Verwaltungsrundschau
Zeitschrift für Verwaltung in Praxis und Wissenschaft

70. Jahrgang · Heft 3 · März 2024

Schriftleitung: Rechtsanwalt Steuerberater Prof. Dr. Jens M. Schmittmann, Veronikastraße 16, 45131 Essen

Prof. Rainer Kirchdörfer und Dr. Gisela Meister-Scheufelen, Stuttgart*

Länderübergreifend hohe Bürokratiebelastung durch die EU-Datenschutzgrundverordnung

Einführung

Die Stiftung Familienunternehmen hat die Bürokratiebelastung von Unternehmen in **Deutschland, Frankreich, Italien und Österreich** durch die A1-Bescheinigung, die Entsenderichtlinie, die EU-Datenschutzgrundverordnung und das Transparenzregister untersuchen lassen.[1] Geprüft wurde jeweils, welche Bürokratiebelastung zusätzlich auf nationales Recht zurückzuführen ist und inwieweit der jeweilige Verwaltungsvollzug zu spezifischen Bürokratiekosten führt. Mit dem Vergleich der Regelungsebene wurde das Centrum für Europäische Politik (CEP) und mit der praktischen Umsetzung die Prognos AG beauftragt. Der Normenkontrollrat Baden-Württemberg hat die Studie mitinitiiert und unterstützt.

In diesem Beitrag soll auf die Ergebnisse des Vergleichs der Bürokratiebelastung durch die EU-Datenschutzgrundverordnung (DSGVO) in den vier Ländern eingegangen und Vereinfachungsvorschläge unterbreitet werden.[2]

Die **EU-Verordnung trat im Mai 2018 in Kraft** und gilt unmittelbar in allen Mitgliedstaaten der EU. Sie dient dem Schutz der Grundrechte und -freiheiten der Personen, deren personenbezogene Daten verarbeitet werden. Ferner soll sie den freien Verkehr von personenbezogenen Daten gewährleisten.

A. Untersuchungsgegenstand

Die Studie vergleicht die Bürokratiebelastungen der Unternehmen in Deutschland, Frankreich, Italien und Österreich, die ihnen durch die rechtlichen Vorgaben und den Verwaltungsvollzug dadurch entstehen, dass sie

- ein Verzeichnis der Verarbeitungstätigkeiten personenbezogener Daten entsprechend Art. 30 DSGVO erstellen und führen müssen (z. B. die Verarbeitung der Daten der Mitarbeiter in der Lohnbuchhaltung zum Zweck der Gehaltsauszahlung) und
- verpflichtet sind, Verletzungen des Schutzes personenbezogener Daten bei der zuständigen Aufsichtsbehörde nach Art. 33 DSGVO zu melden.

Für die Studie wurde damit jeweils eine Norm ausgewählt, die eine planbare und fortdauernde Tätigkeit nach sich zieht, und eine solche, in der ad hoc gehandelt werden muss.

B. Die Verpflichtung, ein Verzeichnis über die Verarbeitung personenbezogener Daten zu führen (Art. 30 DSGVO)

Die EU-Verordnung verlangt, dass Unternehmen sämtliche Verarbeitungstätigkeiten, die personenbezogene Daten betreffen, erfassen, in ein Verzeichnis aufnehmen und dies aktuell halten. Darunter fällt, die verarbeiteten Daten, betroffenen Personen und Empfänger der Daten zu beschreiben. In Deutschland und Frankreich können die betroffenen Personen und Empfänger als Kategorien beschrieben werden, z. B. Mitarbeiter, Betriebsrat, Kunden oder Lieferanten. Des Weiteren müssen u. a. der Name und die Kontaktdaten des für die Verarbeitung Verantwortlichen aufgeführt werden sowie der Zweck der Verarbeitung und die Fristen, wann Daten gelöscht werden sollen.

