



Stellungnahme zum Entwurf einer EU-Datenschutzgrundverordnung der Europäischen Kommission vom 25.01.2012 (VO-Entwurf)

Das angestrebte Ziel der EU-Kommission, ein einheitliches hohes Datenschutzniveau in der EU zu erreichen, wird begrüßt. Der vorliegende Verordnungsentwurf muss jedoch in den angeführten Punkten geändert werden, um die notwendige Klarheit, Rechtssicherheit und Praktikabilität zu gewährleisten. Andernfalls sehen wir wesentliche Abläufe in unseren Unternehmen gefährdet.

Kernthesen:

1. Die Volkswagen AG begrüßt das Ziel der EU-Kommission, ein einheitliches hohes Datenschutzniveau für alle zu schaffen, das in der ganzen EU in gleichem Maße gilt und gleiche Wettbewerbsbedingungen schafft. Der VO-Entwurf lässt jedoch klare Definitionen und rechtssichere Gestaltung vermissen.
2. Die Volkswagen AG befürwortet den Erhalt von Betriebsvereinbarungen als Rechtsgrundlage und Regelungsinstrument des Beschäftigtendatenschutzes.
3. Freiwillige, informierte Einwilligungen der Beschäftigten müssen als Erlaubnisgrundlage für die Verarbeitung von Daten weiterhin zulässig sein.
4. Der Datentransfer innerhalb eines Konzerns ist im VO-Entwurf unzureichend geregelt.
5. Der VO-Entwurf unterscheidet nicht zwischen personenbezogenen Daten, die der Durchführung des Arbeitsverhältnisses dienen, und den Gesundheitsdaten der Beschäftigten. Der VO-Entwurf muss vorsehen, dass personenbezogene Gesundheitsdaten dem Arbeitgeber nicht zugänglich sein dürfen.
6. In der Verordnung müssen die Rechtsgrundlagen Tarifverträge, Betriebsvereinbarung und individuelle Einwilligung für die Verarbeitung von Arbeitnehmerdaten eindeutig vorgesehen werden. Eine Notwendigkeit für die Öffnungsklausel gemäß Art. 82 VO-Entwurf besteht nicht.
7. Die in der Verordnung vorgesehenen Pflichten, den Umgang mit Daten nachvollziehbar zu dokumentieren (Art. 5a, 5f VO-Entwurf), sind ausufernd, und sie binden unnötig Ressourcen.
8. Die Volkswagen AG hält den Auskunftsanspruch nach Art. 15 VO-Entwurf für zu bürokratisch.
9. Die Definition der personenbezogenen Daten (siehe Art. 4, Abs. 1 VO-Entwurf) ist zu weit gefasst.
10. Der VO-Entwurf erhöht die Gefahr von Compliance-Verstößen.
11. Die Volkswagen AG hält die Sanktionen bei Verstößen gegen die Verordnung für undifferenziert.
12. Die Definition eines neuen Schwellenwertes, ab dem die Bestellung eines Datenschutzbeauftragten erforderlich sein soll, ist im Sinne des Bundesdatenschutzgesetzes ein Rückschritt.



Erläuterungen

Zu Ziffer 1: Fehlen von klaren Definitionen und rechtssicherer Gestaltung

Die Volkswagen AG begrüßt das Ziel der EU-Kommission, ein einheitliches hohes Datenschutzniveau für alle zu schaffen, das in der ganzen EU in gleichem Maße gilt und gleiche Wettbewerbsbedingungen schafft. Der vorliegende Entwurf lässt jedoch klare Definitionen und rechtssichere Gestaltung vermissen.

Als weltweit tätiger Konzern, dessen Unternehmen Daten nur im Kontext der Herstellung und des Vertriebs ihrer Produkte und der dafür nötigen Beschäftigungsverhältnisse erheben und verarbeiten, deren unternehmerische Hauptzwecke jedoch nicht das geschäftsmäßige Sammeln von Daten und der Handel mit Daten sind, besteht ein zentrales Interesse, den Umgang mit Daten so effizient wie möglich, natürlich unter voller Beachtung des grundrechtlich gebotenen Datenschutzes, zu gestalten.

