betasystems

Machen Sie Ihr Unternehmen fit für GDPR –

Was Sie jetzt darüber wissen sollten

von Niels von der Hude, Director Product Strategy

Inhalt

Im Mai 2018 tritt eine neue Verordnung in Kraft, auf die sich Unternehmen schon heute vorbereiten sollten. Denn die neue

EU Datenschutz-Grundverordnung

oder

EU-DSGVO / GDPR
(General Data Protection Regulation)

betrifft nahezu alle Unternehmen weltweit.

Dennoch fällt es IT-Spezialisten sehr schwer, diese neue Verordnung einzuordnen, da man sich schnell in den zahlreichen Aspekten verliert, die solch einer multinationalen, themenübergreifenden und unterschiedlichste Firmen betreffenden Verordnung anhängen.

Das Studium vorhandener Veröffentlichungen zum Thema EU-DSGVO würde Tage in Anspruch nehmen, ohne zu einem eindeutigen Ergebnis zu führen.

Aus diesem Anlass hat Beta Systems eine Zusammenfassung der zentralen Auswirkungen dieser Verordnung zusammengestellt, die die meisten in Europa tätigen Unternehmen betreffen wird.

1. Der formale Kontext dieser Verordnung

Um die Zielsetzung und die Inhalte der EU-DSGVO zu verstehen ist es sinnvoll, sich zunächst den derzeitigen Stand bestehender Verordnungen zum Thema Datenschutz zu vergegenwärtigen.

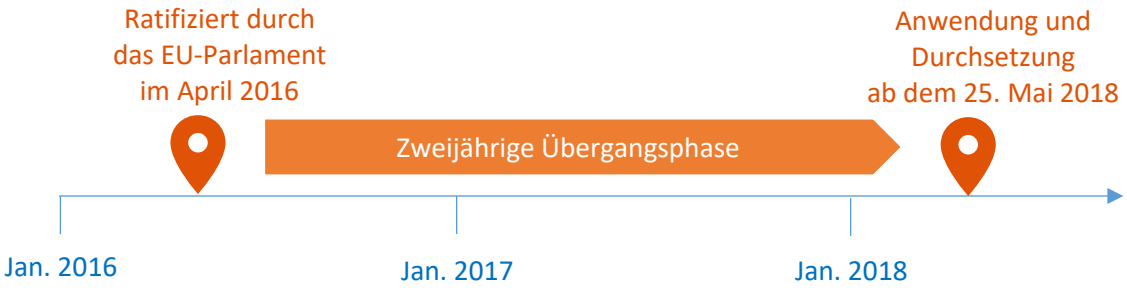
EU-DSGVO ist der Nachfolger einer EU-Direktive aus dem Jahr 1995. Mit diesem Vorläufer (95/46/EC) skizzierte die EU ursprünglich ihre Regeln zum Datenschutz. Aus heutiger Sicht weist diese Verordnung **zwei zentrale Schwachstellen** auf:

1. Als ‚Direktive' war 95/46/EC nicht automatisch für alle Mitgliedsstaaten der EU gültig. Stattdessen lag es an den einzelnen Staaten, diese Verordnung in nationales Recht umzusetzen. Wie üblich führte dies zu einer Vielzahl **abweichender nationaler Interpretationen**. Heutzutage unterliegt der Datenschutz noch immer unterschiedlichen Regelungen der einzelnen EU-Mitgliedsstaaten.

2. Die Inhalte der Direktive 96/46/EC wurden in den frühen 90er Jahren formuliert. Somit erklärt es sich, dass **zentrale IT-Trends der letzten zwei Jahrzehnte**, wie z. B. Mobile Computing, das Potenzial von Big Data-Analysen oder durch die digitale Transformation bewirkte veränderte Geschäftsabläufe und die damit einhergehenden erheblichen datenschutzrelevanten Aspekte in der bestehenden Verordnung **nicht berücksichtigt werden**.

EU-DSGVO nimmt sich dieser vernachlässigten Bereiche an und ist sowohl deutlich umfassender als auch auf rechtlicher Basis anders gestrickt als 96/46/EC. Anders als 95/46/EC ist EU-DSGVO eine ‚Verordnung' und nicht wie vormals eine ‚Direktive'. **Eine Verordnung** ist als ein Gesetzeswerk der EU zu verstehen, das zeitgleich und **umgehend in sämtlichen Mitgliedsstaaten als Gesetz in Kraft tritt**. Die EU-DSGVO wurde am 27. April 2016 beschlossen.

Die Verordnung tritt am 25. Mai 2018 im Anschluss an eine zweijährige Übergangsphase in Kraft. Im Gegensatz zu einer Direktive bedarf die Verordnung keiner legislativen Schritte der nationalen Regierungen.



