



**12110/04/DE
WP 102**

Muster-Checkliste

Antrag auf Genehmigung verbindlicher Unternehmensregelungen

angenommen am 25. November 2004

Die Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges europäisches Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von: Europäische Kommission, GD Binnenmarkt, Direktion E (Dienstleistungen, geistiges und gewerbliches Eigentum, Medien und Datenschutz), B-1049 Brüssel, Belgien, Büro C100-6/136.

Website: www.europa.eu.int/comm/privacy

DIE GRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995¹,

gestützt auf Artikel 29 sowie auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie, ferner auf Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,

gestützt auf ihre Geschäftsordnung, insbesondere Artikel 12 und 14 -

hat folgende Stellungnahme angenommen:

1. Wozu dient diese Checkliste?

2. Diese Checkliste soll einer Unternehmensgruppe beim Antrag auf Genehmigung der verbindlichen Unternehmensregelungen als Anhaltspunkt dienen und vor allem beim Nachweis helfen, dass diese Unternehmen die Voraussetzungen des Arbeitspapiers WP74² erfüllen.

3. Bei welcher Datenschutzbehörde wird der Antrag gestellt?

3.1. Ist die Muttergesellschaft oder die Hauptniederlassung Ihrer Gruppe in einem EU-Mitgliedstaat ansässig, wenden Sie sich an die Datenschutzbehörde des entsprechenden Mitgliedstaates.

3.2. Ist nicht klar, wo sich die Muttergesellschaft oder die Hauptniederlassung Ihrer Gruppe befindet, oder befindet sie sich außerhalb der EU, wenden Sie sich an die Datenschutzbehörde, die nach den unten stehenden Kriterien am ehesten zuständig ist.

3.3. Bei Antragstellung müssen Sie genau darlegen, warum Sie die von Ihnen gewählte Datenschutzbehörde für zuständig halten. Folgende Faktoren werden zur Bestimmung der am ehesten zuständigen Datenschutzbehörde herangezogen:

3.3.1. der Standort der europäischen Hauptniederlassung oder des Unternehmens der Gruppe, das für Datenschutzangelegenheiten verantwortlich ist³;

3.3.2. der Standort des Unternehmens, das (hinsichtlich der Verwaltungsaufgaben, des Verwaltungsaufwands usw.) am besten für die Antragstellung und die Durchsetzung der verbindlichen Unternehmensregelungen innerhalb der Gruppe geeignet ist;

¹ Amtsblatt L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/privacy/law_de.htm

² WP74 ist ein Papier der „Artikel-29-Datenschutzgruppe“, einem Forum, das im Rahmen der Datenschutz-Richtlinie 95/46 eingerichtet wurde. WP74 legt die Voraussetzungen für verbindliche Unternehmensregelungen fest.

³ Befindet sich die Hauptniederlassung der Unternehmensgruppe nicht in der EU/im EWR, muss die Unternehmensgruppe, wie in Arbeitspapier 74 vorgesehen, ein europäisches Unternehmen der Gruppe mit dem Datenschutz betrauen. Dieses Unternehmen ist dafür verantwortlich, dass alle ausländischen Unternehmen der Gruppe ihre Datenverarbeitung an die Regelungen der Unternehmensgruppe anpassen, gegebenenfalls mit der federführenden Behörde zusammenarbeiten und Schadenersatz leisten, sollte ein Mitglied der Unternehmensgruppe gegen die verbindlichen Unternehmensregelungen verstoßen.

3.3.3. der Ort, an dem die meisten Entscheidungen über den Zweck und die Mittel der Datenverarbeitung getroffen werden; und

3.3.4. die Mitgliedstaaten der EU, aus denen die meisten Daten in Länder außerhalb des EWR übermittelt werden.

3.4. Dies sind keine formalen Kriterien. Die Datenschutzbehörde, bei der Sie Ihren Antrag stellen, wird im Rahmen ihrer Verfügungsfreiheit entscheiden, ob sie tatsächlich die am ehesten zuständige Datenschutzbehörde ist. Die Datenschutzbehörden können untereinander beschließen, den Antrag an eine andere als die von Ihnen gewählte Datenschutzbehörde zu verweisen.