Der von der EU-Kommission im Januar 2012 vorgelegte Entwurf zu einer Verordnung, die den Schutz personenbezogener Daten in der EU vereinheitlichen soll, erfüllt diese Kriterien jedoch nicht in vollem Umfang.

Würde er in der vorliegenden Fassung rechtsverbindlich, könnten personenbezogene Daten nur noch eingeschränkt rechtssicher verarbeitet werden. Dies hätte gravierende Auswirkungen auf die Verwendung von Daten z. B. für Personalplanungs- und entwicklungsprogramme sowie die Organisation und Durchführung von dienstlich veranlassten Auslandsaufenthalten von Beschäftigten und ihrer Familienangehörigen. Darüber hinaus wären vielfältige betriebliche Sozialleistungen nicht mehr möglich (z.B. freiwillige Gesundheitsangebote, Umfänge der betrieblichen Altersvorsorge). Schließlich wäre ein effizienter konzerninterner Datenaustausch über Staatsgrenzen hinweg eingeschränkt.

Zu Ziffer 2: Rechtsgrundlagen im Beschäftigungsverhältnis

Volkswagen befürwortet den Erhalt von Betriebsvereinbarungen als Rechtsgrundlage und Regelungsinstrument des Beschäftigtendatenschutzes.

In fast allen Unternehmensbereichen entstehen personenbezogene Daten im Kontext des Arbeitnehmer – Arbeitgeberverhältnisses. Der VO-Entwurf sieht vor, dass die Verarbeitung dieser Daten nur noch zulässig ist, wenn ein Gesetz dies vorsieht bzw. erlaubt.

In Deutschland wird ein erheblicher Teil der Kollektivvereinbarungen auf betrieblicher Ebene abgeschlossen. Der Regelungsgehalt und die Regelungsmöglichkeiten durch Betriebsvereinbarungen sind im Hinblick auf ihren Charakter als Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten unverzichtbar.



In der Verordnung muss eindeutig formuliert sein, dass Tarifverträge und Betriebsvereinbarungen Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten darstellen. Dies ist im aktuellen Entwurf zur Novellierung des Bundesdatenschutzgesetzes zum Arbeitnehmerdatenschutz vorgesehen.

Zu Ziffer 3: Rechtsgrundlagen im Beschäftigungsverhältnis

Freiwillige, informierte Einwilligungen der Beschäftigten müssen als Erlaubnisgrundlage für die Verarbeitung von Daten weiterhin zulässig sein.

Nach Erwägungsgrund 34 und Art. 7 Abs. 4 des VO-Entwurfes bietet eine Einwilligung zur Datenverarbeitung zwischen Personen, zwischen denen ein erhebliches Ungleichgewicht besteht – ausdrücklich erwähnt wird das Verhältnis Arbeitgeber-Arbeitnehmer – keine Rechtsgrundlage für eine personenbezogene Datenverarbeitung.

Eine solche Basis für eine rechtssichere Verarbeitung personenbezogener Daten ist jedoch unerlässlich. Die Einschränkung würde zu einer übermäßigen Bevormundung und dem Abbau von Gestaltungsrechten des Betroffenen und der datenverarbeitenden Stelle führen. Die Einwilligung stellt eine jahrzehntelange unangefochtene Praxis dar und umfasst viele Sachverhalte, welche bei der Durchführung eines Beschäftigungsverhältnisses - auch im Interesse der Beschäftigten - auftreten, wie z.B.:

- Personalplanungs- und -entwicklungsprogramme,
- Organisation und Durchführung von Auslandsaufenthalten von Beschäftigten und Familienangehörigen,
- Betriebliches Eingliederungsmanagement,
- Eignungsuntersuchungen,
- Veröffentlichung von Mitarbeiterfotos im Intranet und Internet,
- betriebliche Sozialleistungen, wie Kindergärten, Kinderbetreuung, Gesundheitsdienstleistungen, betriebliche Altersvorsorge, Unterstützungskassen,
- Durchführung von gemeinsamen Spendenaktionen der Beschäftigten und des Unternehmens für soziale Zwecke und Menschen in akuten Notsituationen (z.B. bei Naturkatastrophen).