2. Wen betrifft die EU-DSGVO?

Wann immer sich Unternehmen mit neuen rechtlichen Rahmenbedingungen auseinandersetzen müssen, steht die folgende Frage stets im Vordergrund: „Hat diese Verordnung eine Auswirkung auf unser Geschäft?“ Im Gegensatz zu anderen Verordnungen ist der Anwendungsbereich der EU-DSGVO schnell erklärt: **Die EU-DSGVO betrifft praktisch jedes Unternehmen.** Die EU-DSGVO ist nicht auf bestimmte Rechtsformen oder Branchen beschränkt. In Artikel 3 der Verordnung steht:

> *„Die EU Datenschutz-Grundverordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.*
>
> *Diese Verordnung **findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen**, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht (a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist; oder (b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.“*

Es folgt eine Zusammenfassung der Inhalte dieses Zitats (sowie anderer Abschnitte der Verordnung) in Klartext:

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 Verordnung

- **Organisationen in der EU**, die personenbezogene Daten von Personen in der EU verarbeiten.
- **Organisationen außerhalb der EU**, die personenbezogene Daten von Personen in der EU verarbeiten.

Der Anwendungsbereich dieser Verordnung zielt auch eindeutig auf die wachsende Zahl von Geschäftsszenarien ab, in denen internationale Unternehmen wie Microsoft, Google oder Alibaba personenbezogene Daten von Personen in der EU außerhalb der EU verarbeiten. Denn gemäß der obigen Definition betrifft die EU-DSGVO auch diese Unternehmen.

In diesem Kontext ist eine präzise Lesung des Gesetzestextes wichtig, denn **die Verordnung bezieht sich nicht auf ‚EU-Bürger‘, sondern auf Personen (Datensubjekte), „die sich in der EU befinden“**. Somit trifft dies auch auf außereuropäische Bürger zu, solange sie sich in der EU aufhalten.

Des Weiteren differenziert die EU-DSGVO bewusst zwischen **Verantwortlichen** (Artikel 4 –(7))

> *„Verantwortlicher bezeichnet die [natürliche oder juristische Person...], die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.“*

und **Auftragsverarbeitern** (Artikel 4 – (8))

> *„Auftragsverarbeiter bezeichnet eine [natürliche oder juristische Person...], die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.“*

Sowohl für ‚Verantwortliche‘ als auch für ‚Auftragsverarbeiter‘ **legt die EU-DSGVO individuelle Verantwortlichkeiten fest**. Der Aufwand, mit dem die Begriffe ‚Verantwortlicher‘ und ‚Auftragsverarbeiter‘ personenbezogener Daten definiert wurden, macht unmissverständlich klar, dass gemäß der EU-DSGVO

→ kein Unternehmen seine Verpflichtungen einfach an einen Dienstleister übertragen kann.

Da bei den Pflichten zwischen denen eines Verantwortlichen und eines Auftragsverarbeiters unterschieden wird, besteht die Notwendigkeit zu ermitteln, ob es sich bei einem Unternehmen um einen Verantwortlichen oder Auftragsverarbeiter handelt. Zahlreiche Artikel und Blogs widmen sich der Interpretation dieser Definition. Als Faustregel lässt sich sagen, dass nur reine Rechenzentrumsdienstleister klar als Auftragsverarbeiter ausgewiesen sind. In allen anderen Szenarien ist die Definition etwas ‚unscharf‘, so dass stets der Einzelfall betrachtet werden muss.

Es gibt nur wenige eindeutige Ausnahmen, welche Organisationen bzw. Situationen nicht unter die EU-DSGVO fallen:

Neben der rein privaten Nutzung personenbezogener Daten (durch eine natürliche Person im Rahmen einer rein persönlichen oder Haushaltsaktivität), ist die **EU-DSGVO nicht anwendbar auf ‚Strafverfolgungsbehörden der EU‘**

> *(„durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.“)*

sowie auf **EU-Institutionen**:

> *(„Für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union.“)*

Die **EU-DSGVO** findet Anwendung, sobald personenbezogene Daten von Personen verarbeitet werden, die sich in der Europäischen Union befinden.

3. Verarbeitung personenbezogener Daten gemäß EU-DSGVO

Die EU-DSGVO regelt die Verarbeitung sämtlicher personenbezogener Daten. Um zu verstehen, welche Geschäftsaktivitäten als ‚Verarbeitung personenbezogener Daten' gelten, ist die entsprechende Definition in der EU-DSGVO von Bedeutung: „Was sind personenbezogene Daten und was stellt ihre Verarbeitung dar?"

Die **Definition von ‚personenbezogenen Daten'** ist im Kontext dieser Verordnung recht weit gefasst. Personenbezogene Daten werden wie folgt beschrieben:

„...alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚Datensubjekt')"

In Artikel 9 der EU-DSGVO werden **bestimmte Arten von Daten** von dieser allgemeinen Definition **ausgeschlossen:**

> *„Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt."*

Die Verarbeitung solcher Daten ist ausdrücklich untersagt, aber es gibt einige Ausnahmeregelungen. Da es sich hierbei um einen Randbereich der Verordnung handelt, gehen wir in diesem Dokument nicht näher darauf ein.

