02107/07/DE
WP 142

Stellungnahme 9/2007 zum Umfang des Schutzes personenbezogener Daten auf den Färöern

Angenommen am 9. Oktober 2007

STELLUNGNAHME DER GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995

zum Umfang des Schutzes personenbezogener Daten auf den Färöern

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1], („die Richtlinie"), insbesondere auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe b,

gestützt auf ihre Geschäftsordnung[2], insbesondere auf Artikel 12 und 14,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINFÜHRUNG: DATENSCHUTZGESETZ AUF DEN FÄRÖERN

1.1. Situation der Färöer

Die Färöer liegen im Nordatlantik. Sie bestehen aus 18 Inseln, die durch Meerengen oder Fjorde voneinander getrennt sind. Die Inseln sind administrativ in sieben Verwaltungsbezirke mit etwa 120 Kommunen unterteilt. Die Färöer bilden zusammen mit Dänemark und Grönland das Königreich Dänemark. Das Königreich ist eine konstitutionelle Monarchie.

Gemäß dem Autonomiegesetz von 1948 sind die Inseln ein selbstverwaltetes Gemeinwesen innerhalb des Königreichs Dänemark. Das Autonomiegesetz unterteilt sämtliche Politikbereiche in zwei Hauptgruppen: Die allgemeinen Angelegenheiten fallen in die Zuständigkeit des Königreichs, die besonderen (färöischen) Angelegenheiten fallen in die Zuständigkeit der autonomen färöischen Verwaltung und Gesetzgebung.

Gemäß dem Autonomiegesetz ist für Gesetzgebung und Verwaltung im Bereich der „besonderen Angelegenheiten" die färöische Staatsgewalt, bestehend aus Parlament und Regierung, zuständig[3]. Bereiche, die nicht als „besondere Angelegenheiten" übertragen wurden, gelten als „allgemeine Angelegenheiten", für die weiterhin die legislativen und administrativen Organe des Königreichs zuständig sind.

---

1 ABl. L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/de/media/dataprot/index.htm

2 Verabschiedet auf der dritten Sitzung der Gruppe vom 11.9.1996.

3 Autonomiegesetz, Artikel 1.

Doch selbst in diesen Bereichen können bestimmte Befugnisse, beispielsweise die Durchführung oder Verabschiedung bestimmter Regelungen im Rahmen der königlichen Verordnungen, delegiert werden. Wurde ein Politikbereich im Zuge der Selbstverwaltung übertragen, ist davon auszugehen, dass die Färöer in vollem Umfang wirtschaftlich, gesetzgeberisch und administrativ für einen spezifischen Bereich zuständig sind.

Die Regelungen auf den Färöern hinsichtlich personenbezogener Daten basieren auf vom färöischen Parlament erlassenen Gesetzen sowie auf Gesetzen zur Regelung „allgemeiner Angelegenheiten". Das Datenschutzgesetz wurde 2001 vom färöischen Parlament verabschiedet und wird von der färöischen Datenschutzbehörde durchgeführt.

Das dänische Datenschutzgesetz gilt nur für die Datenverarbeitung durch Organe und Einrichtungen des Königreichs (wie Polizei, Staatsanwaltschaft, Bezirksgefängnis sowie Gefängnis- und Bewährungswesen, Hoher Kommissar der Färöer, Datenverarbeitung im Bereich des Familienrechts sowie kirchliche Behörden). Da das dänische Datenschutzgesetz[4] auf der Richtlinie beruht, gehen wir davon aus, dass dieses Gesetz zumindest angemessenen Schutz hinsichtlich der Verarbeitung personenbezogener Daten bietet. Die genannten Bereiche sind deshalb in der vorliegenden Stellungnahme nicht berücksichtigt worden.

