ecolex

FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT
OKTOBER 2007
10

737–820

Großer Bruder blickt dich an

Überwachung in Büro und Laden
Datenschutz im Datenverkehr

Umwelthaftung
Deckungsvorsorge und Versicherbarkeit

Private Limited Company UK
Directors' Responsibility

UWG-Novelle 2007
Information bei kommerzieller Kommunikation

Finanzstrafrechtliche
Verbandshaftung

Grenzüberschreitende
Abfallverbringung

Gläubiger ohne Grenzen
Europäisches Bagatellverfahren

MANZ

SCHWERPUNKT

Big Brother im Unternehmen

Unternehmen werden gegenüber ihren Mitarbeitern immer mehr zum „Big Brother". Mitarbeiter werden mit Videokameras aufgezeichnet, durch Zutritts- und Zeiterfassungssysteme kontrolliert, Mitarbeitergespräche werden elektronisch geführt und Mitarbeiterdaten konzernweit vernetzt.

Datenanwendungen, ihre Rechtsprobleme und deren Lösung

RAINER KNYRIM / BARBARA BARTLMÄ

A. Unternehmen unter Druck

Durch Medienberichte,[1]) neuerdings aber auch durch Betriebsräte, geraten Unternehmen in jüngster Zeit verstärkt unter Druck, sich mit den Rechtsfragen ihrer Datenanwendungen auseinanderzusetzen. Jüngst zeigte der Fall einer biometrischen Zeiterfassung in einem Krankenhaus, die mit – vom OGH bestätigter[2]) – EV vom Betriebsausschuss „abgedreht" wurde,[3]) die Notwendigkeit, bei der Einführung oder Erneuerung von Datenanwendungen im Personalbereich die anstehenden Rechtsprobleme eingehend aufzuarbeiten. Die nachstehenden Ausführungen beschränken sich auf vier aktuelle Themen.[4])

B. Datenanwendungen, deren Rechtsprobleme und Lösung

1. Zeiterfassung und Zutrittskontrolle

Der OGH[5]) hat erstmals zur Frage, ob die Speicherung personenbezogener Daten (biologische Merkmale) im Rahmen eines biometrischen Zeiterfassungssystems die Menschenwürde berührt und damit die Zustimmung des Betriebsrats (BR) zur Einführung eines solchen Systems zwingend einzuholen ist, Stellung genommen:

Er beurteilte dieses System als Kontrollmaßnahme iSd § 96 Abs 1 Z 3 ArbVG, die geeignet ist, die Menschenwürde der Arbeitnehmer zu berühren und untersagte es vorläufig mittels EV, weil der BR umgangen worden war. Eine Interessenabwägung habe ergeben, dass die Interessen der Mitarbeiter am Schutz ihrer Privatsphäre schwerer wiegen als das „vergleichsweise triviale Ziel" der Kontrolle der Kommens- und Gehenszeiten. Mit Zustimmung des BR könnten derartige Systeme aber zulässig sein, ebenso bei anderer Ausgestaltung (zB Zutrittskontrollsystem, das nur zwischen „berechtigter" und „unberechtigter" Person unterscheidet). Außerdem schien dem OGH eine differenzierte Betrachtung nach dem Unternehmensbereich geboten (zB strengere Zutrittskontrollen im Bankensektor). Die Argumentation des Krankenhauses war – was bei solchen Projekten oft festzustellen ist – sehr „technisch" (das System sei ua gegen Hitze, direkte Sonneneinstrahlung, Kratzer etc weitgehend resistent) und der OGH kritisierte, dass offensichtlich nur an die „Betriebssicherheit" der Fingerscanner selbst gedacht wurde und weniger an jene der Arbeitnehmer.

