

Harald Eul/Petra Eul

Datenschutz International

Praxisleitfaden zur Übermittlung von
Kunden-, Mitarbeiter- und Lieferantendaten

1. Auflage 2011

DATAKONTEXT

Inhalt

Vorwort.....	5
Verzeichnis der Checklisten/Arbeitshilfen/Übersichten.....	11
Abkürzungsverzeichnis.....	13
Vorbemerkung.....	15

TEIL I: PRAKTISCHE BEISPIELE UND HANDLUNGSEMPFEHLUNGEN

1	Zentralisierung (von Teilbereichen) der Personalverwaltung.....	19
1.1	Auftragsdatenverarbeitung nach § 11 BDSG.....	19
1.2	Zulässigkeit für Zwecke des Arbeitsvertrages.....	20
1.3	Zulässigkeit bei eigenen oder fremden berechtigten Interessen.....	20
1.4	Sonderproblem: Sensitive Daten nach § 3 Abs. 9 BDSG.....	21
1.5	Zulässigkeit aufgrund einer Einwilligung.....	22
1.6	Zulässigkeit aufgrund von Betriebsvereinbarungen.....	22
2	Zentrale Gehaltsabrechnung durch Auslandsgesellschaft.....	24
3	Zentralisiertes Kundenmanagementsystem.....	25
3.1	Zur Erfüllung von Vertragszwecken.....	25
3.2	Internationale Kundenbetreuung.....	25
3.3	Zentrale Kundendatenbank als Auftragsdatenverarbeitung.....	26
4	Datenübermittlung für Werbezwecke und Cross-Selling.....	27
4.1	Gewährleistung eines angemessenen Datenschutzniveaus.....	27
4.2	Grundlage Einwilligung.....	27
5	Konzernweites E-Mail-System.....	29
5.1	Zulässigkeit nach Arbeitsvertrag.....	29
5.2	Zulässigkeit bei eigenen oder berechtigten Interessen Dritter.....	30
5.3	Anforderungen der Datenschutzaufsichtsbehörden.....	31
5.4	Einwilligungserfordernis bei weitergehenden Daten.....	31
6	Whistleblowing (Sarbanes-Oxley oder J-SOX).....	34
6.1	Verstöße gegen unternehmensinterne Verhaltensregeln.....	34
6.2	Inhalte und Datenströme beim Whistleblowing.....	34
6.3	Sarbanes-Oxley Act oder J-SOX keine Rechtsvorschriften im Sinne des BDSG.....	34
6.4	Datenschutzgerechte Gestaltung eines Meldeverfahrens.....	35

7	Zentralisierung von Dienstleistungen: Shared Service Center	39
7.1	Standort des Shared Service Center als entscheidender Faktor.....	39
7.2	Auftragsdatenverarbeitung oder Funktionsübertragung.....	39
7.2.1	Shared Service Center als Auftragsdatenverarbeiter.....	40
7.2.2	Shared Service Center als Funktionsübernehmer.....	40
8	Verkauf des Unternehmens: Due Diligence - Was ist zu beachten?	42
8.1	Umfassende Informationen für potenzielle Käufer.....	42
8.2	Rechtsgrundlage: Interessenabwägung nach § 28 Abs. 1 Nr. 2 BDSG.....	42
8.3	Weitergabe von Beschäftigendaten nur im Ausnahmefall.....	43
8.4	Einfluss des Kundenpotenzials auf den Kaufpreis.....	43
8.5	Kaufinteressenten aus dem Ausland.....	44
8.6	Datenschutz auch nach dem Verkauf.....	44
8.7	Besonderheit: Verschmelzung oder Fusion von Unternehmen.....	44
9	Administration/Wartung der Systeme durch Dritte im Drittland	46
9.1	Lesezugriff gleich Übermittlung.....	46
9.2	Gewährleistung eines angemessenen Datenschutzniveaus.....	46
9.3	Herausforderungen beim „Follow-the-Sun-Prinzip“.....	47
10	Datenexport an Zweigstellen bzw. Niederlassungen	48
10.1	Lösungsmöglichkeiten bei Datenweitergabe an unselbstständige Zweigstelle/Niederlassung.....	48
10.2	Datenweitergabe der deutschen Niederlassung an die Hauptniederlassung im Drittland.....	49
11	Fallgruppen zur internationalen Datenübermittlung auf Basis der „Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung“ vom 19. April 2007	50
11.1	Fallgruppe A.....	51
11.2	Fallgruppe B.....	53
11.3	Fallgruppe C.....	55
11.4	Fallgruppe D.....	56
11.5	Fallgruppe E.....	57
11.6	Fallgruppe F.....	58
11.7	Fallgruppe G.....	59
11.8	Fallgruppe H.....	60
11.9	Fallgruppe I.....	61

TEIL II: RECHTSGRUNDLAGEN

1	Allgemeines	65
1.1	Bestimmung der „datenexportierenden Stelle“.....	65
1.1.1	Konzernunternehmen in mehreren EU-Mitgliedstaaten.....	65
1.1.2	Rechtlich unselbstständige Niederlassungen.....	66