Es sei in diesem Kontext jedoch darauf hingewiesen, dass die EU-DSGVO ausdrücklich keine Anwendung auf die personenbezogenen Daten Verstorbener findet. Dies wird in Paragraph 27 der Verordnung definiert:

> *„Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener. Die Mitgliedstaaten können Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen."*

Was alle anderen personenbezogenen Daten anbelangt, greift die EU-DSGVO gleich zu Beginn der Verarbeitung auf der Grundlage von Grundsätzen (Artikel 5).

Diese Grundsätze verpflichten den ‚Verantwortlichen', solche Daten „rechtmäßig, angemessen, akkurat und sicher" zu verarbeiten.

Das flüchtige Studium dieses Artikels lässt diesen als eher abstrakten und weniger wichtigen Definitionssatz erscheinen – dies ist allerdings weit gefehlt!

Bei näherer Betrachtung beziehen sich die meisten, wenn nicht gar alle, Grundsätze zur Verarbeitung auf ‚den Zweck' – Daten dürfen nur „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden":

→ **Daten dürfen nur „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (‚Datenminimierung');" erhoben werden und müssen**

„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;"

Da gemäß diesen Grundsätzen „Der Verantwortliche [...] für die Einhaltung des Absatzes 1 verantwortlich [ist] und [...] dessen Einhaltung nachweisen können [muss] (‚Rechenschaftspflicht')", zwingt dieser Artikel praktisch

→ jedes der EU-DSGVO unterliegende Unternehmen dazu, die individuellen Zwecke, zu denen personenbezogene Daten verarbeitet werden, zu definieren, dokumentieren und danach zu handeln.

Dies stellt eine große Neuerung im Standard für die Datenverarbeitung dar. Aktuell erfassen viele Unternehmen personenbezogene Daten und legen erst zu einem späteren Zeitpunkt die Verwendungszwecke für diese Daten fest.

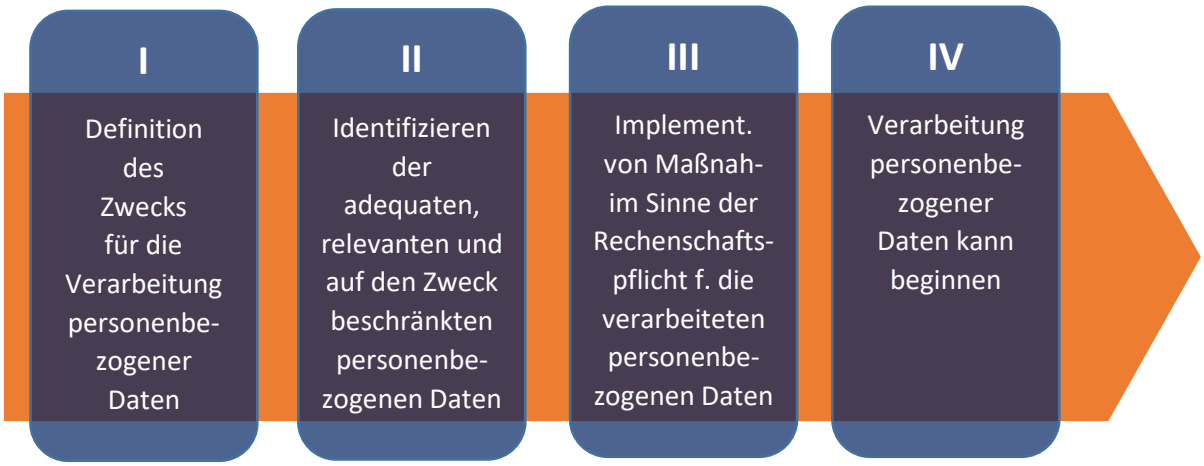
Sobald die EU-DSGVO in Kraft tritt, müssen Unternehmen alle Abläufe rund um die Bearbeitung personenbezogener Daten standardmäßig derart anlegen, dass für die Erfüllung des jeweiligen Zwecks nur die minimal benötigte Datenmenge verarbeitet wird. Eine Möglichkeit, wie diese Vorgabe bezüglich des Verarbeitungszwecks erfüllt werden kann, besteht darin,

→ die ausdrückliche Erlaubnis der Person (Datensubjekt) zur Verarbeitung ihrer Daten einzuholen.

Die EU-DSGVO schreibt eine Zahl konkreter Voraussetzungen vor, die eingehalten werden müssen, um eine valide Einverständniserklärung zu erhalten (spezifisch, informiert, mit der Möglichkeit, die Einwilligung zurückzunehmen, der Verantwortliche muss die Einwilligung nachweisen …).