I. In geringem Umfang Gold Plating

Gold Plating, also zusätzliche länderspezifische regulatorische Anforderungen, die über Art. 30 DSGVO hinausgehen, wurden in den vier Vergleichsländer in geringem Umfang festgestellt. Insbesondere Deutschland und Frankreich verlangen zusätzliche Informationen. So müssen in dem Verzeichnis die Serien- und Referenznummern der Verarbeitungstätigkeiten, das Datum, wann die jeweilige Verarbeitungstätigkeit eingeführt und zuletzt geändert wurde, der Name der zuständigen Abteilung des für die Verarbeitung Verantwortlichen und der Name des operativ verantwortlichen Ansprechpartners aufgeführt werden. Nach Auskunft der interviewten Unternehmen

* *Prof. Rainer Kirchdörfer*, Vorstand der Stiftung Familienunternehmen und Partner der Sozietät Hennerkes, Kirchdörfer & Lorz; *Dr. Gisela Meister-Scheufelen*, Vorsitzende des Normenkontrollrats Baden-Württemberg 2018-2022.

[1] Stiftung Familienunternehmen (eds.): Regulatory and financial burdens of EU legislation in four Member States – a comparative study, Vol. 1 – Vol. 4, Munich 2022-2023, www.familienunternehmen.de.

[2] Stiftung Familienunternehmen (eds.): Vol. 4: Burdens arising from Art. 30 and 33 of the General Data Protection Regulation, Munich 2023, www.familienunternehmen.de.

ist der bürokratische Aufwand – so die Autoren der Studie – allerdings weniger auf diese zusätzlichen Informationen zurückzuführen, sondern vor allem auf die regulatorischen Anforderungen der EU. Dabei spielen die Verfügbarkeit, der Informationsgehalt und die Benutzerfreundlichkeit der offiziellen Vorlagen und Online-Formulare eine wichtige Rolle.

II. Unterschiedliche Interpretation der DSGVO in Deutschland im Bund und in den Ländern

Die Aufsichtsbehörden von Bund und Ländern haben sich zu einer Datenschutzkonferenz zusammengeschlossen, die die Arbeit der Behörden koordinieren soll, um eine einheitliche Anwendung des EU-Rechts zu erreichen. Die Konferenz hat verschiedene Informationsschriften und Mustervorlagen herausgegeben. Gleichwohl geben die Datenschutzbehörden des Bundes und der 16 Länder zusätzliche Informationen und Formulare mit unterschiedlich inhaltlichem Verständlichkeitsgrad und digitaler Nutzungsqualität heraus. So haben einzelne Landesdatenschutzbeauftragte, wie der Landesdatenschutzbeauftragte von Baden-Württemberg, eigene Arbeitsleitfäden veröffentlicht.[3] Im Gegensatz zur DSGVO verknüpft er dabei den Begriff der „Verarbeitungstätigkeit" mit der Größe des Unternehmens. Je größer das Unternehmen sei, desto differenzierter sei der Geschäftsprozess, der als Verarbeitungstätigkeit darzustellen ist. Ferner verlangt er zusätzlich im Gegensatz zur DSGVO, dass neben dem für die Verarbeitung Verantwortlichen auch die Leitungspersonen des Unternehmens zu nennen sind.

Solche Unterschiede führen bei Unternehmen, die in mehreren Bundesländern Niederlassungen haben und deshalb die jeweiligen länderspezifischen Vorgaben erfüllen müssen, zu unnötigen Belastungen.

III. Unterschiedliche Qualität der Informationen über die regulatorischen Anforderungen

In den vier untersuchten Ländern werden die Normadressaten unterschiedlich gut darüber informiert, was sie zu befolgen haben. Österreich und Italien bieten die wenigsten Anleitungen. Die Datenschutzbehörden Deutschlands geben die detailliertesten Hinweise. Die mit Abstand kundenfreundlichsten Informationen und Online-Formulare bietet Frankreich. Sie enthalten u. a. klar strukturierte Excel-Tabellen und Dropdown-Menüs.[4]

Unzureichende oder schwer verständliche Informationen über die regulatorischen Anforderungen führen zu einem **erheblichen Einarbeitungsaufwand.** Allgemein wird bemängelt, dass die Unternehmen unzureichend informiert und unterstützt werden. Es würden Leitlinien sowie Best-Practice-Beispiele fehlen.