Arbeits- und datenschutzrechtlich muss bei der Einführung von Zeiterfassungs- und Zutrittskontrollsystemen unbedingt eine Abwägung zwischen den Interessen der betroffenen Arbeitnehmer und jenen des Unternehmens vorgenommen werden.[6]) Es hängt von der konkreten Ausgestaltung des Systems ab, ob dieses grundsätzlich zulässig ist. So kann es bei einem Zutrittskontrollsystem einen wesentlichen Unterschied machen, ob nur freigeschaltet (bei Durchschieben des Magnetstreifens) oder ob jeder einzelne Zutritt personenbezogen gespeichert und in der Folge zur „Überprüfung" mit den Daten aus der Zeiterfassung verknüpft[7]) oder zur Erstellung von „Bewegungsprofilen" auf Betriebsgeländen oder in Bürogebäuden verwendet wird. In derartigen Fällen müsste einerseits das Zweckbindungs- und Wesentlichkeitsprinzip des § 6 Abs 1 Z 2 und 3 DSG 2000 und die Zulässigkeit eines solchen Systems eingehend hinterfragt werden, andererseits könnte dies wieder arbeitsverfassungsrechtliche Konsequenzen haben: Ist eine genaue Darstellung der Bewegung des Arbeitnehmers – zB das Aufsuchen der Toiletten oder des BR, das Pflegen informeller Kontakte – möglich, kann dies ein die Menschenwürde berührendes Kontrollsystem sein.[8]) Selbst wenn man ein Berühren der Menschenwürde verneint, wäre zu prüfen, ob Zutrittskontrollsysteme nicht als Personaldatensysteme nach § 96a Abs 1 Z 1 ArbVG zustimmungspflichtig wären. Datenschutzrechtlich zu beachten sind überdies allfällige Meldepflichten solcher Systeme. Zwar enthalten sowohl die Standardanwendung SA002 „Personalverwaltung für privatrechtliche Dienstverhältnisse" und die Musteranwendung MA002 „Zu-

Dr. *Rainer Knyrim* ist Partner bei Preslmayr Rechtsanwälte, Wien; Dr. *Barbara Bartlmä,* LL.M., ist Partner bei Bartlmä Madl Köck Rechtsanwälte, Wien.

1) ZB: Titelstory des „Gewinn", Mai 2007: „So werden Sie vom Chef überwacht!".

2) OGH 20. 12. 2006, 9 ObA 109/06d, ecolex 2007/161 = RdW 2007/373 = ARD 5754/1/2007.

3) Der BR ist allerdings nicht immer erfolgreich, s OGH 29. 6. 2006, 6 ObA 1/06z, ecolex 2006/859 = RdW 2007/43.

4) Zu weiteren Themen, etwa Whistleblowing oder Outsourcing s zB *Knyrim/Kurz/Haidinger,* Whistleblowing-Hotlines: Mitarbeiter „verpfeifen" zulässig? ARD 5681/5/2006; *Knyrim/Siegel/Autengruber,* Datenschutz und Datenrettung beim Outsourcing, ecolex 2004, 413.

5) Siehe FN 2.

6) § 1 Abs 1 DSG 2000; näher ausgestaltet in § 8 Abs 1 DSG 2000, wobei die Freiwilligkeit der Mitarbeiterzustimmung immer mehr in Diskussion steht.

7) Die DSK hinterfragt die Zulässigkeit jeder einzelnen im System abgelegten Datenart, s etwa E DSK 16. 11. 2004, K 120.951/0009-DSK/2004 und dazu *Brodil,* Zeiterfassung ohne Zeiterfassung? ecolex 2005, 459.

8) OLG Wien 20. 10. 1995, 9 Ra 123/95, ARD 4714/17/96; s auch die bereits zitierte E des OGH zur biometrischen Zeiterfassung.

trittskontrolle“[9]) eine Reihe von Datenarten, dennoch ist anhand der im System verwendeten Datenarten genau zu vergleichen, ob nicht mehr als die im SA002 oder MA002 enthaltenen Datenarten verarbeitet werden und somit eine DVR-Meldepflicht vorliegt.[10])