Zu Ziffer 4: Konzerninterner Transfer personenbezogener Daten

Der Datentransfer innerhalb eines Konzerns ist im VO-Entwurf unzureichend geregelt.

Der Volkswagenkonzern und seine Teilkonzerne sind international weltweit tätig. Es findet ein ständiger Wechsel von Beschäftigten zwischen Konzernunternehmen statt. Zudem arbeiten Beschäftigte von einzelnen Unternehmen arbeitsteilig zusammen, z.B. um Synergieeffekte zu generieren. Hieraus entsteht die Notwendigkeit, Beschäftigtendaten effizient und schnell auszutauschen. Der Datentransfer innerhalb eines Konzerns ist im VO-Entwurf jedoch nur unzureichend geregelt (vgl. Art. 40 VO-Entwurf und Erwä-



gungsgrund 19). Er wird den tatsächlichen Anforderungen des Volkswagenkonzerns nicht gerecht. Das neue Datenschutzrecht sollte hier Vereinfachungen für Konzerne einführen.

Unverzichtbar ist auch hier, dass Rechtssicherheit durch den Abschluss von Betriebsvereinbarungen und individuellen Vereinbarungen möglich ist.

Wenn die EU-Kommission, wie in Art. 41 vorgesehen, die alleinige Kompetenz hat, darüber zu entscheiden, ob ein Staat ein angemessenes Datenschutzniveau aufweist, kann für ein Unternehmen eine höchst prekäre Situation entstehen: falls ein Staat auf die schwarze Liste gesetzt wird, ist jeglicher Datentransfer mit diesem Staat untersagt, dem Unternehmen folglich der Austausch mit einer Tochter/Niederlassung o.ä. Angesichts der Tragweite eines solchen „Angemessenheitsbeschlusses“ ist er abzulehnen.

Wenn die EU-Kommission keinen Beschluss über das Datenschutzniveau eines Drittstaats fasst, besteht nach dem VO-Entwurf als „geeignete Garantie“ für eine adäquate Datenverarbeitung die Möglichkeit, „verbindliche unternehmensinterne Vorschriften“ (Art. 43) zu erstellen. Diese Möglichkeit ist im Prinzip zu begrüßen. Die vorgesehenen Verfahren sind jedoch teils unklar und viel zu aufwändig; es ist abzulehnen, dass sowohl die nationale Aufsichtsbehörde, die EU-Kommission und die Europäische Datenschutzbehörde zustimmen müssen, also in jedem Fall das Kohärenzverfahren nach Art. 58 angewandt werden muss. Und sollten gemäß der Öffnungsklausel nach wie vor nationale Gesetze beim Beschäftigtendatenschutz entstehen, wäre der Vorteil umgreifender Vorschriften innerhalb eines Konzerns zumindest erheblich vermindert; die Ressourcenbindung, die das Durchlaufen eines solchen Anerkennungsverfahrens für konzerninterne verbindliche Vorschriften mit sich bringt, wäre nicht wenigstens durch die substantielle Erleichterung, nur noch mit einem Datenschutzregime zu tun zu haben, besser ausbalanciert. Außerdem wäre im deutschen Kontext zu prüfen, ob ein solches auf die EU-Ebene zentriertes Verfahren kompatibel mit Mitbestimmungsrechten ist.

Der Ansatz des VO-Entwurfs, den konzerninternen Datentransfer zu erleichtern, geht in die richtige Richtung. Gleichwohl lässt die EU-Kommission bislang die Chance ungenutzt, eine Regelung zum konzerninternen Datentransfer zu schaffen, die Rechtssicherheit beim Datentransfer sowohl innerhalb als auch außerhalb der EU gewährleistet.

Auch für den grenzüberschreitenden konzerninternen Datenverkehr via verbindlicher unternehmensinterner Vorschriften möchte die EU-Kommission die Ermächtigung zu delegierten Rechtsakten haben; „Kriterien und Anforderungen“ dafür festlegen zu können, stellt keine unwesentliche Kompetenz dar und deshalb ist diese Ermächtigung zu streichen.