Bezüglich des Identity & Access Management (IAM) schreibt Artikel 5 zudem vor, 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.*** *“*



4. Rechte von Privatpersonen

Aus der Warte des ‚Datensubjekts‘ (der betroffenen Person), führt die EU-DSGVO einige neue Rechte ein und stärkt einige bestehende Rechte die Individuen nach derzeitigem Rechtsstand zugesprochen werden.

Die EU-DSGVO räumt Privatpersonen folgende Rechte ein:

1. **Informationspflicht und Auskunftsrecht**
   Im Sinne einer gerechten und gesetzeskonformen Verarbeitung personenbezogener Daten müssen Verantwortliche dem Datensubjekt bezüglich der Erhebung und Verarbeitung ihrer personenbezogenen Daten bestimmte Mindestauskünfte zukommen lassen.

2. **Recht auf Zugriff**
   Neben dem zuvor genannten Recht auf Information, welche Daten über welchen Zeitraum von wem verarbeitet werden, können Datensubjekte eine Kopie der verarbeiteten personenbezogenen Daten anfordern.

3. **Recht auf Berichtigung**
   Verantwortliche haben sicherzustellen, dass falsche oder unvollständige Daten gelöscht oder richtiggestellt werden. Datensubjekte haben das Recht auf Korrektur fehlerhafter personenbezogener Daten.

4. **Recht auf Löschung**
   Datensubjekte haben das Recht auf Löschung ihrer personenbezogenen Daten (das ‚Recht auf Vergessenwerden') sobald die Daten nicht mehr für den ursprünglichen Zweck benötigt werden, das Datensubjekt seine Einwilligung zurückzieht und keine anderweitigen Rechtsgründe zur Speicherung vorliegen bzw. die Daten unrechtmäßig verarbeitet wurden.

5. **Recht auf Einschränkung der Verarbeitung**
   Datensubjekte sind berechtigt, unter bestimmten Umständen die Verarbeitung ihrer personenbezogenen Daten einzuschränken (konkret: die Daten dürfen nur vom Verantwortlichen vorgehalten und nur für begrenzte Zwecke verwendet werden).

6. **Recht auf Datenübertragbarkeit**
   Datensubjekte haben das Recht, eine Kopie ihrer personenbezogenen Daten in einem gebräuchlichen, maschinenlesbaren Format zu erhalten und ihre personenbezogenen Daten von einem Verantwortlichen zu einem anderen zu übermitteln bzw. die Datenübermittlung direkt zwischen Verantwortlichen zu veranlassen.

7. **Widerspruchsrecht**
   Sofern sich die Verarbeitung personenbezogener Daten auf einem öffentlichen Interesse oder legitimen Interessen des Verantwortlichen begründet, haben Datensubjekte das Recht, der Verarbeitung ihrer personenbezogenen Daten zu widersprechen.

8. **Rechte in Bezug auf automatisierte Entscheidungsfindung und Profiling**.

Potenzielle Ansatzpunkte für Unternehmen:

Das ‚Recht auf Datenübertragbarkeit' dürfte einige Probleme verursachen und somit Projekte in den IT-Abteilungen bedingen. Personenbezogene Daten werden häufig über mehrere IT-Lösungen verteilt verwaltet. Mit der EU-DSGVO ist zu erwarten, dass eine erhebliche Zahl von Personen vom Recht auf den Erhalt einer Kopie des kompletten Datensatzes Gebrauch machen wird. Aber auch das ‚Recht auf Löschung' und das ‚Recht auf Einschränkung der Verarbeitung' erschweren die Verarbeitung und zwingen Unternehmen dazu, **die vorhandenen IT-Systeme einer Prüfung zu unterziehen**. Falls die Datenverarbeitungssysteme nicht in der Lage sind, alle Kopien sämtlicher personenbezogener Daten eines konkreten Datensubjekts schnell zu ermitteln und separat bereitzustellen, müssen diese Systeme mit Funktionen nachgerüstet werden, um den künftigen Anforderungen zu genügen.

5. Von Verantwortlichen und Auftragsverarbeitern einzuhaltende Pflichten

Für Unternehmen ist es von vorrangiger Bedeutung zu wissen, was ihre Pflichten sind.

Abschnitt IV der EU-DSGVO befasst sich explizit mit den Pflichten von Verantwortlichen und Auftragsverarbeitern. Artikel 24 erläutert alle Auflagen, die der Verantwortliche einhalten muss. Der erste Abschnitt dieses Artikels stellt die **allgemeinen Compliance-Kriterien der EU-DSGVO gegenüber dem Verantwortlichen** bereits eindeutig klar.