2. Videoaufzeichnung

Als am 20. 1. 2006 die Polizei das Foto des mutmaßlichen Diebes der „Saliera“ in den Medien veröffentlichte, das aus der Videoaufzeichnung eines Handyshops stammte, in dem der Dieb ein Wertkartenhandy erworben hatte, war die Zulässigkeit von Videoaufzeichnung durch Unternehmen plötzlich in aller Munde. Datenschutzrechtlich sind Videoüberwachungsanlagen, sofern sie die Videobilder aufzeichnen, vorab bei der Datenschutzkommission (DSK) zu genehmigen. Dies, da nach damaligem Meinungsstand der DSK Videobilder sensible Daten etwa über den Gesundheitszustand (zB Rollstuhlfahrer) bzw ethnische Herkunft (zB Hautfarbe) enthalten können, die eine Vorabgenehmigungspflicht[11]) auslösen (§ 18 Abs 2 Z 1 DSG 2000). Nach aktuellem Meinungsstand wird die Vorabgenehmigungspflicht durch die voraussichtlich enthaltenen strafrechtlich relevanten Daten (zB aufgezeichneter Diebstahl) ausgelöst (§ 18 Abs 2 Z 2 DSG 2000). Es gibt zu den Rechtsfragen der Videoaufzeichnung verschiedene Meinungen.[12]) Das Regierungsprogramm für die 23. GP sieht die Schaffung spezifischer Regelungen für die private Videoaufzeichnung vor. Ob sich an der bestehenden Rechtslage und an der Genehmigungspflicht etwas ändern wird, bleibt abzuwarten. Derzeit ist Unternehmen – allein aufgrund der Sichtbarkeit der Kameras – zu empfehlen, Videoüberwachungsanlagen zur Genehmigung einzureichen. Die Meldung erfolgt grundsätzlich mit einem normalen Registrierungsformular.[13]) Im Meldeverfahren werden oft nähere Angaben über die technische Ausgestaltung des Systems nachgefragt, insb zur Speicherdauer (besonders bei mehr als 72 h), zu den Standorten und Ausführung der Kameras (schwenk-/zoombar?), Ausführungen dazu, ob der angestrebte Zweck (zB Eigentumsschutz und statistisches Material dazu – etwa über stattgefundene Einbrüche, Diebstähle etc) nicht mit anderen, gelinderen Mitteln erreicht werden kann (etwa durch den vermehrten Einsatz von Sicherheitspersonal) etc. Weiters erwartet die DSK die Vorlage einer BV zum geplanten Einsatz der Videoüberwachung, soweit diese Mitarbeiter erfasst.

Aus arbeitsverfassungsrechtlicher Sicht sind gewisse Videoüberwachungssysteme – unabhängig von einer BV – unzulässig, weil sie die Menschenwürde eines Arbeitnehmers verletzen (zB Videoüberwachung in Toiletten oder Waschräumen; Videokameras, die permanent auf den Arbeitsplatz eines Arbeitnehmers gerichtet sind und lediglich der Arbeitnehmerkontrolle dienen). Ist aber primärer Zweck der Überwachungssysteme die Früherkennung oder Abwehr von Gefahren (zB Diebstahlschutz) und ist die Kontrolle der Arbeitnehmer bloß ein Nebenaspekt dieser Gefahrenabwehr, geht man von einem bloßen Berühren der Menschenwürde aus (§ 96 Abs 1 Z 3 ArbVG), sodass mit Zustimmung des BR (in betriebsratlosen Betrieben mit Zustimmung der einzelnen Arbeitnehmer gem § 10 AVRAG) derartige Systeme zulässig sind. Zum Teil wird Videoüberwachung auch als mitbestimmungspflichtiges Personaldatensystem iSd § 96 a Abs 1 Z 1 ArbVG beurteilt.[14]), [15])

3. Konzerndatenbanken

Ergänzend zum Beitrag *Leissler*[16]) wird die aktuelle Jud der DSK zu den in der Praxis häufigen Fällen besprochen, in denen weder ein Safe Harbor-Unternehmen als Empfänger noch die Ausnahmen zur Genehmigungspflicht des § 12 DSG 2000 vorliegen.

Aufgrund eines im Datenschutzrecht fehlenden „Konzernprivilegs“ führt bereits die bloße Speicherung von Personaldaten in einem Konzern-Rechenzentrum in einem Drittstaat (etwa auf dem zentralen Server der Konzernmutter) zu einer Genehmigungspflicht, sofern keine der Ausnahmen gem § 12 DSG 2000 vorliegen. Sinnvollerweise greift man dabei auf die Standardvertragsklauseln (SVK) „Dienstleister“[17]) der EU-Kommission zurück, lässt diese vom öDatenexporteur und der ausländischen Konzerngesellschaft, die die Datenspeicherung als Dienstleister vornimmt, unterfertigen und reicht diese bei der DSK ein. Wichtig ist, dass in diesem Fall bloß eine rein technische Dienstleistung (Speicherung) vorgenommen wird und von der ausländischen Konzerngesellschaft keine weitergehende Verwendung der Daten erfolgt. Ist der Antrag auf die reine Speicherung beschränkt und werden die unterschriebenen SVK vorgelegt, so ist die Genehmigung von der DSK zu erteilen.[18])