IV. Der Begriff der „Verarbeitungstätigkeit" ist unklar

Der Begriff der Verarbeitungstätigkeit wird in der DSGVO nicht definiert. In Österreich und Italien werden dazu keine Hinweise gegeben. Die deutschen und französischen Datenschutzbehörden geben an, dass nicht jeder einzelne Verarbeitungsvorgang in das Verzeichnis aufgenommen werden muss, sondern eine Kategorisierung vorgenommen werden kann. Was unter „Kategorie" verstanden wird, ist allerdings nicht selbsterklärend.

Im Kern geht es darum, ob personenbezogene Daten gesammelt (Erhebung), in einer sicheren Umgebung aufbewahrt (Speicherung), für bestimmte Zwecke genutzt (Verwendung) und verbreitet (Verbreitung) bzw. dauerhaft gelöscht werden, wenn sie nicht mehr benötigt werden (Vernichtung). Dies ist z. B. der Fall, wenn eine Personalakte angelegt und geführt wird oder Kundendaten gespeichert werden. Die deutschen Datenschutzbehörden gehen davon aus, dass eine neue Verarbeitungstätigkeit vorliegt, wenn die Verarbeitung personenbezogener Daten zu einem neuen Zweck erfolgt.

V. Last und Segen detaillierter Vorgaben und Hinweise

Wie häufig sind auch hier die Hinweise der Datenschutzbehörden in Deutschland am umfangreichsten und detailliertesten. Dies erhöht den Aufwand, da sie zur Kenntnis genommen und berücksichtigt werden müssen und zu entsprechend langen Einarbeitungszeiten führen. Andererseits erleichtern sie die Anwendung der DSGVO, da sie insbesondere bei unbestimmten Rechtsbegriffen (wie Risiko, Gefahr) Unsicherheiten vermeiden und Rückfragen vorbeugen. Die interviewten Unternehmen haben dies überwiegend eher als Erleichterung eingeschätzt.

VI. Das Verarbeitungsverzeichnis dient dem Datenschutz, aber keinem betrieblichen Zweck

Einer der Gründe für die teilweise geringe Akzeptanz des Verarbeitungsverzeichnisses ist, dass es zu keinem betrieblichen Zweck genutzt werden kann, sondern nur der Erfüllung des Art. 30 DSGVO dient. Die detaillierten Empfehlungen der deutschen Datenschutzbehörden zeigen, dass sie das Verzeichnis der Verarbeitungstätigkeiten als zentralen Bestandteil der Dokumentation des für die Verarbeitung Verantwortlichen sehen. Sie betrachten es als den Kern eines jeden Datenschutzkonzepts. Insoweit gehen sie über die Anforderungen des Art. 30 DSGVO hinaus.

VII. Die Befreiung mittelständischer Unternehmen von der Verpflichtung, ein Verzeichnis zu führen, geht ins Leere

Die EU wollte kleine und mittlere Unternehmen die Verzeichnispflicht nicht auferlegen, um ihnen hohe Bürokratielasten zu ersparen. Deshalb wird in Art. 30 Abs. 5 DSGVO geregelt, dass Unternehmen, die weniger als 250 Mitarbeiter beschäftigen, von der Verpflichtung, ein Verzeichnis zu führen, ausgenommen sind. Diese Ausnahme gilt aber dann nicht, wenn die von ihnen vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt oder wenn die Verarbeitung nicht nur gelegentlich erfolgt. Da Beschäftigtendaten als personenbezogene Daten anzusehen sind und von einem Unternehmen ab einem Mitarbeiter regelmäßig in der Personalverwaltung verarbeitet werden, fällt bereits schon jedes Unternehmen ab einem Mitarbeiter unter die Verzeichnispflicht. Gleiches gilt für Kleinst-

[3] LfDI, Mustervorlage für ein Verarbeitungsverzeichnis nach Art. 30 GDPR mit Löschkonzept nach Art. 17 (1) GDPR (Excel-Tabelle) mit Mustereinträgen für Bewerberdaten. Die Vorlage ist verfügbar unter: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.baden-wuerttemberg.datenschutz.de%2Fwp-content%2Fuploads%2F2021%2F11%2F211129_Arbeitshilfe_VV_und_Loeschkonzept_Tabelle-mit-Bsp-Bewerberdaten.xlsx&wdOrigin=BROWSELINK (Stand: 24.9.2023).

