Automatische Benutzeranlage und Berechtigungsvergabe im HCM Teil 2

Der Datenschutz und seine Auswirkungen auf die Berechtigungen

im HCM

EU-Datenschutz-Grundverordnung

Auswirkungen auf
Berechtigungen
und HCM

Gültigkeit und Ziele

- Endgültiges Inkrafttreten 25.05.2018
- Ersatz der EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) von 1995
- Zur Zeit gültig: Bundesdatenschutzgesetz

  (schrittweise Anpassung an EU-Recht)
- Einheitliche Standards in Europas Datenschutz
- Keine “Rückzugsräume” mehr
- Stärkere Nutzerrechte

Eckpunkte

- US-Unternehmen an europäisches Datenschutzrecht gebunden
- Höhere Bußgelder möglich
- zweijährige Übergangszeit für Unternehmen
- Konzernprivileg

  (erleichterte Weitergabe von Daten in Unternehmensgruppe)
- **Recht auf Vergessenwerden**
- One-Stop Shop Prinzip

  (Kontakt mit eigener

  Datenschutzbehörde reicht)

Vertrag zur Auftragsverarbeitung

Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten
➔ Schriftlicher Vertrag erforderlich

- Gegenstand und Dauer der Verarbeitung
- Art und Zweck der Verarbeitung
- Art der personenbezogenen Daten & Kategorien von betroffenen Personen
- Umfang der Weisungsbefugnisse
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit
- Sicherstellung von technischen & organisatorischen Maßnahmen
- Hinzuziehung von Subunternehmern
- Unterstützung des für die Verarbeitung Verantwortlichen bei Anfragen und Ansprüchen Betroffener
- Unterstützung des für die Verarbeitung Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsdatenverarbeitung
- Kontrollrechte des für die Verarbeitung Verantwortlichen und Duldungspflichten des Auftragsverarbeiters
- Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt

Pflichten für Unternehmen

- geeignete technische und organisatorische Maßnahmen (Virenscanner, Zutrittskontrollen usw.)
- Verfahrensverzeichnis
- **Informationspflicht**

„wer was wann und bei welcher Gelegenheit über sie weiß.“

Bußgelder und Sanktionen

„Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder moralischer Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den für die Verarbeitung Verantwortlichen oder gegen den Auftragsverarbeiter.“(Gemeinsame Haftung)

Bei Auftragsdatenverarbeitung

- Geldbußen in Höhe von bis zu 10 Millionen Euro
- oder 2% des gesamten weltweit erzielten Jahresumsatzes
- je nachdem welcher Betrag höher ist

Bei einzelnen Unternehmen:

- Geldbußen in Höhe von bis zu 20 Millionen Euro
- oder 4% des gesamten weltweit erzielten Jahresumsatzes
- je nachdem welcher Betrag höher ist

Beschäftigtendatenschutz

Ist der Arbeitnehmerdatenschutz in der EU-DSGVO geregelt?

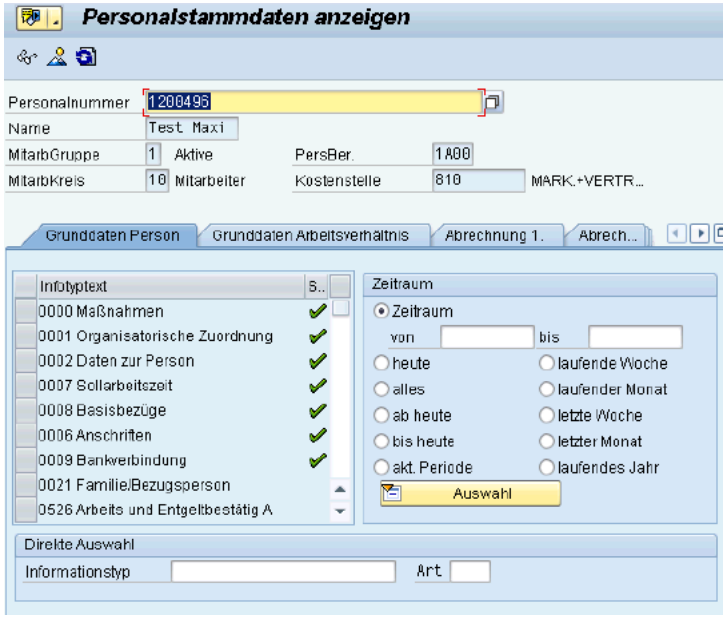
Nein, die EU-Datenschutz-Grundverordnung wie sie nunmehr im Arbeitsergebnis der Trilog-Parteien vom 15. Dezember 2015 ihre Endfassung gefunden hat, wird keinerlei spezifische, rechtsgestaltende Regelungen zum Beschäftigtendatenschutz enthalten.