Zu Ziffer 5: Gesundheitsdaten in Arbeitsmedizin und Arbeitsschutz

Der VO-Entwurf unterscheidet nicht zwischen personenbezogenen Daten, die der Durchführung des Arbeitsverhältnisses dienen, und den Gesundheitsdaten der Beschäftigten.

Der VO-Entwurf muss vorsehen, dass personenbezogene Gesundheitsdaten dem Arbeitgeber nicht zugänglich sein dürfen.

Arbeitsmedizin und Arbeitsschutz spielen in unseren Unternehmen eine große Rolle. Deshalb begrüßen wir es, dass der VO-Entwurf die Verarbeitung gesundheitsbezogener Daten - auf der Basis der nationalen Gesetzesvorschriften – ausdrücklich vorsieht. Wichtig ist dabei, den Schutz individueller Gesundheitsdaten der Beschäftigten und den Schutz Dritter in einen interessensgerechten Ausgleich zu bringen. Auch ist es im medizinischen Kontext im Interesse des Patienten(!), Daten über längere Zeiten zu speichern; das „Recht auf Vergessenwerden“ muss in dieser Hinsicht eingeschränkt werden.

In der Arbeitsmedizin spielt Prävention eine große Rolle. Entsprechend unterliegen im deutschen Arbeitsschutzrecht Werksärzte der Verpflichtung, arbeitsmedizinische Befunde beschäftigungsgruppenspezifisch zu analysieren. Datendokumentation und gruppenbezogene -auswertung zu epidemiologischen Zwecken muss deshalb auch weiterhin als Grund für eine rechtssichere Datenverarbeitung gelten.

Dasselbe gilt für Datenverarbeitung bei der arbeitsmedizinischen Vorsorge, um die erst 2009 in Deutschland neu gefassten Standards halten zu können.

In Arbeitsmedizin und Arbeitsschutz werden besonders sensible Daten erhoben und verarbeitet. Es bedarf zwingend sicherer Rechtsgrundlagen dafür, d.h. u.a. einer begrifflichen Abgrenzung von personenbezogenen Beschäftigtendaten des Arbeitgebers und von Gesundheitsdaten, die im Rahmen arbeitsmedizinischer Betreuung erhoben werden. Solche Daten dürfen dem Arbeitgeber nicht zugänglich sein – was die Verordnung vorschreiben sollte.

Teilweise wird der Umgang mit Gesundheitsdaten auch in unseren Unternehmen durch Betriebsvereinbarungen geregelt. Deshalb sind Betriebsvereinbarungen als eine mögliche Rechtsgrundlage ebenso nötig für uns an dieser Stelle wie die Möglichkeit, dass ein Arbeitnehmer durch seine individuelle Einwilligung freiwillige Gesundheitsdienstleistungen, die in der Volkswagen AG angeboten werden (z. B. Impfungen), in Anspruch nehmen kann.

Im VO-Entwurf vorgeschlagene Verfahren (Art. 33, Art. 34 VO-Entwurf) zur Datenschutz-Folgeabschätzung beim Umgang mit Gesundheitsdaten, zur vorherigen Genehmigung und zur Zurateziehung der Aufsichtsbehörde wären außerordentlich aufwändig, auslegungsbedürftig und würden unnötig Ressourcen binden.

Abzulehnen ist, dass die EU-Kommission hier zu delegierten Rechtsakten ermächtigt wird (Art. 81 Abs. 3 VO-Entwurf), „Kriterien und Anforderungen in Bezug auf die Garantien für die Verarbeitung personenbezogener Daten ... festzulegen“. Eine solche Definition umfasst mehr als eine „nicht wesentliche Vorschrift eines Gesetzgebungsaktes“, die Charakteristikum eines delegierten Rechtsaktes sein soll.



Zu Ziffer 6: Öffnungsklausel in Art. 82

In der Verordnung müssen die Rechtsgrundlagen Tarifvertrag, Betriebsvereinbarung und individuelle Einwilligung für die Verarbeitung von Beschäftigtendaten eindeutig vorgesehen werden; die Notwendigkeit für eine Öffnungsklausel gem. Art. 82 VO-Entwurf besteht nicht.