> *„Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen* ***geeignete technische und organisatorische Maßnahmen*** *um, um sicherzustellen und den* ***Nachweis dafür erbringen*** *zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.“*

Der erste Teil dieses Anschnitts ist eher schwach formuliert und liest sich mehr wie eine Empfehlung („Der Verantwortliche setzt [...] geeignete technische und organisatorische Maßnahmen um …“), aber die Verordnung wird dann kritisch für Unternehmen, wenn die **Pflicht, Maßnahmen zu implementieren mit der Anforderung, die Einhaltung dieser Pflicht nachzuweisen kombiniert wird.**

Alle von der EU-DSGVO betroffenen ‚Verantwortlichen‘ müssen auf Unternehmens-prüfungen vorbereitet sein, in deren Rahmen von ihnen verlangt wird, ihre komplette EU-DSGVO-Implementierung zu erläutern und zu demonstrieren.

Sowohl die Definition von Zwecken, die entsprechende Datenverarbeitung sowie die Implementierung technischer und organisatorischer Maßnahmen kann potenziell Bestandteil einer Unternehmensprüfung werden.

Die Pflichten, die sich aus diesem Artikel ergeben, sind zwar einfach verständlich, aber dennoch für Unternehmen schwer greifbar. In den USA führte die Einführung des Sarbanes-Oxley Acts beispielsweise dazu, dass Unternehmen die Einhaltung der Vorgaben faktisch erst nach einem Audit sicherstellen konnten, da die speziellen Compliance-Kriterien zu einem früheren Zeitpunkt nicht konkret definiert waren.

Bei der Ausarbeitung der EU-DSGVO war der Gesetzgeber bemüht, solche Zustände zu vermeiden, indem im Abschnitt V die ‚Verhaltensregeln und Zertifizierung‘ beschrieben werden.

In Artikel 41 dieses Abschnitts zielt die EU-DSGVO auf die Schaffung unabhängiger ‚Zertifizierungsstellen‘ ab, die von der nationalen Aufsichtsbehörde eingesetzt und befugt werden.

Diese ‚**Zertifizierungsstellen**' sind dazu ermächtigt, spezielle Zertifikate auszugeben und zu prüfen (‚**Datenschutzsiegel**'). Obgleich solch ein freiwilliges Zertifikat keine vollständige ‚Immunität' vor der Prüfung durch eine Aufsichtsbehörde gewährt, wird dem zertifizierten Verantwortlichen bzw. Auftragsverarbeiter durch das ‚Datenschutzsiegel' ein gewisser Grad an Compliance attestiert.

Der zweite Absatz des Artikels 25, Stichwort ‚**Security by Design**' (integrierte Sicherheit), geht auf die Frage ein, ob ein Identity und Access Management-System eingerichtet werden muss.

> *„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."*

Diese Verpflichtung bezieht sich auf die Menge erhobener personenbezogener Daten, das Ausmaß der Verarbeitung, die Verwahrungsdauer sowie die Datenverfügbarkeit.

> *„Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden."*

Diese Klausel nimmt (unter anderem) **direkten Bezug auf die Funktionen eines IAM-Systems**. Zwar werden IAM-Systeme nicht explizit erwähnt, aber die Notwendigkeit eines solchen Systems zur Sicherstellung der Konformität mit der EU-DSGVO erschließt sich aus derselben Logik wie bei der Umsetzung vorausgegangener Verordnungen.

Jeder Rechtsberater in Sachen Basel III, Solvency II und PCI-DSS wird für sämtliche Standards bestätigen, **dass der Einsatz eines IAM-Systems zwar nicht konkret gefordert wird, es aber kein einziger Fall bekannt ist, in dem ein Unternehmen ohne ein solches System eine entsprechende Prüfung bestanden hätte.**

Obgleich die Anforderungen an Auftragsverarbeiter im Vergleich zum Verantwortlichen stärker eingeschränkt und auftragsbezogen erscheinen, weist die EU-DSGVO mehr Bestimmungen und Definitionen für Auftragsverarbeiter auf als für Verantwortliche.

Hintergrund dieser Schwerpunktsetzung hinsichtlich der Pflichten des Auftragsverarbeiters ist voraussichtlich die ständig wachsende Zahl an **Cloud Computing**-Szenarien. Hinzu kommt die Sorge des Gesetzgebers, der ‚Verantwortliche' könnte seine Pflichten an globale Auftragsverarbeiter übertragen, die außerhalb des Geltungsbereichs der EU-DSGVO agieren.

Die Betrachtung dieses Abschnitts der EU-DSGVO zeigt unmissverständlich, dass sich der Verantwortliche unabhängig vom konkreten Auftragsverarbeiter-Szenario hauptverantwortlich für die Einhaltung der Compliance-Pflichten zeigt. Gemäß der EU-DSGVO sind nur solche Auftragsverarbeitungsstrukturen (einschließlich der kaskadierenden Weitervermittlung an Subunternehmer) gestattet, denen eine schriftliche Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeitenden zugrunde liegt, welche die Datensicherheit durch diverse Maßnahmen sowie die Einhaltung der Anforderungen der EU-DSGVO durch den Auftragsverarbeiter gewährleistet und die Tätigkeit des Auftragsverarbeiters auf die Verarbeitung personenbezogener Daten auf Basis dokumentierter Anweisungen des Verantwortlichen beschränkt.