Bedeutet das, es gibt keinen Beschäftigtendatenschutz?

Nein, auch nach der EU-DSGVO werden Beschäftigte innerhalb ihrer Arbeitsverhältnisse nicht rechtlos sein. So verweisen einzelne Vorschriften der EU-DSGVO (z.B.: Art. 9 Abs. 2 h DSGVO Verarbeitung von besonderen Kategorien von personenbezogen Daten) auf den Mitarbeiterdatenschutz und auch die allgemeine Grundätze der Datenverarbeitung (Art. 5 DSGVO) gelten selbstverständlich auch im Beschäftigtenverhältnis. Allerdings wird es keine zentrale Regelungsvorschrift zu diesem Thema in der EU-DSGVO geben.

Nationale Gesetzgebung kann dies verschärfen!

Berechtigungsprüfung



authority-check object 'P_ORGIN'
id 'INFTY' field '0008'
id 'SUBTY' dummy
id 'AUTHC' field 'R'
id 'PERSA' field pa0001-werks
id 'PERSG' field pa0001-persg
id 'PERSK' field pa0001-persk
id 'VDSK1' field pa0001-vdsk1.

Grundsätze für die Verarbeitung personenbezogener Daten

Art. 5 DSGVO

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) 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“);

Überlegungen

- **Reicht das Infotypenkonzept nun noch aus?**
- **Wie und wann werden Daten gelöscht?**
- **Wie müssen die Berechtigungen reorganisiert werden?**

Governance, Risikomanagement und Compliance (GRC)

Finanzwesen

- Drei Verteidigungslinien für das Risikomanagement
- Straffe Zugriffsanalysen
- International erfolgreich

SAP-Software

für die drei Verteidigungslinien

SAP Risk Management
SAP Process Control
SAP Business Integrity Screening
SAP Audit Management

für die Zugriffssteuerung

SAP Access Control

Straffen Sie die Verwaltung und Validierung der Zugriffsrechte mit Governance-Lösungen, die Ihnen helfen, die Vergabe von Zugriffsrechten zu automatisieren und den Zugriff auf Anwendungen und Daten zu zertifizieren. Setzen Sie durch die Integration vorbeugender Richtlinienprüfungen und die Überwachung von Notfallzugriffen die Zugriffsrechte sicher durch.

SAP Cloud Identity Access Governance

Verbessern Sie die Identitäts- und Zugriffsverwaltung und bieten Sie ein intuitives Anmeldeverfahren mit umfangreichen Funktionen für das Identitätsmanagement und die Zugriffssteuerung. Vereinfachen Sie das Identitätsmanagement in komplexen Umgebungen mit einer intuitiven Oberfläche in Form eines Dashboards.

SAP Enterprise Digital Rights Management von NextLabs

Bieten Sie Ihren Fachanwendern und Partnern rund um die Uhr Zugriff auf Unternehmensdaten. Schützen Sie aber gleichzeitig Geschäftsgeheimnisse und geistiges Eigentum, indem Sie für Dateien wahlweise umfangreiche Bearbeitungsberechtigungen oder auch nur den Lesezugriff gewähren. Ermöglichen Sie den Benutzern, Dateien jedes Typs mit jedem Gerät und ohne Installation von Client-Software gemeinsam zu bearbeiten.

SAP Access Violation Management von Greenlight

Kontrollieren Sie die Zugriffsrisiken und bewerten Sie deren finanzielle Auswirkungen mit integrierter Software, die die Risikoerkennung automatisiert. Verringern Sie den manuellen Aufwand für Kontrollen und vermeiden Sie Falschmeldungen mit einer ausnahmebasierten Überwachungssteuerung und Funktionen für die Nachverfolgung.

für das internationale Handelsmanagement

SAP Global Trade Services

Bei weiteren Fragen stehen wir Ihnen gerne zur Verfügung

Vielen Dank für Ihre Aufmerksamkeit !

Kontakt

IPS Training und Consulting GmbH
Peter Klimke
Geschäftsführer
Stieghorster Str.60
33605 Bielefeld
pk@IPS-IT.de
Tel.: 0521 / 20889-30
Mobil: 0172 / 5217206