4. Welche Angaben sind bei der Antragstellung notwendig?

4.1. Folgende Unterlagen sind vorzulegen:

4.1.1. Eine Aufstellung, die folgende Angaben enthält:

4.1.1.1. die Kontaktdaten der Person, die innerhalb der Unternehmensgruppe für einschlägige Fragen zuständig ist;

4.1.1.2. alle Angaben, die die Wahl der Datenschutzbehörde rechtfertigen, einschließlich der Angaben über die Grundstruktur Ihrer Unternehmensgruppe und die Art und Struktur der Datenverarbeitung in der EU/im EWR, insbesondere der Standort von Entscheidungsträgern und Tochtergesellschaften in der EU, die Mittel und Zwecke der Verarbeitung, die Orte, von denen aus Daten in Drittländer übermittelt werden und die Drittländer, in die diese Daten übermittelt werden (letztere Angaben sind erforderlich, damit sie von der „Eingangs-Datenschutzbehörde“ an die betreffenden Datenschutzbehörden weitergeleitet werden können);

4.1.2. Eine Zusammenfassung, auf welche Art und Weise die Forderungen in WP74 (siehe unten) erfüllt wurden (dies hilft den Datenschutzbehörden, in Ihren Unterlagen die entscheidenden Stellen zu finden).

4.1.3. Alle einschlägigen Unterlagen, in denen die „verbindlichen Unternehmensregelungen“, die von Ihrem Unternehmen aufgestellt werden sollen, enthalten sind (z. B. Grundsatzpapiere, Kodizes, Mitteilungen, Verfahrensvorschriften und Verträge, die für den Antrag relevant sein könnten). Ebenso eine allgemeine Grundsatzklärung, damit sich die Datenschutzbehörden ein Bild über die Art und Weise der Verarbeitung personenbezogener Daten in Ihrer Unternehmensgruppe machen können.

5. Rechtsverbindlichkeit der Maßnahmen

5.1. Die Regelungen müssen verbindlich sein,

5.1.1. sowohl innerhalb des Unternehmens,

5.1.2. als auch nach außen zugunsten Dritter.

5.2. Diese Anforderung kann auf unterschiedliche Art erfüllt werden. Wie Sie es tun, hängt von der Struktur und Größe Ihres Unternehmens ab, sowie von den Maßnahmen, die gegebenenfalls zur Einhaltung anderer Vorschriften, an die Ihr Unternehmen gebunden ist, getroffen wurden. Des Weiteren ist die nationale Gesetzgebung in den Mitgliedstaaten von Bedeutung, in denen sich Standorte Ihrer Unternehmensgruppe befinden.

5.3. Verbindlichkeit innerhalb des Unternehmens

5.4. **Wie wird die Verbindlichkeit der Regelungen für die Unternehmen der Gruppe erreicht?**

5.5. Sie müssen die Einhaltung der verbindlichen Unternehmensregelungen durch alle Mitglieder der Unternehmensgruppe gewährleisten. Dies gilt besonders dann, wenn keine Hauptniederlassung existiert oder wenn sich diese außerhalb des EWR befindet. Wie die Einhaltung der Regelungen gewährleistet wird, hängt von der Struktur Ihrer Unternehmensgruppe ab und unterliegt außerdem der nationalen Gesetzgebung der Mitgliedstaaten, in denen sich Standorte Ihrer Unternehmensgruppe befinden.

5.6. Im Folgenden finden Sie Beispiele, wie die Verbindlichkeit von Unternehmensregelungen in einer Unternehmensgruppe erreicht werden kann, doch können je nach Situation auch andere Möglichkeiten geeignet sein:

5.6.1. verbindliche Unternehmensregelungen oder Verträge, die Sie gegenüber Mitgliedern der Gruppe durchsetzen können;

5.6.2. einseitige Erklärungen oder Zusagen der Muttergesellschaft, die für andere Mitglieder der Gruppe verbindlich sind;

5.6.3. Einbeziehung anderer Regelungen, z. B. von Verpflichtungen aus Statuten in einem festgelegten rechtlichen Rahmen; oder

5.6.4. Aufnahme der Regelungen in die allgemeinen Geschäftsgrundsätze einer Unternehmensgruppe und Durchsetzung mit Hilfe geeigneter Strategien, Prüfungen und Sanktionen.