Der nächste Schritt der „Datenglobalisierung“ im Konzern ist oft die Auswertung der Personaldaten in Form sog „Konzernreports“ für Statistik und Planung. Handelt es sich dabei um ausschließlich indirekt personenbezogene Daten, so wäre die Übermittlung nach § 12 Abs 3 Z 2 DSG 2000 genehmigungsfrei. Regelmäßig ist bei Konzernplanungen (etwa bei der Planung eines internationalen Personaleinsatzes für Großprojekte oder der Planung neuer Stellen) aber ein personenbezogener Zugriff notwendig. Auch hier empfiehlt sich wieder der Abschluss der SVK, allerdings jener für Auftraggeber[19]) inkl einer ausdrücklichen Zusage der Konzernmutter, dass die Daten

9) Standard- und Muster-Verordnung 2004 (StMV 2004), BGBl II 2004/312.

10) Siehe auch *Burgstaller,* Arbeitszeitkontrolle durch Fingerscans, lex:itec 03/2007, 16.

11) Siehe das Ausfüllmuster auf www.dsk.gv.at mit Stand v 25. 7. 2007.

12) Siehe etwa *König,* Videoüberwachung und Datenschutz: Ein Kräftemessen, in *Jahnel/Siegwart/Fercher* (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) 109 f; *Steiner/Andréewitch,* Videoüberwachung aus datenschutzrechtlicher Sicht, MR 2006, 80.

13) DVR Form 2 (Anl 2 zur DVRV 2002, BGBl II 2002/24).

14) AK Wien, Rechtsgutachten Videoüberwachung im Betrieb, infas 2006, 121 f.

15) Siehe dazu auch *Riesenkampff* in diesem Heft, S 743.

16) In diesem Heft, S 747.

17) Standardvertragsklauseln für die Übermittlung personenbezogener Daten und Auftragsverarbeiter in Drittländern nach der Datenschutz-RL 95/46/EG, Kom 2002/16/EG, ABl 2002 L 6 S 52.

18) Siehe etwa DSK 21. 3. 2007, K178.234/0006-DSK/2007, ARD 5784/8/2007; *Knyrim* vertrat den Antragssteller im Verfahren vor der DSK.

19) E der Kom 2001/497/EG, ABl 2001 L 181 S 19 oder Kom 2004/915/EG, ABl 2004 L 385 S 74.

nur für den beantragten Zweck und nicht für sonstige personenbezogene Auswertungen verwendet werden. Die DSK hat einen derartigen Antrag unter der Auflage genehmigt, dass diese Zusage der Konzernleitung eingehalten wird.[20]) Liegt diese Erklärung nicht vor und ist der im Genehmigungsantrag angegebene Zweck – zB „Bearbeitung" – der Daten unklar, so kann es zu ernsthaften Problemen bis hin zu einer Nichtgenehmigung durch die DSK kommen.[21])

Weitere typische Konzernanwendungen sind die Zuteilung von Mitarbeiteraktienoptionen, die Verteilung von Bonuszahlungen, Schulungsplanung durch damit befasste Konzerngesellschaften, Zentralisierung der Daten hinsichtlich der EDV-Ausstattung und des EDV-Zugangs der Mitarbeiter sowie die Übermittlung von Daten der oberen Führungsebene oder von „High Potential"-Mitarbeitern.[22]) Die DSK prüft dabei die Zulässigkeit der Übermittlung jeder einzelnen Datenart äußerst genau.[23])

Je umfangreicher die Datenanwendungen und je breiter ihr Verwendungszweck, desto schwieriger ist eine Genehmigung der DSK zu erhalten und desto ausführlicher muss das Vorbringen sein, warum überwiegende berechtigte Konzerninteressen bestehen. In einer der jüngsten E[24]) der DSK sprach diese sehr weitgehende, überwiegende berechtigte Konzerninteressen zu:

