Stiftung
Familienunternehmen

Regulatorische und finanzielle Belastungen durch EU-Gesetzgebung in vier Mitgliedstaaten – eine vergleichende Untersuchung

Bd. 4: Belastungen aufgrund von Art. 30 und 33 der Datenschutz-Grundverordnung

Zusammenfassung der wichtigsten Ergebnisse

Die wesentlichen Erkenntnisse der rechtlichen Untersuchung (cep und Alerion)

Zur gesamten Studie in englischer Sprache geht es hier:

1. In Teil A dieser Studie werden die regulatorischen Belastungen im Zusammenhang mit der Befolgung von zwei Artikeln aus der europäischen Datenschutz-Grundverordnung (DSGVO) in Österreich, Frankreich, Deutschland und Italien verglichen. Die Studie konzentriert sich auf die rechtlichen und administrativen Anforderungen in Bezug auf
   - das Erstellen und Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO sowie
   - die Anforderungen im Zusammenhang mit der Meldung von Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde gemäß Art. 33 DSGVO.
2. Art. 30 DSGVO verlangt von Verantwortlichen und Auftragsverarbeitern personenbezogener Daten das Führen eines Verzeichnisses von Verarbeitungstätigkeiten (VVT) mit einer Reihe von Angaben der vom Unternehmen verarbeiteten Daten, darunter
   - den Namen und die Kontaktdaten des Verantwortlichen,
   - die Zwecke der Verarbeitung,
   - eine Beschreibung der Kategorien verarbeiteter Daten sowie der Kategorien betroffener Personen,
   - die Kategorien von Empfängern, gegenüber denen diese Daten offengelegt werden,
   - eine Angabe, ob die Daten in ein Drittland übermittelt werden, sowie
   - wenn möglich, die Fristen für die Löschung der Daten sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, die das Unternehmen bezüglich der Daten ergriffen hat.

Keine Definition von „Verarbeitungstätigkeit" in Art. 30 DSGVO

3. Da die oben genannten Angaben für jede „Verarbeitungstätigkeit" bereitzustellen sind, hängt der Umfang des VVT vom Verständnis des Begriffs „Verarbeitungstätigkeit" ab. Dieser Begriff ist in der DSGVO allerdings nicht definiert. Während die österreichischen und die italienischen Datenschutzbehörden hier keine relevante Unterstützung bieten, geht aus den Anleitungen der französischen und deutschen[1] Datenschutzbehörden hervor, dass nicht jeder einzelne Verarbeitungsvorgang im VVT aufgeführt sein muss, sondern in gewissem Umfang abstrahiert werden darf. Das Abstraktionsniveau ist allerdings nicht vollständig klar.

1 Die Datenschutzaufsicht in Deutschland ist föderal gegliedert. Sie besteht aus den Datenschutzbehörden des Bundes sowie der 16 Länder. Sofern die Datenschutzbehörden der Länder als zuständige Behörde in Erscheinung treten, basiert die vorliegende Studie auf den Vorlagen und Anleitungen des Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) Baden-Württemberg.

4. Der Umfang der Anleitungen sowie der Unterstützung im Zusammenhang mit der Erstellung eines VVT auf den Websites der nationalen Datenschutzbehörden unterscheidet sich beim Vergleich der untersuchten vier Mitgliedstaaten erheblich. Während die österreichische Datenschutzbehörde keine Vorlage und nur sehr wenige Informationen zu den Pflichten in Bezug auf die Erstellung eines VVT bereitstellt, sind Anleitung und Unterstützung der anderen Behörden wesentlich umfassender.

5. Während die DSGVO die im VVT verlangten Angaben aufführt, ohne sie zu spezifizieren, weichen die von den nationalen Datenschutzbehörden bereitgestellten offiziellen Vorlagen in gewissem Umfang davon ab. So ist in den Vorlagen Deutschlands und Frankreichs – im Gegensatz zu Österreich (wo überhaupt keine offizielle Vorlage angeboten wird) und Italien – eindeutig aufgeführt, welche genauen Kontaktdaten angegeben werden müssen. Auch wenn eine umfassendere Vorlage eine größere Belastung zu sein scheint, ist es doch für den Verantwortlichen klarer, welcher Informationsumfang genau verlangt wird.

6. Einige untersuchte Mitgliedstaaten verlangen, dass im VVT zusätzliche Angaben gemacht werden, die als aufwertende Zusatzangaben gelten können, wobei diese Aufwertung marginal ist.

7. Die bürokratische Belastung in Bezug auf die Erstellung eines VVT hängt auch von der Verfügbarkeit und Benutzerfreundlichkeit der von den zuständigen Datenschutzbehörden bereitgestellten offiziellen Vorlagen ab.