5.7. Sämtliche oben angeführten Beispiele können in unterschiedlichen Mitgliedstaaten unterschiedliche Auswirkungen haben. Einfache einseitige Erklärungen werden beispielsweise in einigen Mitgliedstaaten nicht als verbindlich angesehen. Wenn Sie auf derartige Erklärungen zurückgreifen wollen, sollten Sie sich vor Ort beraten lassen.

Bitte erläutern Sie, wie die Verbindlichkeit der Regelungen innerhalb der Unternehmensgruppe erreicht wird.

5.8. **Wie wird die Verbindlichkeit für die Mitarbeiter erreicht?**

5.9. Die Regelungen müssen für Mitarbeiter verbindlich sein. Dies könnte erreicht werden, indem zum Beispiel Verpflichtungen im Arbeitsvertrag festgelegt werden oder Verstöße gegen die Regelungen Disziplinarverfahren zur Folge haben. Außerdem sollten angemessene Schulungen stattfinden, und die Führungskräfte

sollten sich für die Regelungen engagieren. Die Person, die innerhalb der Unternehmensgruppe letztlich für die Einhaltung der Regelungen verantwortlich ist, sollte im Antrag namentlich angeführt werden.

Bitte erläutern Sie, wie die Verbindlichkeit der Regelungen für die Mitarbeiter Ihrer Unternehmensgruppe erreicht wird und welche Sanktionen bei Verstößen vorgesehen sind.

5.10. Wie wird die Verbindlichkeit der Regelungen für Unterauftragnehmer erreicht, die Daten verarbeiten?

5.11. Sie müssen darlegen, wie Sie erreichen, dass Ihre verbindlichen Unternehmensregelungen auch für Unterauftragnehmer verbindlich sind. Bitte legen Sie Beispiele für Vertragsklauseln vor, an die sich Ihre Unterauftragnehmer halten müssen, und erläutern Sie, wie in diesen Verträgen die Folgen eines Verstoßes geregelt sind.

Bitte erläutern Sie, wie die Verbindlichkeit der Regelungen für Unterauftragnehmer erreicht wird und welche Sanktionen bei Verstößen vorgesehen sind.

5.12. Wie wird die Verbindlichkeit nach außen zugunsten Dritter erreicht?

5.13. Einzelpersonen, die von den verbindlichen Unternehmensregelungen betroffen sind, müssen die Einhaltung der Regelungen sowohl mit Hilfe der Datenschutzbehörden als auch der Gerichte durchsetzen können.

5.14. Einzelpersonen müssen den Rechtsweg einschlagen können,

5.14.1. entweder am Gerichtsstand des Mitglieds der Unternehmensgruppe, von dem aus die Daten übermittelt wurden,

5.14.2. oder am Gerichtsstand der EU-Hauptniederlassung oder des europäischen Unternehmens der Gruppe, das mit dem Datenschutz beauftragt ist.

5.15. In Ihrem Antrag muss dargelegt werden, welche Schritte die Betroffenen unternehmen können, um von Ihrem Unternehmen Schadenersatz zu erhalten, und wie Beschwerden bearbeitet werden.

5.16. Wenn sich Ihre Hauptniederlassung und die federführende Behörde zum Beispiel in Belgien befinden und ein Unternehmen Ihrer Gruppe in Italien Ihre verbindlichen Unternehmensregelungen verletzt, sollten die Betroffenen wissen, dass sie gegen das rechtsverletzende Unternehmen in Italien und/oder in Belgien vorgehen können.

5.17. Ihr Antrag sollte eine Bestätigung enthalten, dass die europäische Hauptniederlassung der Unternehmensgruppe oder das mit dem Datenschutz betraute, in der EU ansässige Unternehmen der Gruppe über ausreichende Mittel verfügt oder angemessene Vorkehrungen getroffen hat, um Schadenersatz leisten

zu können, sollte ein Mitglied der Unternehmensgruppe die verbindlichen Unternehmensregelungen verletzen.