Es wurde neben einer Standardanwendung zum „Rechnungswesen" auch das Software-Modul „mySAP CRM" zur Genehmigung eingereicht, wobei die empfangenden Konzerngesellschaften in ca 50 Drittstaaten ansässig waren. Neben den SVK wurde ein umfangreiches Dokument vorgelegt, in dem die Funktionsweise des internationalen Konzerns erklärt wurde. Die beiden Datenanwendungen enthielten Kunden-, Interessenten- und Mitarbeiterdaten und umfassten mehrere Zwecke. Zur Übermittlung von Mitarbeiterdaten zur Ermöglichung der Kommunikation mit anderen Konzernunternehmen ging die DSK schlicht von einem Vorliegen eines überwiegenden berechtigten Interesses der beteiligten Unternehmen aus. Für die Verwendung von Daten zum Zweck des „Leistungsmanagements" machte die DSK das Vorliegen einer entsprechenden BV zur Bedingung der Zulässigkeit der Datenübermittlung für diesen Zweck. Zum Zweck der finanziellen und betriebswirtschaftlichen Analyse und zur Geschäftsstrategieentwicklung und der dafür notwendigen Datenübermittlung hielt die DSK sogar fest, dass es einsichtig sei, dass innerhalb eines Konzerns gerade der Zweck unternehmensübergreifender Analyse und Planung berechtigt sei, wenn nicht die Sinnhaftigkeit der Konzernstruktur an sich in Frage gestellt werden soll.

Arbeitsverfassungsrechtlich werden die zuvor genannten Datenanwendungen meistens als Personaldatensysteme iSd § 96 a Abs 1 Z 1 ArbVG eingestuft. Nach dieser Bestimmung bedarf die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen der Zustimmung des BR. Eine Zustimmung ist nicht erforderlich, soweit die tatsächliche oder vorgesehene Verwendung dieser Daten über die Erfüllung von Verpflichtungen nicht hinausgeht, die sich aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergeben. Die Zustimmung des BR kann im Streitfall allenfalls über die Schlichtungsstelle erzwungen werden.

4. Elektronische Mitarbeitergespräche, -beurteilungen und -schulungen

Aktueller Trend in Unternehmen ist, dass immer mehr Bereiche der „Human Resources"-Verwaltung auf elektronische Basis – insb Internet/Intranet-Applikationen – umgestellt werden. So werden Mitarbeitergespräche nicht mehr mit dem Vorgesetzten unter vier Augen, sondern mittels Web-Formularen erledigt. Beurteilungen von Mitarbeitern durch Vorgesetzte und Mitarbeiterschulungen werden nur mehr „virtuell" über das Internet durchgeführt. Da die verwendeten Applikationen höchst unterschiedlich und meist sehr neu sind, können hier nur einige Problemfelder angerissen werden: Bei den elektronischen Mitarbeitergesprächen und -beurteilungen zeigt sich zunächst, dass in internationalen Konzernen zum Teil eine andere Fragekultur vorherrscht und eine sehr allgemeine, vage und verbale Beurteilung von „Soft Skills" erfolgt.[25]) Hier ist uU eine „Filterung" der Fragen und Beurteilungsmöglichkeiten angebracht, um nicht beim BR oder den Mitarbeitern Unverständnis auszulösen. Weiters ist zeitversetztes Bearbeiten durch den Mitarbeiter selbst und durch den Vorgesetzten möglich, was zu vollkommen unterschiedlichen Ergebnissen führen kann, deren Auswertung und Auswirkung hinterfragt werden muss. Abgeklärt werden muss, ob Zugriffe von anderen Konzerngesellschaften erfolgen, wie weit sie gehen und welche Rechtfertigung es dafür gibt. Bei Online-Mitarbeiterschulungen oder -umfragen ist zu klären, ob und unter welchen Voraussetzungen ein Personenbezug hergestellt werden kann und inwieweit Prüfungserfolge durch Mitprotokollierung kontrolliert werden könnten. Derartige technische Möglichkeiten der Beurteilung können zu einer Mitbestimmung durch den BR führen und die Zulässigkeit ist auch datenschutzrechtlich zu hinterfragen.