Erwägungsgrund 124 und Art. 82 VO-Entwurf sehen bei Datenverarbeitung im Beschäftigungskontext eine Öffnungsklausel (im Übrigen die einzige im VO-Entwurf) vor: Mitgliedstaaten wird erlaubt, „in den Grenzen dieser Verordnung“ ein nationales Gesetz zur Verarbeitung solcher Daten zu erlassen. Da die Verordnung die Datenverarbeitung generell umfänglich regelt und Rechtsvorrang hat, die EU-Kommission in 26 Sachverhalten (zusätzlich einer entsprechenden Generalklausel durch Art. 86 VO-Entwurf) die Ermächtigung zu delegierten Rechtsakten erreichen will, ist höchst unklar, welcher Spielraum für nationale Regelungen überhaupt noch bestehen kann. Dazu kommt, dass gerade auch EU-weit einheitliche Standards und Regeln für den Schutz von Beschäftigtendaten für Unternehmen, die in mehreren EU-Mitgliedstaaten Produktionsstätten und Geschäftssitze haben, wesentliche Arbeitserleichterungen und Kosteneinsparungen mit sich bringen und den konzerninternen Datenverkehr erheblich erleichtern würden.

Die Öffnungsklausel widerspricht dem Ziel, das Datenschutzrecht zu vereinfachen, da der Beschäftigtendatenschutz in vielen nationalen Regelwerken verankert würde. Die angestrebte Harmonisierung des Datenschutzrechts würde in einem zentralen Bereich nicht erreicht.

Eine solche besteht auch nicht dafür, der EU-Kommission hier delegierte Rechtsakte zu ermöglichen: „Kriterien und Anforderungen in Bezug auf die Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext“ festlegen zu können, stellt keine unwesentliche Vorschrift des Gesetzgebungsaktes dar.

Zu Ziffer 7: Dokumentationspflichten

Die in dem VO-Entwurf vorgesehenen Pflichten, den Umgang mit Daten nachvollziehbar zu dokumentieren (Art. 5 lit. a, lit. f, Art. 28), sind ausufernd und sie binden unnötig Ressourcen.

Es ist nicht klar, wie die geforderte „Nachvollziehbarkeit“ (Art. 5 lit. a, lit. f VO-Entwurf) der Verarbeitung für den Betroffenen umgesetzt und dokumentiert werden soll.

Generell sind die in der Verordnung vorgesehenen Pflichten, den Umgang mit Daten zu dokumentieren, ausufernd und sie binden unnötig Ressourcen. Sie müssen einerseits effizienter abgefasst werden, andererseits Spezifika besonderer Daten (Gesundheit) berücksichtigen.

Nach dem VO-Entwurf werden die datenverarbeitenden Unternehmen mit einer Vielzahl von weiteren Informations- und Dokumentationspflichten sowie Pflichten zur Erstellung von Folgenabschätzungen (Art. 33) und Genehmigungserfordernissen (Art. 34) belastet. Es sollte jede formale Anforderung einer Aufwand-Nutzen-Prüfung unterzogen werden.



Die Meldepflichten bei Datenpannen (Art. 31) müssen wie bisher auf wesentliche Ereignisse begrenzt werden, d.h. nur dann erfolgen, wenn schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Zu Ziffer 8: Auskunftspflichten

Volkswagen hält den Auskunftsanspruch nach Art. 15 VO-Entwurf für zu bürokratisch.

Um den Auskunftsanspruch zu erfüllen, müssten die betreffenden Daten aus verschiedenen Quellen zusammengeführt werden (Einwilligungen werden nicht zentral gespeichert, sondern dem jeweiligen Zweck entsprechend im Fachbereich aufbewahrt). Dieser Vorgang wäre extrem bürokratisch und zeitaufwändig. Zudem müssten die so erstellten Auskunftsprofile zu Beweis Zwecken dauerhaft gespeichert werden, um im Zweifel nachweisen zu können, dass der Auskunftsanspruch gegenüber dem jeweiligen Beschäftigten erfüllt wurde.

Zu Ziffer 9: Definition Personenbezogene Daten

Die Definition der personenbezogenen Daten (Art. 4 Abs. 1 und Abs. 2) ist zu weit gefasst.