- 5.18. Geben Sie in Ihrem Antrag bitte an, welcher Teil der Unternehmensgruppe für die Bearbeitung von Beschwerden zuständig ist, und wie Betroffene Beschwerde einlegen können.
- 5.19. Aus Ihrem Antrag muss eindeutig hervorgehen, dass die Beweislast bei einem angeblichen Verstoß gegen die Regelungen unabhängig vom Ort des Verstoßes bei dem Mitglied der Unternehmensgruppe liegt, von dem aus die Daten übermittelt wurden, oder bei der europäischen Hauptniederlassung oder dem mit dem Datenschutz betrauten Unternehmen der Gruppe.
- 5.20. In Ihrem Antrag sollten Sie bestätigen, dass Sie den betroffenen Personen die in Richtlinie 95/46/EG festgelegten Rechte zugestehen.
- 5.21. In Ihrem Antrag sollten Sie auch bestätigen, dass Sie bei allen Entscheidungen der Kontrollbehörde mit den Datenschutzbehörden zusammenarbeiten und bezüglich der Auslegung des WP 74 dem Rat der Datenschutzbehörde folgen werden.

Bitte erläutern Sie, wie die Verbindlichkeit der Regelungen nach außen zugunsten Dritter erreicht wird.

6. Überprüfung der Einhaltung der Regelungen

- 6.1. In WP74 ist festgelegt, dass in den verbindlichen Unternehmensregelungen einer Unternehmensgruppe interne oder externe Audits oder eine Kombination der beiden vorgesehen sein müssen.
- 6.2. Das Datenschutz-Auditprogramm und der Auditplan müssen klar festgelegt werden, entweder in einer Unterlage, die Ihre Datenschutzregelungen enthält, oder in anderen internen Verfahrensvorschriften. Datenschutzbehörden können auf Anfrage Kopien dieser Audits erhalten. Die Behörde muss davon überzeugt werden, dass das Auditprogramm alle Aspekte der verbindlichen Unternehmensregelungen in angemessener Weise abdeckt und Methoden beinhaltet, die gewährleisten, dass Korrekturmaßnahmen durchgeführt wurden. Der Auditplan sollte der Kontrollbehörde die Möglichkeit einräumen, gegebenenfalls ein eigenes Datenschutzaudit durchzuführen.
- 6.3. Datenschutzbehörden müssen und wollen in Ihren Auditberichten keine Daten einsehen, die sich nicht auf den Datenschutz beziehen. Die Behörden befassen sich nur dann mit der Unternehmensverfassung, wenn sie mit der Einhaltung der Datenschutzbestimmungen kollidiert. Die Behörden haben auch kein Interesse an vertraulichen Geschäftsinformationen. Ihre Angaben sollten sich auf die Anforderungen des Arbeitspapiers WP 74 beschränken. Es lässt sich aber wohl nicht immer vermeiden, dass Informationen, die mit der Einhaltung der Datenschutzregelungen in Zusammenhang stehen, in Berichten enthalten sind, die auch andere Informationen enthalten. Manchmal wird es nicht möglich sein, datenschutzrelevante Elemente von nicht relevanten Elementen zu trennen.

6.4. Alle Informationen werden von der Datenschutzbehörde streng vertraulich behandelt. Informationen, die nicht den Datenschutz betreffen, werden nicht ohne Ihre Zustimmung an Dritte (d. h. andere Datenschutzbehörden) weitergegeben.

6.5. Bitte beschreiben Sie kurz Ihr Datenschutz-Auditprogramm und wie Auditberichte innerhalb Ihrer Unternehmensgruppe behandelt werden (d. h. Angaben zu den Empfängern der Berichte und deren Stellung innerhalb der Unternehmensgruppe).

Bitte beschreiben Sie Ihr Datenschutz-Auditprogramm und Ihren Auditplan.