1.2. Geltender datenschutzrechtlicher Rahmen:

Der Kommentar über die vorbereitenden Arbeiten zur Erstellung eines färöischen Datenschutzgesetzes lässt darauf schließen, dass sowohl dänisches als auch norwegisches Datenschutzrecht berücksichtigt wurde. Gemäß einer Reihe durch Dänemark zwischen 1994 und 2003 abgegebener Erklärungen wurden die Protokolle 7, 9 und 13 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten von 1950 in den Färöern umgesetzt. Gemäß einer zum Zeitpunkt der Ratifizierung von Dänemark abgegebenen Erklärung gilt Konvention Nr. 108 nicht für die Färöer.

Das Datenschutzsystem umfasst eine Reihe unterschiedlicher Regelungen zum Schutz von Personen, über die Daten verarbeitet werden. Diese Regelungen basieren auf ähnlichen Prinzipien und Werten wie sie auch durch das EU-Recht begründet werden. Das Gesetz über die Verarbeitung personenbezogener Daten („Datenschutzgesetz")[5] ist die wichtigste für den Bereich des Datenschutzes geltende Rechtsvorschrift auf den Färöern. Dieses Gesetz spiegelt eindeutig den Inhalt der Richtlinie wider.

Gemäß Artikel 299 des Vertrags zur Gründung der Europäischen Gemeinschaft gilt die Richtlinie nicht für die Färöer. Die Färöer gelten deshalb als Drittland im Sinne von Artikel 25 und 26 der Richtlinie.

---

4 Gesetz Nr. 429 vom 31. Mai 2000 über die Verarbeitung personenbezogener Daten. Dieses Gesetz dient zur Umsetzung der Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

5 Gesetz Nr. 73 vom 8. Mai 2001.

2. BEURTEILUNG DES DATENSCHUTZGESETZES DER FÄRÖER IM HINBLICK AUF EINEN ANGEMESSENEN SCHUTZ PERSONENBEZOGENER DATEN

Die Artikel-29-Datenschutzgruppe („Gruppe“) beurteilt die Angemessenheit des Datenschutzrechts der Färöer anhand des Gesetzes über die Verarbeitung personenbezogener Daten („Datenschutzgesetz“).

Beurteilungskriterien

Die Kriterien für die Beurteilung des Datenschutzsystems auf den Färöern, die im Dokument *Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU* (WP 12 5025/98)[6] der Datenschutzgruppe niedergelegt sind, lassen sich wie folgt zusammenfassen:

1. Inhaltliche Grundsätze
    - Beschränkung der Zweckbestimmung
    - Datenqualität und -verhältnismäßigkeit
    - Transparenz
    - Sicherheit
    - Recht auf Auskunft, Berichtigung und Widerspruch
    - Beschränkung der Weiterübermittlung in andere Drittländer
    - Weitere, auf spezifische Arten der Verarbeitung anwendbare Grundsätze, wie z. B. auf i) sensible Daten, ii) Direktmarketing und iii) automatisierte Einzelentscheidungen

2. Verfahrensrechtlicher Mechanismus/Durchsetzungsmechanismus
    - Gewährleistung einer guten Befolgungsrate der Vorschriften
    - Unterstützung für einzelne betroffene Personen
    - Gewährleistung angemessener Entschädigung für die geschädigte Partei

Das Datenschutzgesetz gilt für die Verarbeitung personenbezogener Daten von natürlichen Personen im privaten und öffentlichen Sektor.[7] Es gilt jedoch nur, *„falls: 1) die Verarbeitung personenbezogener Daten ganz oder teilweise automatisiert geschieht, 2) die personenbezogenen Daten in einer Datei gespeichert sind oder gespeichert werden sollen, und dies eine nicht automatisierte, systematische Verarbeitung von Daten darstellt“*.[8] Das Datenschutzgesetz gilt nicht für die Verarbeitung personenbezogener Daten, die von einer natürlichen Person zur Durchführung von Aktivitäten rein privater Natur vorgenommen wird.[9]

Gemäß dem Datenschutzgesetz werden „personenbezogene Daten“ als *„alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person’)“* definiert.[10] Diese Definition stimmt mit dem ersten Teil der in der

---

6 Siehe auch Europäische Kommission (Hg.), *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data*, Luxemburg: Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften, 1998.