6. Sicherheit personenbezogener Daten

In den Ausführungen der Pflichten des Verantwortlichen und Auftragsverarbeiters finden sich zahlreiche Verweise auf Kapitel IV, Abschnitt 2 der Verordnung. Abschnitt 2 befasst sich mit dem Thema ‚Sicherheit personenbezogener Daten'. In diesem Abschnitt verpflichtet die EU-DSGVO den Verantwortlichen und Auftragsverarbeiter grundsätzlich dazu, **„geeignete technische und organisatorische Maßnahmen [zu treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.**"

In der näheren Ausführung, was in diesem Zusammenhang unter ‚angemessenen Maßnahmen' zu verstehen sei, fordert die EU-DSGVO von den Parteien, diese „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen" individuell festzulegen.

Neben diesem eher allgemeinen ‚Grundsatz' führt die Verordnung in Abschnitt 2 mehrere

Mindestvoraussetzungen auf, die zu gewährleisten sind:

- *die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
- *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;*
- *die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;*
- *ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*

Aus Sicht des Identity und Access Management ist der zweite Punkt ohne wirksames Identity Management-System nur schwer umzusetzen:

Weder kann die ‚Vertraulichkeit' effektiv gewährleistet werden, falls der Verantwortliche oder Auftragsverarbeiter das ‚Need-to-know'-Prinzip nicht umsetzt, noch lässt sich die ‚Verfügbarkeit' sicherstellen, wenn die Benutzer keinen Zugriff auf die entsprechenden IT-Systeme erhalten.

Zusätzlich wird in Artikel 32 des Abschnitts 2 gefordert:

> *„Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet."*

Dieser Passus bezieht sich nicht direkt auf die Zugriffsverwaltung, aber die angemessene Umsetzung solcher Zugriffsrechte verweist implizit auf den Einsatz eines Identity und Access Management-Systems, da **die Steuerung der Verarbeitung personenbezogener Daten weniger komplex ausfällt, wenn die Anzahl der Personen, die zur Verarbeitung personenbezogener Daten berechtigt sind, durch ein Identity Management-System begrenzt wird.**

Abschnitt 2 behandelt jedoch nicht nur Sicherheitsaspekte für die Verarbeitung von personenbezogenen Daten. In Artikel 33 dieses Abschnitts wird der Meldeprozess im Falle einer Verletzung des Schutzes personenbezogener Daten ausgeführt.

Gemäß dieses Artikels muss der Verantwortliche **die zuständige Aufsichtsbehörde und die betroffene Person (Datensubjekt) unverzüglich bzw. bis spätestens 72 Stunden nach Feststellen des Vorfalls benachrichtigen. Diese Benachrichtigung hat sämtliche Details zur Verletzung des Schutzes personenbezogener Daten zu beinhalten, z. B. die betroffenen Daten und die voraussichtlichen Konsequenzen.**

7. Aufsichtsbehörden und Sanktionen

Es gibt weltweit vermutlich eine große Zahl unwirksamer Verordnungen, da diese weder überwacht noch durch Strafen durchgesetzt werden. Bei der Ausgestaltung der EU-DSGVO wurde der Durchsetzbarkeit der Verordnung viel Aufmerksamkeit gewidmet. Somit folgt die Frage, welche Konsequenzen bei Nichtbeachtung der EU-DSGVO drohen?

Die EU-DSGVO überträgt die Aufsichtspflicht und Anwendung der Verordnung an die jeweiligen Mitgliedsstaaten. In Artikel 51 steht:

> *„Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Union erleichtert wird (im Folgenden ‚Aufsichtsbehörde').“*

Der Artikel legt darüber hinaus fest, dass diese Aufsichtsbehörden unter den Mitgliedsstaaten kooperieren müssen und unabhängig zu sein haben.

Die Aufsichtsbehörden sollen zudem dazu beitragen, Verantwortliche und Auftragsverarbeiter für die Verordnung zu sensibilisieren. Sie sollen außerdem staatlichen Institutionen in Fragen zum Datenschutz beratend zur Seite stehen.

Auch wird ihnen die Autorität zugesprochen, die Anwendung der EU-DSGVO zu überwachen und durchzusetzen. Hierfür erhalten die Aufsichtsbehörden eine Reihe an Kompetenzen, die in Artikel 58 aufgeführt sind.

→ Aufsichtsbehörden dürfen bei Verantwortlichen und Auftragsverarbeitern Nachforschungen anstellen, um die Einhaltung der EU-DSGVO zu prüfen.
Im Rahmen solcher Untersuchungen müssen Verantwortliche und Auftragsverarbeiter vollständig kooperieren und die angeforderten Informationen bereitstellen.