1.2	Zweistufige Zulässigkeitsprüfung bei der Übermittlung in ein Drittland.....	67
1.2.1	Prüfschritte gemäß Stufe 1.....	68
1.2.2	Prüfschritte gemäß Stufe 2.....	69
2	Keine Hürden innerhalb der EU und des EWR.....	70
2.1	Prüfschritte für die zulässige Übermittlung in ein anderes EU/EWR-Land.....	70
2.2	Hinweis auf Besonderheiten bei der Auftragsdatenverarbeitung nach § 11 BDSG.....	71
3	Zulässigkeit von Datentransfers in Drittstaaten bei angemessenem Datenschutzniveau.....	72
3.1	Prüfschritte zur Ermittlung des angemessenen Datenschutzniveaus im Drittland.....	72
4	Sonderfall Safe Harbor bei Datenübermittlungen in die USA.....	73
4.1	Offizielle Website für nach Safe Harbor zertifizierte Unternehmen.....	73
4.2	Prüfung des Inhalts der Safe Harbor-Zertifizierung.....	73
4.3	Besondere Anforderungen des Düsseldorfer Kreises.....	73
4.4	Kein Safe Harbor bei bestimmten Branchen.....	74
4.5	Prüfschritte Safe Harbor.....	75
5	Ausnahmen vom Verbot bei nicht angemessenem Datenschutzniveau.....	76
5.1	Einwilligung.....	76
5.2	Erfüllung eines Vertrages (rechtsgeschäftliches Schuldverhältnis).....	77
5.3	Wichtiges öffentliches Interesse oder Verteidigung von Rechtsansprüchen	77
5.4	Lebenswichtige Interessen des Betroffenen.....	77
5.5	öffentliches Register.....	78
5.6	Genehmigung der Aufsichtsbehörde.....	78
5.6.1	Individuelle Vertragsklauseln.....	78
5.6.2	Verbindliche Unternehmensregelungen (BCR).....	78
6	EU-Standardvertragsklauseln.....	80
6.1	Standardvertragsklauseln für die Übermittlung personenbezogener Daten. . . .	80
6.2	Alternative Standardvertragsklauseln für die Übermittlung.....	80
6.3	Standardvertragsklauseln für die Auftragsdatenverarbeitung.....	82
6.3.1	Abgrenzung zu § 11 BDSG.....	82
6.3.2	Besonderheiten beim neuen Standardvertrag für Auftragsdatenverarbeitung.....	83
6.3.2.1	Problemstellungen bei EU/EWR-ansässigen Auftragsdatenverarbeitern.....	83
6.3.2.2	Problemstellungen bei Auftragsdatenverarbeitern im Drittland.....	85
6.4	Funktionsübertragung vs. Auftragsdatenverarbeitung.....	87
6.5	Sonderfall Wartung und Pflege.....	89

7	Vergleich Standardvertragsklauseln mit Binding Corporate Rules und Safe Harbor sowie Vor- und Nachteile der einzelnen Instrumente	91
7.1	Standardvertragsklauseln.....	91
7.2	Binding Corporate Rules.....	92
7.3	Safe Harbor.....	92
8	Zulässigkeit der Datenübermittlung in Drittstaaten auf Grundlage von Betriebsvereinbarungen	94
9	Zusammengefasster Überblick über grenzüberschreitenden Datentransfer	95

ANHANG

A	EU-Standardvertragsklauseln	101
A.1	C2C (Alternativer Standardvertrag).....	101
A.2	C2P.....	109
B	Dokumente des Düsseldorfer Kreises	119
B.1	Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigendatenschutz.....	119
B.2	Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen.....	126
B.3	Auszug aus „abgestimmte Positionen der Aufsichtsbehörden in der AG 'Internationaler Datenverkehr'“.....	128
C	Länder, für die die EU-Kommission ein angemessenes Datenschutzniveau festgestellt hat	129
C.1	Kommissionsentscheidung zu Argentinien.....	130
C.2	Kommissionsentscheidung zu Guernsey.....	137
C.3	Kommissionsentscheidung zu Isle of Man.....	139
C.4	Kommissionsentscheidung zu Jersey.....	143
C.5	Kommissionsentscheidung zu Kanada.....	146
C.6	Kommissionsentscheidung zur Schweiz.....	150
D	Adressen	153
E	Inhalt der CD-ROM	165
	Glossar	167
	Datenschutzverstöße sicher vermeiden durch DLP und Endgeräteschutz	
	Autor: Hilde v. Waidenfels, Sales Manager, itWatch	169
	Index	179

Verzeichnis der Checklisten/Arbeitshilfen/ Übersichten

Checklisten:

Weitergabe von Mitarbeiterdaten an verbundene Unternehmen im Ausland.....	23
Mitarbeiterdaten in unternehmensübergreifenden E-Mail-Systemen und Verzeichnissen.....	32
Whistleblowing.....	37
Prüfschritte angemessenes Datenschutzniveau im Drittland.....	72
Prüfschritte Safe Harbor.....	75
Prüfschritte Einwilligung.....	76
Prüfschritte Vertrag.....	77
Prüfschritte Funktionsübertragung.....	87
Prüfschritte Auftragsdatenverarbeitung.....	88
Zulässigkeit/Nichtzulässigkeit der Datenübermittlung in das Ausland.....	97

Arbeitshilfen:

Beispiel einer Einwilligungserklärung zur Datenweitergabe zu Werbezwecken.....	28
--	----

Übersichten:

Mitgliedstaaten der EU sowie des EWR (Stand September 2010).....	70
Rechtliche Möglichkeiten der Übermittlung pb Daten in Drittländer.....	95
Länder mit angemessenem Datenschutzniveau.....	129
Adresse Europäische Kommission.....	153
Adressen der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten.....	153
Adressen der Datenschutzaufsichtsbehörden der EWR-Mitgliedstaaten.....	160
Adressen Datenschutzaufsichtsbehörden Privatwirtschaft Deutschland.....	161