7 Artikel 1 sowie Artikel 3 Absatz 1 Datenschutzgesetz.

8 Artikel 3 Absatz 1 Datenschutzgesetz. Diese Regelung stimmt mit Artikel 3 Absatz 1 der Richtlinie 95/46/EG überein.

9 Artikel 3 Absatz 2 Datenschutzgesetz.

10 Artikel 2 Absatz 1 Datenschutzgesetz.

Richtlinie in Artikel 2 Buchstabe a enthaltenen Definition von „personenbezogenen Daten“ überein.

2.1. Inhaltliche Grundsätze

Fundamentale Grundsätze

Der Grundsatz der Beschränkung der Zweckbestimmung verlangt, dass Daten für einen spezifischen Zweck zu verarbeiten und dementsprechend nur zu verwenden oder weiter zu übermitteln sind, soweit dies mit der Zweckbestimmung der Übermittlung nicht unvereinbar ist. Die einzigen Ausnahmen von dieser Regel sind die in einer demokratischen Gesellschaft aus einem der in Artikel 13 der Richtlinie aufgeführten Gründe notwendigen Fälle. Gemäß Artikel 9 der Richtlinie sind zur Gewährleistung der freien Meinungsäußerung ebenfalls Ausnahmen möglich.

Die Gruppe ist der Überzeugung, dass das färöische Recht diesem Grundsatz entspricht. Artikel 8 Absatz 2 des Datenschutzgesetzes sieht vor, dass personenbezogene Daten ausschließlich für festgelegte und rechtmäßige Zwecke in Einklang mit der Tätigkeit des für die Verarbeitung Verantwortlichen erhoben und in keiner mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Ausnahmen hiervon gelten im Falle der ausdrücklichen Zustimmung und im Falle von Daten zu historischen, statistischen oder wissenschaftlichen Zwecken. Es gibt weniger Ausnahmen als dies im Artikel 13 der Richtlinie vorgesehen ist.

Der Grundsatz der Datenqualität und -verhältnismäßigkeit verlangt, dass Daten sachlich richtig und, wenn nötig, auf dem neuesten Stand gehalten werden. Die Daten sollen angemessen, relevant und nicht über den Zweck hinausgehen, für den sie übermittelt oder weiterverarbeitet werden.

Artikel 8 Absatz 3 des Datenschutzgesetzes sieht vor, dass die Daten für die Zwecke, für die sie erhoben und/oder weiterverarbeitet werden, erheblich sein müssen und nicht darüber hinausgehen dürfen. Artikel 8 Absatz 6 sieht vor, dass die Verarbeitung von Daten sachlich richtig zu erfolgen hat und dass diese Verarbeitung so organisiert sein muss, dass eine erforderliche Aktualisierung der Daten gewährleistet ist. Durch dazu notwendige Überprüfungen ist außerdem sicherzustellen, dass Daten, die sich als nichtzutreffend oder irreführend herausstellen, unverzüglich gelöscht oder berichtigt werden. Die Gruppe ist deshalb der Auffassung, dass das färöische Recht diesem Grundsatz entspricht.

Der Grundsatz der Transparenz verlangt, dass natürliche Personen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Drittland für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten müssen, sofern dies aus Billigkeitsgründen erforderlich ist. Ausnahmen sind lediglich im Einklang mit den Artikeln 11 Absatz 2 und 13 der Richtlinie möglich.

Dieser Grundsatz wird durch Artikel 21 des Datenschutzgesetzes erfüllt, der für den Fall, dass die Daten von einer anderen als der betroffenen Person erhalten wurden, vorsieht, dass der für die Erhebung der Daten Verantwortliche die betroffene Person darüber informiert, welche personenbezogenen Daten erhoben wurden, und zudem

den Namen und die Anschrift des für die Verarbeitung Verantwortlichen und die Zweckbestimmungen der Verarbeitung angibt. Der für die Erhebung der Daten Verantwortliche muss außerdem für den Fall, dass die personenbezogenen Daten weitergeleitet werden, über diese Tatsache und den Empfänger der Daten informieren und zusätzlich sämtliche anderen Informationen zur Verfügung stellen, die erforderlich sind, damit die betroffene Person ihre rechtmäßigen Interessen wahren kann. Diese Regelungen gelten nicht, falls die betroffene Person bereits über die genannten Informationen verfügt, falls die Speicherung oder Weitergabe per Gesetz vorgesehen ist oder falls es unmöglich ist bzw. unverhältnismäßigen Aufwand erfordert, die betroffene Person zu informieren.