8. Die Befreiung kleinerer Unternehmen mit weniger als 250 Beschäftigten von der Pflicht zum Führen eines VVT in Art. 30 (5) DSGVO läuft größtenteils ins Leere. Da die Einschränkungen weit gefasst sind, greift die Befreiung nur selten.

Befreiung für kleinere Unternehmen greift selten

9. Anhand der vorangegangenen Ausführungen sprechen wir folgende Empfehlungen aus: Die bürokratische Belastung ließe sich verringern durch Bereitstellung besserer offizieller Vorlagen für ein VVT, die folgende Kriterien erfüllen:

Potenzial für Vereinfachung und Verbesserung

   - Sie sind harmonisiert und in die jeweiligen Landessprachen übersetzt.
   - Sie verbinden die Vorteile der bestehenden Vorlagen der nationalen Datenschutzbehörden, z. B. dadurch,
     - dass sie klar strukturiert sind,
     - dass sie selbsterklärend sind oder direkte Links zu Quellen enthalten, in denen weitere Informationen angeboten werden, und
     - dass sie wenigstens für die wichtigsten Angaben Kästchen zum Ankreuzen oder – vorzugsweise – Drop-down-Menüs enthalten (wie die Vorlage der französischen Datenschutzbehörde).
   - Sie bieten mehr Unterstützung für kleine und mittlere Unternehmen dazu, wie ein vereinfachtes VVT erstellt werden sollte.

10. Art. 33 DSGVO verpflichtet die Verantwortlichen zur Erfassung von Verletzungen des Schutzes personenbezogener Daten sowie zur Meldung konkreter Verletzungen an die zuständige Datenschutzbehörde. Die Meldung hat „unverzüglich" und „möglichst" innerhalb von 72 Stunden zu erfolgen, nachdem die Verletzung dem Verantwortlichen „bekannt wurde".

11. In der DSGVO ist eine „Verletzung des Schutzes personenbezogener Daten" definiert als Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

12. Gemäß Art. 33 DSGVO enthält die Meldung zumindest folgende Informationen:

    - eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten;
    - den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
    - eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten; sowie
    - eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten.

Gold Plating in Frankreich, Deutschland und Italien

13. Darüber hinaus fragen Frankreich, Deutschland[2] und Italien einige Informationen ab, die von der DSGVO nicht verlangt werden. So fragen Frankreich und Italien beispielsweise unter anderem nach Maßnahmen, die vor der Datenschutzverletzung ergriffen wurden, sowie nach dem geschätzten Schweregrad. Wir betrachten diese Anforderungen als Gold Plating.

14. Interessanterweise wird nicht in allen Meldeformularen nach sämtlichen Informationen gefragt, die in Art. 33 DSGVO verlangt werden. So werden im deutschen Online-Meldeformular nicht der Name und die Kontaktangaben des Datenschutzbeauftragten verlangt.

15. Insgesamt unterscheiden sich die in der Meldung zu übermittelnden Angaben in Bezug auf ihren Genauigkeitsgrad erheblich. Im österreichischen Formular werden die wenigsten Informationen abgefragt, gefolgt vom deutschen, französischen und italienischen Formular. Allerdings ist auch zu berücksichtigen, dass im italienischen Formular hauptsächlich Kästchen zum Ankreuzen verwendet werden – im Gegensatz zu den im österreichischen und im deutschen Formular vorrangig verwendeten offenen Textfeldern. Während Italien mehr Informationen abfragt als die anderen drei Mitgliedstaaten, gibt es auch Hinweise zu einigen Aspekten, die in den anderen Mitgliedstaaten nicht weiter ausgeführt werden, wie beispielsweise in Bezug auf die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten.

2 Für Deutschland wurde das Meldeformular des LfDI Baden-Württemberg analysiert.

16. Anhand der vorangegangenen Ausführungen sprechen wir folgende Empfehlungen aus:
    - Die Mitgliedstaaten sollten auf die Abfrage von Informationen verzichten, die von der DSGVO nicht verlangt werden, und
    - die Meldeformulare sollten benutzerfreundlicher gestaltet werden, z. B. durch den Einsatz von Kästchen zum Ankreuzen statt offener Textfelder.

Empfohlen wird der Verzicht auf Gold Plating sowie benutzerfreundliche Meldeformulare

Die wesentlichen Erkenntnisse der Bewertung der regulatorischen Belastungen (Prognos AG und CSIL)

Vorgehensweise

1. In Teil B dieser Studie werden die regulatorischen Belastungen im Zusammenhang mit der Umsetzung der Art. 30 und 33 der **Datenschutz-Grundverordnung (DSGVO)** in vier EU-Mitgliedstaaten anhand des Konzepts der Erfüllungskosten verglichen. Die empirische Bewertung erfolgte anhand von insgesamt 67 ausführlichen Interviews, die mit Unternehmen und Experten in allen vier Mitgliedstaaten geführt wurden.