Aufsichtsbehörden haben die Möglichkeit, Verantwortliche und Auftragsverarbeiter zu warnen bzw. zu verwarnen, um Verstöße gegen die EU-DSGVO zu verhindern bzw. zu unterbinden. Im Falle gravierender Verstöße gegen die EU-DSGVO haben Aufsichtsbehörden die Befugnis, **harte Sanktionen zu verhängen**:

> *(d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen;*
> *(e) den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person entsprechend zu benachrichtigen;*
> *(f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,*
> *(g) die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß den Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten gemäß Artikel 17 Absatz 2 und Artikel 19 offengelegt wurden, über solche Maßnahmen anzuordnen,*
> *(h) eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine gemäß den Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden,*
> *(i) eine Geldbuße gemäß Artikel 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls,*
> *(j) die Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation anzuordnen.*

Insbesondere die Klausel (i) bezüglich dem Verhängen von Geldbußen sorgt im Vorfeld des Inkrafttretens der EU-DSGVO für große Aufmerksamkeit. Im Artikel 83 wird sehr detailliert beschrieben, **welche Geldbuße für die jeweilige Verletzung anzusetzen ist.** Von allen möglichen Geldbußen ist die in Paragraph 5 beschriebene die folgenschwerste:

> *Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:*
> *a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;*
> *b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;*
> *c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;*
> *d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;*
> *e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.3;*

Somit muss jedes Unternehmen, das in den Anwendungsbereich der EU-DSGVO fällt, mit möglichen Sanktionen in Höhe von bis zu 20 Mio. Euro bzw. bis zu 4 % des weltweit erzielten Jahresumsatzes rechnen.

Hier ein Beispiel, um die Tragweite dieser Klausel zu unterstreichen: Gegen ein global aktives Unternehmen mit einem jährlichen Umsatz von 500 Mio. Euro kann für die Verletzung der EU-DSGVO ein Bußgeld in Höhe von bis zu 20 Mio. Euro verhängt werden. Ist der Jahresumsatz höher, können entsprechend höhere Geldbußen verhängt werden. Hieraus wird ersichtlich, dass **Verstoße gegen die EU-DSGVO für jeden Vorstand ein hohes Gefahrenpotenzial bergen.**

8. Zusammenfassung aus IAM-Sicht

In der EU-DSGVO finden sich zahlreiche Hinweise, welche die Notwendigkeit von Identity & Access Management-Systemen andeuten. Wie auch in anderen Bereichen dieser Verordnung finden sich hierfür jedoch keine expliziten Verweise. Was viele Verantwortliche und Auftragsverarbeiter vermissen dürften sind klare Aussagen zu konkreten Erwartungen. Vielmehr fordert die EU-DSGVO Verantwortliche dazu auf, über die Verarbeitung personenbezogener Daten nachzudenken.

Dies beinhaltet den Zweck der Verarbeitung, angemessene Schutzmaßnahmen und den Ablauf der Verarbeitung. Aber eine Verordnung, die vornehmlich das Zielszenario und die angestrebte Einstellung von Organisationen beschreibt, liefert keine konkreten Hinweise dazu, wie die Forderungen umzusetzen sind. Somit finden sich keine Vorschriften wie bspw. „zum Schutz personenbezogener Daten ist der Einsatz eines Identity & Access Management-Systems verpflichtend."

Allerdings stellt die EU-DSGVO diverse Forderungen auf, die sich am besten mit einem IAM-System umsetzen lassen:

Rechenschaftspflicht

Diese ‚Rechenschaftspflicht' stellt eine zentrale/konstituierende Säule der EU-DSGVO dar. In Kapitel II, Artikel 5, Klausel 2, fordert die EU-DSGVO:

> *„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (‚Rechenschaftspflicht')."*

In Paragraph 1 werden die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten beschrieben. Aus dieser Beschreibung lassen sich drei Kernbereiche ableiten, in denen spezielle Forderungen gestellt werden:

1. Definition der Menge der verarbeiteten personenbezogenen Daten
   Paragraph 1, Grundsätze (b) und (c)
   → Compliance-Anforderungen in Bezug auf Abläufe

2. Richtigkeit, Schutz und Pseudonymisierung der verarbeiteten personenbezogenen Daten
   Paragraph 1, Grundsätze (d) (e) und (f)
   → IT-Anforderungen / Sicherheit der Repositories und Archivsysteme

3. Kontrolle des Zugriffs auf verarbeitete personenbezogene Daten
   Paragraph 1, Grundsatz (f)
   → **Identity & Access Management-Anforderungen**

Analog zu anderen rechtlichen Rahmenbedingungen **impliziert die Forderung nach einer ‚Rechenschaftspflicht' in diesem Kontext, dass die konforme Handhabung (und damit einhergehend der Zugriff auf) personenbezogene(r) Daten durchgehend sichergestellt ist.** Dies ist nur durch Implementierung eines effektiven Identity Management-Systems möglich.