Die Ausnahmen – falls die Weitergabe die Sicherheit des Staates oder die Außenpolitik beeinträchtigen würde, falls ein Zusammenhang mit der Verhütung von Straftaten besteht, falls die Weitergabe aus gesundheitlichen oder persönlichen Gründen nicht im Interesse der betroffenen Person ist, falls das Gesetz Vertraulichkeit vorschreibt, falls die Nutzung intern innerhalb eines Büros stattfindet oder falls es ein überwiegendes öffentliches oder privates Interesse gibt – sind in Artikel 22 des Datenschutzgesetzes geregelt. Sie sind im Allgemeinen mit den gemäß der Richtlinie zulässigen Ausnahmen vereinbar.

Der Grundsatz der Sicherheit verlangt, dass der für die Verarbeitung Verantwortliche geeignete technische und organisatorische Sicherheitsmaßnahmen für die Risiken der Verarbeitung zu treffen hat. Alle unter der Verantwortung der für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Auftragsverarbeiter, dürfen Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

Die Absätze 2 bis 5 des Artikels 31 Datenschutzgesetz beziehen sich auf die Sicherheit. Personen und Unternehmen, die für einen für die Verarbeitung Verantwortlichen oder für einen Auftragsverarbeiter Arbeiten durchführen und Zugang zu Daten haben, dürfen diese Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten. Die Verarbeitung ist in diesem Fall gemäß einer schriftlichen Vereinbarung zwischen den Partnern durchzuführen; Die Vereinbarung selbst muss die vorgenannte Klausel enthalten. Bei der Anwendung geeigneter technischer und organisatorischer Sicherheitsmaßnahmen haben der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter sicherzustellen, dass die Verarbeitung personenbezogener Daten mit den Bestimmungen des Datenschutzgesetzes hinsichtlich der Zuverlässigkeit sowie der persönlichen Freiheit und der Auskunft übereinstimmt; Außerdem haben sie geeignete technische und organisatorische Sicherheitsmaßnahmen durchzuführen, die für den Schutz personenbezogener Daten gegen zufällige oder unrechtmäßige Zerstörung, Verlust oder die Änderung, die unberechtigte Weitergabe, Missbrauch oder eine andere in Unvereinbarkeit mit den Bestimmungen des Datenschutzgesetzes durchgeführte Verarbeitung erforderlich sind. Urkundliche Belege für die organisatorischen Sicherheitsmaßnahmen sind dem Arbeitgeber des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters sowie der Datenschutzbehörde zugänglich zu machen. Die Weisungen des für die Verarbeitung Verantwortlichen dürfen die journalistische Freiheit nicht einschränken und die Schaffung eines künstlerischen oder literarischen Werks nicht behindern.

Die Vorschriften des färöischen Rechts hinsichtlich der technischen und organisatorischen Sicherheitsmaßnahmen stimmen mit diesem Grundsatz überein.

Das Recht auf Auskunft, Berichtigung und Widerspruch verlangt, dass die betroffene Person das Recht hat, eine Kopie aller sie betreffenden Daten zu erhalten, die verarbeitet werden, sowie das Recht auf Berichtigung dieser Daten, wenn diese sich als unrichtig erweisen. In bestimmten Situationen muss sie auch Widerspruch gegen die Verarbeitung der sie betreffenden Daten einlegen können. Die einzigen Ausnahmen von diesen Rechten sind die in Artikel 13 der Richtlinie genannten Ausnahmen.