7. Datenverarbeitung und Informationsfluss

7.1. Aus den verbindlichen Unternehmensregelungen muss Folgendes hervorgehen:

7.1.1. die Art der Daten, d. h. ob sich die verbindlichen Unternehmensregelungen ausschließlich auf eine Datenkategorie, z. B. auf Daten über Humanressourcen, beziehen oder - falls sie sich auf mehrere Datenkategorien beziehen - wie dem in den verbindlichen Unternehmensregelungen Rechnung getragen wird. Die im Antrag enthaltenen Information sollten auf jeden Fall ausreichend sein, dass eine Kontrollstelle feststellen kann, ob die getroffenen Schutzmaßnahmen der Art der Verarbeitung gerecht werden;

7.1.2. die Zwecke der Datenverarbeitung;

7.1.3. das Ausmaß der Übermittlungstätigkeit innerhalb der an die Regelungen gebundenen Unternehmensgruppe. Wir benötigen Angaben über:

7.1.3.1. alle in der EU ansässigen Unternehmen der Gruppe, von denen aus personenbezogene Daten übermittelt werden; und

7.1.3.2. alle außerhalb des EWR ansässigen Unternehmen der Gruppe, an die personenbezogene Daten übermittelt werden können.

7.2. Sie müssen auch angeben, ob die verbindlichen Unternehmensregelungen nur für Datenübermittlungen aus der EU oder für alle Übermittlungsaktivitäten zwischen den Unternehmen der Gruppe gelten. Den Datenschutzbehörden muss klar sein, auf welcher Grundlage Weiterübermittlungen erfolgen (d. h. Datenübermittlungen von nicht im EWR ansässigen Unternehmen an Dritte).

Bitte geben Sie die Art der Daten und die Verarbeitungszwecke an und erläutern Sie das Ausmaß der Übermittlungen innerhalb der Unternehmensgruppe.

8. Datenschutzgarantien

8.1. Die Regelungen müssen eine genaue Beschreibung der Datenschutzgarantien im Sinne der Richtlinie 95/46/EG enthalten und festlegen, wie diesbezügliche Anforderungen innerhalb der Unternehmensgruppe zu erfüllen sind.

8.2. In den verbindlichen Unternehmensregelungen muss insbesondere Folgendes behandelt werden:

- 8.2.1. Transparenz und Fairness gegenüber den betroffenen Personen;
- 8.2.2. Zweckbindung;
- 8.2.3. Gewährleistung der Datenqualität;
- 8.2.4. Sicherheit;
- 8.2.5. Recht des Einzelnen auf Auskunft, Berichtigung und auf Widerspruch gegen die Verarbeitung;
- 8.2.6. Beschränkung der Weiterübermittlung der Daten an Dritte außerhalb der an die Regelungen gebundenen Unternehmensgruppe (obwohl dies unter bestimmten Bedingungen eventuell möglich ist).

Bitte erläutern Sie kurz, wie diese Angelegenheiten in den verbindlichen Unternehmensregelungen Ihrer Unternehmensgruppe behandelt werden und legen Sie die entsprechenden Unterlagen, z. B. Grundsatzpapiere, bei.

9. Meldung und Registrierung von Änderungen

9.1. Gemäß Absatz 4.2 des WP74 muss die Unternehmensgruppe über ein System verfügen, durch das die einzelnen Unternehmen der Gruppe und die Datenschutzbehörde über etwaige Änderungen der Regelungen informiert werden können. Die Datenschutzbehörde muss nur über Änderungen informiert werden, die für die Einhaltung der Datenschutzbestimmungen von Bedeutung sind. Verwaltungstechnische Änderungen müssen beispielsweise nicht mitgeteilt werden, sofern sie keine Auswirkung auf die Gültigkeit der verbindlichen Unternehmensregelungen haben. Ihre federführende Behörde wird Sie über etwaige konkrete Auflagen informieren, die die Meldung oder Aktualisierung der Regelungen bei der Datenschutzbehörde betreffen.

Bitte beschreiben Sie den Mechanismus, mit dessen Hilfe Ihre Unternehmensgruppe Änderungen der Regelungen mitteilt.