zyklisch eingelesen und in dem sogenannte Identity Datastore gespeichert.

Über unterschiedliche Kriterien erfolgt eine Zuordnung der verschiedenen Nutzerkonten nebst den applikationsspezifischen Berechtigungen zu Identitäten. Die sog. Identitätenbildung erfolgt automatisch anhand einstellbarer Kriterien wie Vorname, Nachname, Geburtsdatum, Personalnummer, etc. automatisch durch OGiTiX unimate. Damit entsteht eine übergreifende Sicht auf die vorher verteilten und inkonsistenten Daten, die jederzeit von der IAM Software aktuell gehalten wird.

✓ **Identity Datastore mit OGiTiX unimate**

- Automatisches Datenmanagement (HR, Org. Mgmt., AD, Apps)
  - über Schnittstellen, CSV-Dateien oder Aufgaben
- Synchronisierung von Berechtigungs- & Organisationsstrukturdaten
- Verknüpfung der unterschiedlichen Benutzerkonten zu Identitäten
  - über sog. Identifier wie Personalnummer, Name, Geburtsdatum usw.
- Automatischer Aufbau und Pflege einer übergreifenden Identitätsdatenbank

3.7 Medienbrüche und fehlende Nachvollziehbarkeit

Heute werden enorm viele Tools und Verwaltungsprogramme genutzt, um Konten und Rechte zu administrieren: Checklisten, Ticketsysteme, E-Mails, Telefonate, Formulare und diverse Management-Konsolen. Durchgeführte Entscheidungen sind häufig nicht oder nur schwer auswertbar dokumentiert.

Diese fragmentierten Tools und Prozesse machen eine lückenlose Protokollierung und Nachvollziehbarkeit über die Entstehung oder den Status-quo von Benutzerrechten nahezu unmöglich. Bestenfalls lassen sich diese Information mühsam zusammen sammeln. OGiTiX unimate protokolliert jeden Prozessschritt systemseitig und unabhängig davon, ob es sich um einen Antrag, eine Entscheidung, eine Aufgabe oder die (automatische) Vergabe von Zugriffsrechten handelt.

✓ **Lückenlose Nachvollziehbarkeit mit OGiTiX unimate**

- Systembedingte lückenlose Nachvollziehbarkeit
- Vom Antrag über Entscheidungen bis zur technischen Umsetzung
- Jeder einzelne Schritt wird vom IAM System automatisch protokolliert
- Über alle verwalteten Systeme hinweg, ob mit oder ohne Schnittstelle

3.8 Keine validen Audit Reports und Auswertungen

Verteilte Verwaltungs-Werkzeuge, Datenhaushalte und Prozesse machen die Erstellung von Audit Reports und Auswertungen nur mit extrem hohem manuellem Aufwand möglich.
Zu dem hohen Arbeits- und Zeitaufwand kommt hinzu, dass manuell zusammengetragene Informationen für Reports fehleranfällig sind und somit die Vollständigkeit sowie die Belastbarkeit der Auswertungen fraglich ist. Die Auswertung über die Historie und Herkunft ist meist gar nicht dokumentiert, was die Einhaltung von Compliance-Richtlinien schwierig oder unmöglich macht.

OGiTiX unimate bietet eine ständig aktuelle Identitätsdatenbank sowie eine lückenlose Protokollierung der Prozesse und Provisionierung in den Zielsystemen und stellt auf dieser Grundlage die unterschiedlichsten Reports zum Abruf bereit. Ob für die Revision, einen Audit oder den Fachbereich, Reports über aktuelle u. historische Berechtigungen lassen sich mit wenigen Mausklicks tagesaktuell erstellen.

✓ **User- & Rechte-Reports & Dashboards mit OGiTiX unimate**

- Anwendungsübergreifende Reporting Datenbank
- Bildung und Revisionierung von Identitäten
  - Eine Art „Time Machine“ für den Stand an Rechten
- Auswertungen auf Knopfdruck | Self-Service
  - Wer hatte wann welche Rechte?
  - Wer hat diese beantragt und genehmigt?
  - Benutzerreports über den Status-quo
  - Reports pro Abteilung, Standort, Org.-Einheit
  - Mitgliederreports für Gruppen, Rollen und Profilen
  - u.v.m.
- Zyklisch-automatische Reports für Vorgesetzte oder Data Owner

4 Eigene Bewertungen & Bemerkungen

Arbeitsintensive, fehleranfällige Konten- & Rechteverwaltung

Bewertung: ☐ trifft zu ☐ trifft teilweise zu ☐ trifft nicht zu

Zu viele administrative Rechte zur Erfüllung der Aufgaben erforderlich

Bewertung: ☐ trifft zu ☐ trifft teilweise zu ☐ trifft nicht zu

Manuelle Koordination und unklare Vergabeprozesse

Bewertung: ☐ trifft zu ☐ trifft teilweise zu ☐ trifft nicht zu

Rechte-Entzug bei Mitarbeiter-Austritt unzureichend

Bewertung: ☐ trifft zu ☐ trifft teilweise zu ☐ trifft nicht zu

Rechte-Zuwachs bei organisatorischen Wechseln

Bewertung: ☐ trifft zu ☐ trifft teilweise zu ☐ trifft nicht zu

Inkonsistente, redundante Datenhaushalte

Bewertung: ☐ trifft zu ☐ trifft teilweise zu ☐ trifft nicht zu

Medienbrüche und fehlende Nachvollziehbarkeit

Bewertung: ☐ trifft zu ☐ trifft teilweise zu ☐ trifft nicht zu

Keine validen Audit-Reports und Auswertungen

Bewertung: ☐ trifft zu ☐ trifft teilweise zu ☐ trifft nicht zu

WIR SIND IAM

SEIT ÜBER 15 JAHREN LEBEN UND ENTWICKELN WIR IAM-LÖSUNGEN FÜR SIE!

WIR ÜBERZEUGEN SIE GERNE:

MAIL TO

WEB-SEMINARE

UNSERE KUNDEN BERICHTEN:

KUNDENBERICHTE

Imprivata OGiTiX GmbH
(vormals OGiTiX Software AG)
Hans-Böckler-Str. 12
40764 Langenfeld
Deutschland

Fon +49 2173 99385-0
Fax +49 2173 99385-900
Mail info@ogitix.de
Web www.ogitix.de

Vertretungsberechtigt:
Geschäftsführer Ingo Buck
Jeffrey Kowalski

Amtsgericht Düsseldorf
Nummer: HRB 100306
Sitz der Gesellschaft:
Langenfeld