Was das Recht auf Auskunft anbetrifft, so muss gemäß Artikel 19 des Datenschutzgesetzes der für die Verarbeitung Verantwortliche die betroffene Person auf Verlangen über Folgendes Auskunft geben: Name und Anschrift des für die Verarbeitung Verantwortlichen und seiner Vertreter, den Namen der Untergebenen des für die Verarbeitung Verantwortlichen, Art und Zweckbestimmung sämtlicher Verarbeitungen, die Art der verarbeiteten Daten, die Herkunft der Daten, ob die Daten an jemanden weitergegeben wurden und, falls zutreffend, an wen. Außerdem muss er darüber informieren, welche Sicherheitsmaßnahmen angewandt werden, solange diese Auskunft die Sicherheit selbst nicht beeinträchtigt. In dieser Hinsicht entspricht das färöische Recht wohl den Anforderungen von WP 12.

Die in den Absätzen 1, 3 und 4 des Artikels 22 Datenschutzgesetz enthaltenen Ausnahmen dürften mit den gemäß Artikel 13 der Richtlinie zulässigen Ausnahmen übereinstimmen. Fraglich könnte sein, ob die Ausnahme hinsichtlich von Daten, die nur innerhalb eines Büros genutzt und nicht an andere Personen weitergeben werden, mit diesem Artikel der Richtlinie im Einklang steht. Für diesen Fall scheinen die Auskunftsregelungen nicht zu gelten. Falls Daten nur innerhalb eines Büros verwendet und nicht an andere Personen weitergeben werden, entfällt dadurch das Recht auf Auskunft.

Die Färöer haben die Artikel-29-Datenschutzgruppe darüber informiert, dass die ursprüngliche Übersetzung von Artikel 22 Absatz 1 Nummer 5 des färöischen Datenschutzgesetzes fehlerhaft ist. Die Übersetzung hätte wie folgt lauten müssen: „die nur in Texten zu finden sind, die für interne, vorbereitende Zwecke erstellt und nicht an andere Personen weitergegeben wurden“[11].

Die Färöer haben die Artikel-29-Datenschutzgruppe weiter darüber informiert, dass diese Ausnahme im Zusammenhang mit dem färöischen Gesetz über die Auskunft über Dokumente in Verwaltungsakten bewertet werden muss, auf das das färöische Gesetz über die Verarbeitung personenbezogener Daten Bezug nimmt. Das Gesetz über die Auskunft über Dokumente in Verwaltungsakten legt unter anderem fest, dass für interne Dokumente eine Ausnahme hinsichtlich der Auskunftsregelungen gilt. Es ist aber trotzdem möglich, Auskunft über die tatsächlich in diesen Dokumenten enthaltenen Informationen zu erhalten. Diese Regelung ähnelt den Regelungen für interne Dokumente, die im dänischen Gesetz über die Auskunft über staatliche Urkunden enthalten sind.

[11] Anm. d. Übers.: Freie Übersetzung aus der englischen Sprache.

Die Färöer haben die Artikel-29-Datenschutzgruppe schließlich darüber informiert, dass die in Artikel 22 Absatz 1 Nummer 5 genannte Ausnahme direkt aus dem norwegischen Gesetz über die Verarbeitung personenbezogener Daten übernommen wurde.

Unter Berücksichtigung dieser zusätzlichen, von den Färöern hinsichtlich des Wortlauts und dessen Auslegung zur Verfügung gestellten Informationen, dürfte die Ausnahme in Hinsicht auf das Recht, über interne Dokumente Auskunft zu erhalten, keine ernstliche Einschränkung des Auskunftsanspruchs darstellen.

Was das Recht auf Berichtigung anbelangt, so verpflichtet Artikel 27 des Datenschutzgesetzes den für die Verarbeitung Verantwortlichen, von Amts wegen oder auf Antrag der betroffenen Person personenbezogene Daten zu berichtigen, zu löschen oder zu sperren sowie einen Dritten, an den personenbezogene Daten weitergegeben wurden, über diese Tatsache zu benachrichtigen. Insoweit erfüllt das Datenschutzgesetz die Anforderungen in WP 12, dass die betroffene Person in der Lage sein muss, eine Berichtigung nichtzutreffender Daten zu erwirken.