Sinnvoller ist es, unter personenbezogenen Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) zu verstehen, also die Definition des Bundesdatenschutzgesetzes zugrunde zu legen. Außerdem sollten die Aspekte der Pseudonymisierung und Anonymisierung von zu verarbeitenden personenbezogenen Daten aufgenommen werden. Noch deutlicher sollte herausgestellt werden, dass anonymisierte Daten keine personenbezogenen Daten sind. Für die Verarbeitung pseudonymisierter Daten sollten gezielt erleichterte Bedingungen geschaffen werden, wie dies im deutschen Datenschutzrecht schon heute der Fall ist.

Zu Ziffer 10: Gefahr von Compliance-Verstößen

Der VO-Entwurf erhöht die Gefahr von Compliance-Verstößen.

Der VO-Entwurf sieht als Voraussetzung für die rechtmäßige Verarbeitung personenbezogener Daten auch eine nachhaltig zu dokumentierende Interessenabwägung durch die Unternehmen vor. Dies führt zu einem erheblichen, zusätzlichen Dokumentationsaufwand und zu einem gesteigerten Maß an Rechtsunsicherheit. Dies dürfte die Gefahr von Compliance-Verstößen erhöhen.



Zu Ziffer 11: Sanktionen

Volkswagen hält die Sanktionen bei Verstößen gegen die Verordnung für undifferenziert.

Der VO-Entwurf atmet den Geist einer lex facebook, also eines Regelungsentwurfs für Unternehmen, die vom Sammeln und Vermarkten von Daten leben. Der Umgang mit personenbezogenen Daten in Unternehmen, in denen dies nötiges Beiwerk für die Herstellung und den Vertrieb realer Produkte ist, unterscheidet sich hiervon maßgeblich – er ist nicht Basis des Unternehmensergebnisses.

Dem muss der VO-Entwurf durchgehend Rechnung tragen. So z.B. bei den Sanktionen, die allein an den weltweiten Jahresumsatz gebunden werden – adäquater wäre, Fahrlässigkeit oder Vorsatz zu bewerten, und zu differenzieren, ob ein formeller Verstoß oder ein materieller Verstoß vorliegt, und ob der Verstoß mit Bereicherungs- oder Gewinnerzielungsabsicht erfolgte.

Richtig ist, dass die Verletzung des Schutzes personenbezogener Daten geregelt werden muss.

Anders als es die Verordnung jedoch vorsieht, muss dies angemessen sein, d.h. dabei differenziert werden nach der Schwere der Verletzung (z.B. fahrlässig, Berufsgeheimnis verletzend, vorsätzlich, Straftat) und entsprechend müssen die Mitteilungspflichten und –fristen an Aufsichtsbehörden und Betroffene geregelt werden.

Die strenger Sanktionen von bis zu 2% des weltweiten Jahresumsatzes sollten vor dem Hintergrund geprüft werden, dass die Sanktionen in dieser Größenordnung ungeachtet von Vorsatz, Fahrlässigkeit und Geschäftszweck des Unternehmens formuliert sind.

Zu Ziffer 12: Pflicht zur Bestellung eines Datenschutzbeauftragten

Die Definition eines neuen Schwellenwertes, ab dem die Bestellung eines Datenschutzbeauftragten erforderlich sein soll, ist im Sinne des BDSG ein Rückschritt.

Statt des bislang in Deutschland geltenden Wertes von mehr als 9 Beschäftigten, die mit personenbezogenen Daten arbeiten, soll nun eine generelle Grenze ab 250 Mitarbeitern eingeführt werden – ohne Berücksichtigung des Geschäftszweckes des Unternehmens.

Aus Konzernsicht hat sich das Instrument des betrieblichen Datenschutzbeauftragten in Deutschland sehr bewährt. Er nimmt eine wichtige Funktion in der Selbstkontrolle wahr und hilft, gesetzeskonforme Datenverarbeitungen zu betreiben. Eine Absenkung des Schwellenwertes könnte jedenfalls in Deutschland eine Verschlechterung des Datenschutzes zur Folge haben.