In den meisten Fällen werden diese Datenanwendungen nicht unter die Standardanwendung SA002 „Personalwesen" subsumierbar und daher beim DVR zu melden sein; sofern internationaler Datenverkehr stattfindet, ist dieser entsprechend aufzuarbeiten, wobei die Rsp der DSK zu elektronischen Mitarbeitergesprächen und -beurteilungen derzeit noch spärlich ist.[26])

20) DSK 10. 5. 2006, K178.211/0012-DSK/2006, ARD 5784/9/2007.

21) Zu einer Nichtgenehmigung kam es in der E DSK 21. 3. 2007, K178.231/0007-DSK/2007, ARD 5784/10/2007.

22) Alle genehmigt durch DSK 20. 10. 2006, K178.215/008-DSK/2006; *Knyrim* vertrat das Unternehmen im Verfahren vor der DSK.

23) Siehe etwa E DSK 20. 10. 2006, K178.215/008-DSK/2006 zu bestimmten Daten in einer Notfallkontaktdatenbank.

24) E DSK 15. 6. 2007, K178.248/0006-DSK/2007 verbunden mit K178.234/0008-DSK/2007, abrufbar unter www.ris.bka.gv.at/dsk; *Knyrim* vertrat das Unternehmen im Verfahren vor der DSK. Zum internationalen Datenverkehr ist im Übrigen auf die bestehende Lit zu verweisen, etwa *Knyrim,* Datenschutzrecht 115 ff; *Knyrim,* Checkliste: Zulässigkeit internationalen Datenverkehrs nach DSG 2000, ecolex 2002, 470; *Räther/Seitz,* Übermittlung personenbezogener Daten in Drittstaaten, MMR 2002, 425.

25) Siehe etwa www.lominger.com, wo nicht nur standardisierte verbale Fragen und Beurteilungskataloge, sondern dazu Handbücher, Schulungen und auch gleich Softwaremodule angeboten werden.

26) ZB E DSK 23. 5. 2007, K178.239/006-DSK/2007; 20. 1. 2006, K178.215/0008-DSK/2006.

Aus arbeitsverfassungsrechtlicher Sicht ist zu beachten, dass die Einführung von Systemen zur Beurteilung von Arbeitnehmern des Betriebs, sofern mit diesen Daten erhoben werden, die nicht durch die betriebliche Verwendung gerechtfertigt sind, der Zustimmung des BR bedarf (§ 96a Abs 1 Z 2 ArbVG). Gemeint sind hier planmäßige, nach einem bestimmten Konzept geordnete Bewertungen, deren Grundlage zur Beurteilung des Arbeitnehmers geeignete Daten sind (zB Verantwortungsbewusstsein, Teamfähigkeit, Belastbarkeit, Selbständigkeit, Risikobereitschaft etc). Daten iZm unsicherer oder erst in späterer Zukunft geplanter Verwendung des Mitarbeiters sind nicht durch die betriebliche Verwendung gerechtfertigt und bedürfen somit der Zustimmung des BR (zB Eignungstests, aufgabenorientierte Förderungen oder leistungsorientierte Beförderungen, Beurteilungen wie Assessment-Center, Gespräche zum Erkennen von Potenzialen etc). Durch Involvierung des BR sollen subjektive Elemente in der Beurteilung hintangehalten und eine Objektivierung des Beurteilungssystems erreicht werden.

SCHLUSSSTRICH

Permanent fortschreitende Vernetzung der Mitarbeiterdatenverarbeitungen und verstärkte elektronische Überwachung setzen Unternehmen – va durch Anfrage der Betriebsräte – unter Druck, Rechtsprobleme dieser Datenanwendungen zu analysieren und so zu lösen, dass ein rechtskonformer Zustand eintritt. Arbeitsverfassungsrechtlich erfordert dies meist die Involvierung des BR und den allfälligen Abschluss von Betriebsvereinbarungen. Aufgrund der schutzwürdigen Geheimhaltungsinteressen jedes einzelnen Mitarbeiters ist eine datenschutzrechtliche Aufarbeitung notwendig: Diese beginnt mit einer (rechtzeitigen!) Analyse der geplanten Datenanwendungen (Ziele, Funktionsweise, Datenarten, Übermittlungsempfänger) und endet mit deren allenfalls notwendigen Registrierung im Datenverarbeitungsregister; oft parallel dazu mit der Einholung von Vorab-Genehmigungen zum internationalen Datenverkehr bei der DSK.