Das Widerspruchsrecht wird in Artikel 26 des Datenschutzgesetzes behandelt. Dort ist vorgesehen, dass die betroffene Person jederzeit der Verarbeitung von sie betreffenden Daten widersprechen kann und dass, falls einem solchen Widerspruch anschließend stattgegeben wird, die Verarbeitung nur ohne die entsprechenden Daten durchgeführt werden darf. Diese Bestimmung gewährt der betroffenen Person weitergehende Rechte als dies in WP 12 vorgesehen ist. Dort ist festgelegt, dass es „unter gewissen Voraussetzungen“[12] ein Widerspruchsrecht geben sollte.

Die Beschränkung der Weiterübermittlung in andere Drittländer verlangt, dass weitere Übermittlungen personenbezogener Daten vom ursprünglichen Bestimmungsdrittland in ein anderes Drittland lediglich zulässig sind, wenn das zweite Drittland (d.h. der Empfänger der Weiterübermittlung) ebenfalls ein angemessenes Schutzniveau aufweist. Die einzigen zulässigen Ausnahmen müssen mit Artikel 26 Absatz 1 der Richtlinie übereinstimmen.

Gemäß Artikel 16 des Datenschutzgesetzes ist eine Übermittlung von Daten ins Ausland nur zulässig, falls das fragliche fremde Land ein angemessenes Schutzniveau gewährleistet und die Übermittlung von der Datenschutzbehörde genehmigt wurde. Die Angemessenheit des von einem fremden Land gebotenen Schutzniveaus ist unter Berücksichtigung aller Umstände zu beurteilen, die bei einer Datenübermittlung eine Rolle spielen; insbesondere sind die Zweckbestimmung und Dauer der Verarbeitung, die Art der Daten, die in dem betreffenden fremden Land geltenden Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen zu berücksichtigen.

Für die Übermittlung personenbezogener Daten ins Ausland muss eine Genehmigung der Datenschutzbehörde vorliegen.[13] Der Justizminister kann jedoch – auf Empfehlung der Datenschutzbehörde – festlegen, dass Daten in bestimmte Länder

[12] Anm. d. Übers.: Freie Übersetzung aus der englischen Sprache („in certain circumstances“). Vgl. Richtlinie 95/46/EG, Erwägungsgrund 25.

[13] Artikel 16 Absatz 1 Datenschutzgesetz.

ohne Genehmigung der Datenschutzbehörde übermittelt werden dürfen.[14] Diese Bestimmungen sind in der Ministerialverordnung Nr. 33 enthalten, die vorsieht, dass personenbezogene Daten in die Mitgliedstaaten der EU, nach Island, Norwegen, in die Schweiz, nach Argentinien, Guernsey sowie Isle of Man ohne Genehmigung der Datenschutzbehörde übermittelt werden dürfen.[15] Die Übermittlung personenbezogener Daten ins Ausland dürfte deshalb eine Beurteilung voraussetzen, die der gemäß EU-Recht durchgeführten Beurteilung ähnelt.[16] Die Beurteilung wird von der Datenschutzbehörde durchgeführt.

Die Vorschriften des Datenschutzgesetzes über die Übermittlung personenbezogener Daten dürften den Kriterien von WP 12 entsprechen. Die Ausnahmen[17] beschränken sich auf die gemäß Artikel 26 der Richtlinie genehmigten Ausnahmen.

Weitere Grundsätze, die auf spezifische Arten der Verarbeitung anwendbar sind:

Sensible Daten - Sind „sensible" Kategorien von Daten betroffen (die in Artikel 8 der Richtlinie aufgeführt sind), so haben zusätzliche Garantien wie das Erfordernis zu gelten, dass die betroffene Person ausdrücklich in die Verarbeitung einwilligt. Die Definition sensibler Daten im Datenschutzgesetz[18] entspricht Artikel 8.