Gegenwärtige Handhabung

2. Art. 30 DSGVO verlangt von Unternehmen die Erfassung sämtlicher Verarbeitungstätigkeiten im Zusammenhang mit personenbezogenen Daten in einem Verzeichnis von Verarbeitungstätigkeiten (VVT). Bei einer Datenschutzverletzung sind Unternehmen gemäß Art. 33 verpflichtet, die Aufsichtsbehörde innerhalb von 72 Stunden zu informieren. Bis auf eine Ausnahme hatten alle untersuchten Unternehmen die Anforderungen aus den Art. 30 und 33 umgesetzt.
3. In der Praxis können Firmen die Ausnahmeregelung für kleine und mittlere Unternehmen laut Art. 30 (5) nicht in Anspruch nehmen, da praktisch alle Unternehmen besondere Kategorien personenbezogener Daten im Sinne von Art. 9 (1) verarbeiten (z. B. Gehaltsabrechnung) und damit zum Erstellen und Führen eines VVT verpflichtet sind.
4. **Die Meldung laut Art. 33 kann digital erfolgen.** In Frankreich und Italien muss die Meldung an die Behörde anhand eines elektronischen Formulars übermittelt werden, in Österreich per Post oder E-Mail und in Deutschland – je nach den Bestimmungen der Datenschutzbehörden der einzelnen Bundesländer – häufig als elektronisches Formular und alternativ per E-Mail oder telefonisch.
5. **Die Umsetzung und Einhaltung der Art. 30 und 33 ist für Unternehmen mit erheblichen Aufwänden verbunden.** Bei den auferlegten Belastungen wurden in der vergleichenden Studie keine länderspezifischen Unterschiede festgestellt. Die Belastungen entsprechen vielmehr der Größe des Unternehmens sowie der Zahl der Verarbeitungstätigkeiten.

Unsicherheiten aufgrund unzureichend definierter Rechtsbegriffe prägen Unternehmenspraxis

6. **Aufgrund unzureichend definierter Rechtsbegriffe sind Unternehmen bei der Einhaltung von Art. 30 DSGVO in hohem Maße auf offizielle Informationen und Vorlagen angewiesen.** Da der Begriff der „Verarbeitungstätigkeit" in der DSGVO nicht definiert wird, sondern nur eine sehr breit gefasste Definition des Begriffs „Verarbeitung" enthalten ist, die jeden ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten meint, haben Unternehmen in allen Mitgliedstaaten Vorlagen verwendet, die entweder von den Behörden, von Beratern oder – in seltenen Fällen – von Unternehmen selbst bereitgestellt wurden.

7. **Insbesondere Groß- und Kleinstunternehmen sind von den Bestimmungen in Art. 30 DSGVO betroffen.** Kleinstunternehmen besitzen oft nicht genügend Ressourcen und/oder Kompetenzen und sind deshalb besonders abhängig von externen Dienstleistern, was zu zusätzlichen Kosten führt. Andererseits haben Großunternehmen häufig komplexere Geschäftsmodelle, die mit personenbezogenen Daten arbeiten.

8. Die Studie zeigt den umfassenden Rückgriff auf externe Beratung als Ergänzung zu den internen Maßnahmen. Externes Expertenwissen war erforderlich, um eine pünktliche und angemessene Einhaltung der Vorgaben zu gewährleisten und gleichzeitig Sanktionen sowie eine Schädigung des Markenimages der Unternehmen zu vermeiden.

9. **Unternehmen mit B2C-Geschäftsmodellen sehen sich aufgrund von Art. 30 DSGVO** erheblichen Belastungen ausgesetzt, da hier besonders viele Verarbeitungstätigkeiten auftreten.

Beim Führen und Aktualisieren des VVT gibt es keine länderspezifischen Unterschiede; diese Arbeiten verursachen aber erhebliche Kosten.

10. **Das Führen und Aktualisieren des VVT führt zu erheblichen jährlichen Ausgaben, die als deutliche Belastung wahrgenommen werden.** Unternehmen wenden jährlich durchschnittlich eine Stunde je Verarbeitungstätigkeit für die Pflege der enthaltenen Informationen auf. Im Ländervergleich wurden keine Unterschiede festgestellt. So sind die Compliance-Kosten abhängig von der Größe des Unternehmens und des VVT und liegen zwischen 30 und 40 Stunden für Kleinst- und Kleinunternehmen sowie zwischen 92 und 297 Stunden für mittlere und große Unternehmen. Die Mehrzahl hat darauf hingewiesen, dass das VVT ausschließlich für Compliance-Zwecke genutzt wird. Dementsprechend werden die Aufwände zur Pflege und Aktualisierung als besondere Belastung wahrgenommen.