Security by Design

Das allgemeine Konzept der ‚Rechenschaftspflicht' wird im Abschnitt über die Pflichten des Verantwortlichen eingeführt.
In Artikel 25, Paragraph 2, schreibt die EU-DSGVO vor:

> *„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. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden."*

Dieser Passus wirkt sich auf mehrere Bereiche und Prozesse des ‚Verantwortlichen' aus: Was „die Menge der erhobenen personenbezogenen Daten [und] den Umfang ihrer Verarbeitung" anbelangt, so erfordert dies in der Regel die Absprache zwischen den Geschäftsbereichen, der Compliance-Abteilung und der Geschäftsleitung. Die explizite Forderung bezüglich des **Zugriffs ist zweifelsohne eine Aufgabe, für die es eines leistungsfähigen Access Governance/Access Management-Systems bedarf**.

In diesem Kontext ist in der EU-DSGVO von technischen und organisatorischen Maßnahmen die Rede. Dies entspricht der allgemein akzeptierten Meinung, dass jede IAM-Implementierung ein Mischprojekt darstellt, das sowohl technische als auch organisatorische Aspekte beinhaltet. „Data Protection by Design" ist vermutlich der konkreteste Verweis in der gesamten EU-DSGVO auf die Notwendigkeit eines IAM-Systems.

Sicherheit personenbezogener Daten / Sicherheit der Verarbeitung

In Kapitel IV, Abschnitt 2, Artikel 32, Paragraph 1(b) schreibt die EU-DSGVO vor: „…der Verantwortliche und der Auftragsverarbeiter [treffen] geeignete technische und organisatorische Maßnahmen, um …"

> *„die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;"*

Selbst eine hartnäckige Suche wird keine andere Technologie zutage führen, mit der sich der Widerspruch zwischen hoher Vertraulichkeit und schneller Verfügbarkeit überwinden ließe. Tatsächlich befasst sich die komplette EU-DSGVO mit dem naturgegebenen **Konflikt zwischen der geschäftsbedingt erforderlichen Verwendung personenbezogener Daten und dem Ziel, diese sowohl mengenmäßig als auch im Zugriff soweit wie möglich einzuschränken.** Diese widersprüchlichen Anforderungen lassen sich nur durch ein **Identity & Access Management-System** erfüllen.

Der Zugriff auf personenbezogene Daten muss auf einen bestimmten Zweck beschränkt sein – mit IAM gelingt es Organisationen, den Zugriff auf diejenigen Personen zu beschränken, die diesem Zweck dienen.

Sicherheit der Verarbeitung

Die folgende Klausel erweckt den Eindruck, sich auf Identity Management zu beziehen, jedoch ist dies nicht der Fall. Somit ist sie ein gutes Beispiel dafür, dass selbst IAM nicht jede Schwachstelle in Bezug auf die Verarbeitung personenbezogener Daten beheben kann. Artikel 32 der EU-DSGVO fordert:

> *„Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.“*

Hierbei geht es um die Herausforderung, Personen mit Zugriff auf personenbezogene Daten (dies lässt sich mit einem IAM-System lösen) diesen Zugriff nur dann erhalten, wenn sie dazu angewiesen werden (jenseits des Funktionsumfangs eines IAM-Systems).

Logischerweise ist ein IAM-System nicht in der Lage, die Intention eines Benutzers zu prüfen, der von eine Zugriffsberechtigung Gebrauch macht, aber dennoch ist es möglich, durch die Implementierung eines IAM-Systems diese Herausforderung zumindest teilweise zu bewältigen: **Durch sinnvolles Einschränken der Benutzer, die Zugriff auf personenbezogene Daten erhalten, wird die Überwachung/Kontrolle der Aktivitäten des verbleibenden Benutzerstamms erheblich realistischer**, als dies bei einem weitaus weniger transparenten Zugriff der Fall wäre.

Identity that works: Passende Identity and Access Management Lösungen für dynamische Unternehmen

Mit der Identity Access Management Suite von Beta Systems steuern und überwachen Unternehmen den Zugriff auf Daten und Anwendungen gemäß der organisatorischen Anforderungen und fachlichen Rolle eines jeden Benutzers.

Beta Systems IAM Software AG

Alt-Moabit 90d | 10559 Berlin | Germany
Tel: +49 (0) 30 726 118-0 | Fax: +49 (0) 30 726 118-800
iam@betasystems.com | www.betasystems-iam.com

Die Beta Systems IAM Software AG ist der größte unabhängige europäische Anbieter von Identity- und Access- Management-Lösungen (IAM) für Unternehmen. Seit über 30 Jahren unterstützt Beta Systems seine Kunden aus den Bereichen Finanzdienstleistungen, Fertigung, Handel und IT-Dienstleistungen mit Softwareentwicklung und Support „Made in Germany“.