Das Datenschutzgesetz schreibt vor, unter welchen Bedingungen sensible Daten verarbeitet werden dürfen. WP 12 verlangt, dass für die Verarbeitung sensibler personenbezogener Daten zusätzliche Sicherheitsmaßnahmen mit einem besonderen Verweis auf die ausdrückliche Einwilligung der betroffenen Person getroffen werden. In Artikel 10 des Datenschutzgesetzes ist aufgeführt, welche Bedingungen bei der Verarbeitung sensibler personenbezogener Daten erfüllt sein müssen.

Direktmarketing - Werden Daten zum Zwecke des Direktmarketings übermittelt, so muss die betroffene Person die Möglichkeit haben, sich jederzeit gegen die Verwendung ihrer Daten für derartige Zwecke zu entscheiden.

Gemäß dem Datenschutzgesetz setzt die Übermittlung von Daten zum Zweck der kommerziellen Werbung voraus, dass sich die betroffene Person für die Verwendung ihrer Daten entscheidet. Die Weitergabe von einen Verbraucher betreffenden Daten an Dritte zum Zweck der kommerziellen Werbung bzw. die Nutzung solcher Daten im Auftrag von Dritten zum Zweck der kommerziellen Werbung setzt die ausdrückliche Zustimmung der betroffenen Person voraus[19]. Diese Zustimmung kann jederzeit widerrufen werden.[20] Die betroffene Person hat das Recht, der Verarbeitung der sie betreffenden Daten zu widersprechen.[21] Ist der Widerspruch gerechtfertigt,[22] so bedeutet dies, dass die betroffene Person sich gegen die Verwendung der Daten zum Zweck der kommerziellen Werbung entscheiden kann. Dieses Widerspruchsrecht kann jederzeit ausgeübt werden.[23]

---

14 Artikel 16 Absatz 2 Datenschutzgesetz.
15 Ministerialverordnung Nr. 33 vom 11.4.2005 über die Übermittlung personenbezogener Daten in andere Länder ohne Genehmigung der Datenschutzbehörde, Artikel 1 Absatz 1.
16 Das färöische Datenschutzgesetz weicht jedoch etwas von Artikel 25 der Richtlinie 95/46/EG ab.
17 Artikel 17 Datenschutzgesetz.
18 Artikel 2 Absatz 9 Datenschutzgesetz.
19 Artikel 9 Absatz 3 Datenschutzgesetz.
20 Artikel 29 Datenschutzgesetz.
21 Artikel 26 Absatz 1 Datenschutzgesetz.
22 Artikel 26 Absatz 2 Datenschutzgesetz.
23 Artikel 26 Absatz 1 Datenschutzgesetz.

Das gemäß dem Datenschutzgesetz bestehende Schutzniveau hinsichtlich des Direktmarketings entspricht deshalb WP 12.

Automatisierte Einzelentscheidung - Erfolgt die Übermittlung mit dem Ziel, eine automatisierte Entscheidung im Sinne von Artikel 15 der Richtlinie zu treffen, so muss die natürliche Person das Recht haben, die dieser Entscheidung zugrunde liegende Logik zu erfahren, und andere Maßnahmen müssen getroffen werden, um die berechtigten Interessen der Person zu schützen.

Die Färöer haben die Artikel-29-Datenschutzgruppe darüber informiert, dass das färöische Datenschutzgesetz derzeit keine spezifische Bestimmung in Hinsicht auf automatisierte Entscheidungen enthält.

Die Färöer haben festgestellt, dass eine betroffene Person gemäß anderen Bestimmungen des Datenschutzgesetzes, beispielsweise durch das Auskunfts-, Informations- und Widerspruchsrecht, geschützt wird.

Was die Entscheidungen öffentlicher Stellen anbelangt, so wird eine betroffene Person zusätzlich durch das Verwaltungs- und das Auskunftsrecht geschützt. Gemäß auf den Färöern geltenden ungeschriebenen Verwaltungsregeln müssen öffentliche Stellen jeden Fall einzeln beurteilen; sie können deshalb keine automatisierten Entscheidungen verwenden.