11. **Bei der Meldung von Datenschutzverletzungen entfällt für die Unternehmen der meiste Zeit- und Arbeitsaufwand auf interne Prozesse und die Risikobewertung.** Der Datenschutzbeauftragte ist über den Datenschutz-Zwischenfall in Kenntnis zu setzen, hat eine Risikobewertung vorzunehmen und zu entscheiden, ob der Zwischenfall an die Behörde gemeldet werden muss. Weil Risiken nicht genau bestimmbar sind, ist damit häufig ein hoher Bewertungsaufwand verbunden, der als Belastung wahrgenommen wird.

12. **Die Umsetzung des Meldeprozesses ist mit Ausnahme von Frankreich keine besondere Belastung.** Das Online-Formular in Frankreich stellt eine Belastung dar, weil Benutzerorientierung und damit ein gutes Benutzererlebnis fehlen (z. B. durch eine intuitive

Benutzeroberfläche, klare Anweisungen sowie die Möglichkeit, wiederkehrende Angaben zu speichern). So ist es beispielsweise nicht möglich, Einträge zur späteren Verwendung zu speichern oder wegen Korrekturen zu vorangegangenen Seiten zurückzukehren. In Italien und einigen deutschen Bundesländern gibt es ebenfalls Online-Portale, die aber nicht als Belastung angeführt wurden. Ansonsten erfolgt die Meldung per E-Mail oder über vorgegebene Formulare, die an die Behörden zu schicken sind. In Österreich besteht die Pflicht zur Verwendung des vorgegebenen Formulars.

Vorschläge zur Verringerung des Verwaltungsaufwands

13. **Präzisere Definitionen unbestimmter Rechtsbegriffe.** Unbestimmte Rechtsbegriffe sorgen für Unsicherheit, zusätzlichen Aufwand und Beratungskosten. Die DSGVO sollte durch Kommentare ergänzt bzw. geändert werden, damit die verwendeten Begriffe klar definiert sind. Damit wäre es auch möglich, die Vorlagen für Verzeichnisse von Verarbeitungstätigkeiten (VVT) für alle Mitgliedstaaten zu vereinheitlichen und zu standardisieren.
14. **Durchsetzung der Öffnungsklausel für kleine und mittlere Unternehmen.** Die praktische Umsetzung der Ausnahmeregelung für kleine und mittlere Unternehmen würde die Belastung der Unternehmen erheblich reduzieren. Das erfordert eine klare Festlegung, welche Daten, die dem besonderen Schutz laut Art. 9 (1) DSGVO unterliegen, ohne die Vorgabe der Erstellung eines VVT verarbeitet werden dürfen.
15. **Bessere Unterstützung seitens der Behörden.** Beratungsleistungen sowie bewährte Praxisbeispiele, Vorlagen und Informationen, die besonders praxisorientiert sind und den betroffenen Unternehmen damit unmittelbar einen Mehrwert bieten.
16. **Einheitliches Meldeverfahren bei den Datenschutzbehörden unter Berücksichtigung von Nutzerorientierung, reibungslosem Nutzererlebnis und Automatisierung.** Die administrative Umsetzung von Art. 33 sollte als Online-Lösung standardisiert werden, um die Zeit je Meldung zu reduzieren. Eine Meldung über eine automatisierte und benutzerfreundliche Online-Plattform spart Zeit, vor allem dann, wenn Unternehmensdaten gespeichert und/oder typische Fälle abgerufen werden können.

KMUs brauchen Rechtssicherheit bei der Inanspruchnahme der Öffnungsklausel

Impressum

Herausgeber:

Stiftung Familienunternehmen

Stiftung Familienunternehmen
Prinzregentenstraße 50
80538 München
Telefon: +49 (0) 89 / 12 76 400 02
Telefax: +49 (0) 89 / 12 76 400 09
E-Mail: info@familienunternehmen.de
www.familienunternehmen.de

Teil A erstellt von:

cep
Kaiser-Joseph-Straße 266
79098 Freiburg im Breisgau

Dr. Lukas Harta, LL.M.
Dr. Anja Hoffmann
Dr. Matthias Kullas
Prof. Dr. Andrea de Petris

Alerion
137 rue de l'Université
75007 Paris
Frankreich

Carole Bui
Caroline Leroy-Blanvillain
Corinne Thierache

Teil B erstellt von:

Prognos AG
Goethestraße 85
10623 Berlin

Jan Tiessen
Michael Schaaf
Jan-Felix Czichon

CSIL
Corso Monforte 15
20122 Mailand
Italien

Jessica Catalano
Sara Banfi
Anthony Bovagnet

Titelbild: SrdjanPav | iStock