[4] Das Dropdown-Menü ist eine spezielle Form eines Auswahlmenüs. Nach dem Klick auf einen entsprechenden Button oder durch die Berührung mit dem Mauszeiger erscheint eine Auswahlliste auf dem Bildschirm. Durch einen weiteren Klick auf den gewünschten Menüpunkt wird dieser aufgerufen (Definition bei e-teaching.org).

unternehmen, die Kundendaten verarbeiten. Die eigentliche Absicht einer Mittelstandsklausel wird durch die von der EU vorgesehenen Einschränkung konterkariert.

C. Die Verpflichtung, Verstöße gegen den Schutz personenbezogener Daten zu melden (Art. 33 DSGVO)

Der für die Verarbeitung personenbezogener Daten Verantwortliche eines Unternehmens hat innerhalb von 72 Stunden der Aufsichtsbehörde einen Verstoß zu melden, es sei denn, die Verletzung des Schutzes personenbezogener Daten führt zu keinem Risiko für die Rechte und Freiheiten von natürlichen Personen. Der für den Datenschutz Verantwortliche muss also eine Risikoabwägung durchführen. Der Begriff des „Risikos" wird in der DSGVO nicht definiert.

Die Meldung muss u. a. beschreiben, um welche Art der Verletzung des Schutzes personenbezogener Daten es sich handelt und welche Folgen voraussichtlich ausgelöst werden. Sie muss auf die Maßnahmen eingehen, die ergriffen worden sind und den Namen und die Kontaktdaten des Datenschutzbeauftragten angeben. Deutschland verzichtet darauf, dass der Name und die Kontaktdaten des Datenschutzbeauftragten angegeben werden müssen.

Typische meldepflichtige Fälle entstehen bei sichtbaren E-Mail-Adressen in Sammelmails und bei Cyberangriffen.

I. Weitergehende Angaben, die gemeldet werden müssen

In Frankreich, Deutschland und Italien müssen zusätzlich die Sicherheitsmaßnahmen gemeldet werden, die **vor der Datenverletzung** ergriffen wurden. Außerdem wird nach dem geschätzten Schweregrad der Datenverletzung gefragt.

II. Der Begriff des Risikos für die Rechte und Freiheiten von natürlichen Personen ist unklar

Der Umstand, dass die EU nicht erläutert, wann davon ausgegangen werden kann, dass der Verstoß gegen den Datenschutz zu keinem Risiko für die Rechte und Freiheiten von natürlichen Personen führt, löst – so die befragten Unternehmen – einen erheblichen Aufwand aus. Es folgen Rückfragen bzw. erhöhte Kosten bei externen Beratungsunternehmen.

Beispiel: Muss der Diebstahl eines Tablets gemeldet werden, das ausgeschaltet und durch starke Passwörter geschützt war und die Daten auf dem Tablet kurzfristig aus der Ferne gelöscht werden konnten?

III. Über die Anwendung der 72-Stunden-Schwelle herrscht Unklarheit

Nach Art. 33 Abs. 1 DSGVO muss die Datenpanne „möglichst binnen 72 Stunden gemeldet werden". Aufgrund des Risikos von Bußgeldzahlungen verstehen die Unternehmen darunter eine feste Frist und machen von der in Art. 30 Abs. 4 DSGVO erwähnten schrittweisen Zurverfügungstellung der Information keinen Gebrauch. Hier fehlen klare Hinweise der Aufsichtsbehörden.

IV. Das Meldeverfahren ist in den vier Ländern und innerhalb Deutschlands unterschiedlich

In Italien und einigen Bundesländern in Deutschland gibt es Online-Portale. Ansonsten erfolgt die Meldung per E-Mail oder über Formulare, die an die Behörden geschickt werden müssen. In Österreich ist das vorgegebene Formular obligatorisch. **In Frankreich** bildet das Online-Formular eine besondere Belastung, weil es nicht benutzerorientiert gestaltet und damit zeitraubend auszufüllen ist.

V. Der Aufwand für die internen Prozesse ist deutlich höher als die Meldung selbst

Aufwendig ist für die Unternehmen, die erforderlichen Informationen zu sammeln und zu bewerten, ob der Vorfall gemeldet werden muss oder nicht. Die Meldung selbst ist dann in der Regel – Frankreich ausgenommen – mit relativ wenig Aufwand verbunden.

D. Schlussfolgerung aus dem EU-Vergleich

Der Vergleich ergab, dass die länderspezifischen Unterschiede eine eher geringe Rolle spielen. Die Befolgungskosten der beiden EU-Vorgaben ist für jedes Unternehmen, das personenbezogene Daten verarbeitet, sehr hoch. Die nennenswerte Bürokratiebelastung ergibt sich also unmittelbar aus dem EU-Recht, wobei der Grad der Belastung vor allem von der Größe des Unternehmens und der Zahl der Verarbeitungsvorgänge abhängt. Größere Unternehmen haben einen größeren bürokratischen Aufwand, weil sie mehr Unternehmensprozesse haben als kleinere Unternehmen. Dafür verfügen größere Unternehmen über mehr finanzielle und personelle Ressourcen, um die DSGVO umzusetzen. Die Digitalisierung führt zu einer Zunahme der Datenprozesse und damit der Datenschutzanforderungen.[5]

Aufgrund von Rechtsunklarheiten und der Komplexität der Anforderungen haben Unternehmen hohe Schulungskosten und bedienen sich externer Beratung. Dies allein erhöht die Fixkosten.

Die Autoren der Studie haben in den Interviews eine Reihe von Anregungen erhalten, die die Bürokratiebelastung senken und zur besseren Akzeptanz der rechtlichen Vorgaben führen würden:

- Für die Meldung von Datenpannen sollte eine deutschlandweit standardisierte **Online-Plattform** eingerichtet werden. Sie sollte benutzerfreundlich sein, es ermöglichen, dass Unternehmensdaten gespeichert werden können und typische Fälle beschreibt.
- Hilfreich wären EU-weit **einheitliche Vorlagen für das Verfahrensverzeichnis**, die in die jeweilige Landessprache übersetzt werden.
- **Bessere Information und Kundenorientierung:** Verständliche Formulare, selbsterklärende Hinweise, Best-Practice-Beispiele, Ankreuzkästchen oder Dropdown-Menüs[6] und auf offene Textfelder verzichten.
- **Besserer Service:** Die Erreichbarkeit der Datenschutzaufsicht verbessern, die Auskunftsbereitschaft und -fähigkeit und die Kommunikationsqualität steigern. So sollte zu-

[5] *Engels/Scheufen* (2020), Wettbewerbseffekte der Europäischen Datenschutzgrundverordnung: Eine Analyse basierend auf einer Befragung unter deutschen Unternehmen, IW-Report, Nr. 1/2020, Institut der deutschen Wirtschaft (IW), Köln, 5.

[6] Vgl. Fn. 4.

rückgemeldet werden, ob der Vorgang aufgrund der Meldung der Datenpanne erledigt ist.

- **Wirksame Öffnungsklausel** für kleine und mittlere Unternehmen. Ein Landesdatenschutzbeauftragter schlägt vor, dass Unternehmen mit weniger als 250 Beschäftigten grundsätzlich nur dann verpflichtet werden sollten, ein Verzeichnis der Verarbeitungstätigkeit personenbezogener Daten erstellen zu müssen, wenn ihre Haupttätigkeit in der Datenverarbeitung besteht.
- **Konkretisierung unbestimmter Rechtsbegriffe** wie „Verarbeitung von personenbezogenen Daten“ (Art. 30 DSGVO) und „Risiko für Rechte und Freiheiten natürlicher Personen“ (Art. 33 DSGVO).