2.2. Verfahrensrechtlicher Mechanismus/Durchsetzungsmechanismus

Nach den WP-12-Grundsätzen sind als Grundlage für die Beurteilung der Angemessenheit des Rechtssystems eines Drittlandes zunächst die Ziele des zugrunde liegenden verfahrensrechtlichen Systems für den Datenschutz zu bestimmen. Darauf aufbauend ist das Spektrum der verschiedenen in diesem Land bestehenden gerichtlichen und außergerichtlichen Verfahrensmechanismen zu bewerten.

Ziel eines Datenschutzsystems ist es, dafür zu sorgen, dass die Datenschutzvorschriften eingehalten werden, betroffene Personen Unterstützung und Hilfe bei der Wahrnehmung ihrer Rechte erhalten und bei einem Verstoß gegen die Bestimmungen angemessen entschädigt werden.

Gewährleistung einer guten Befolgungsrate der Vorschriften bedeutet, dass sich die für die Verarbeitung Verantwortlichen ihrer Pflichten deutlich bewusst sind und dass die betroffenen Personen ihre Rechte und die Mittel zu deren Wahrnehmung gut kennen. Wirksame, abschreckende Sanktionen können erheblich dazu beitragen, dass die Bestimmungen eingehalten werden; gleiches gilt natürlich für Systeme, die eine direkte Überprüfung durch Behörden, Buchprüfer oder unabhängige Datenschutzbeauftragte ermöglichen.

Die Gruppe stellt fest, dass das färöische Recht eine Reihe von Maßnahmen vorsieht, die diesem Ziel dienen.

(a) Datenschutzbeauftragter

Das färöische Recht sieht eine Datenschutzbehörde vor.[24]

Die Datenschutzbehörde besteht aus einem Verwaltungsrat und einem Sekretariat und ist für die Kontrolle sämtlicher vom Datenschutzgesetz abgedeckten Verarbeitungen zuständig. Die Behörde handelt bei der Erfüllung der ihr zugewiesenen Aufgaben komplett unabhängig.
Dies bedeutet, dass die Regierung der Datenschutzbehörde keinerlei Anordnungen oder Weisungen erteilen kann. Die von der Datenschutzbehörde getroffenen Entscheidungen sind endgültig. Gegen sie kann weder beim Justizministerium noch bei einer anderen Verwaltungsbehörde Beschwerde eingelegt werden.

Die Mitglieder des Verwaltungsrats werden vom Justizminister für eine Amtszeit von 4 Jahren ernannt. Die Verwaltungsratsmitglieder können in der Regel nicht entlassen werden. Mitglieder können jedoch in Ausnahmefällen vom Minister entlassen werden, beispielsweise bei finanziellem Betrug. Die Mitglieder arbeiten außerdem gemäß den Regeln der „Handlungskompetenz“, welche gewährleisten, dass die vom Verwaltungsrat getroffenen Entscheidungen unabhängig sind.

Die Datenschutzbehörde wird aus dem färöischen Haushalt finanziert, welcher vom färöischen Parlament beschlossen wird. Die Datenschutzbehörde fällt unter das dem Justizminister vom Parlament bewilligte Budget. Sobald das Parlament entschieden hat, erhält die Datenschutzbehörde die Verfügungsgewalt über die bewilligten Mittel.

Berücksichtigt man die oben genannten Garantien, sollten keinerlei Zweifel mehr darüber bestehen, dass die erforderlichen Voraussetzungen zu Gewährleistung einer vollständigen Unabhängigkeit der Datenschutzbehörde gegeben sind.

Abschließend sollte noch erwähnt werden, dass die färöische Datenschutzbehörde in genau derselben Weise organisiert ist wie die dänische Datenschutzbehörde.

Die Datenschutzbehörde gewährleistet entweder auf eigene Initiative oder auf die Beschwerde einer betroffenen Person hin, dass Daten in Übereinstimmung mit dem Datenschutzgesetz verarbeit werden. Sie bearbeitet Meldungen und Anträge auf Genehmigung, führt ein öffentliches Register sämtlicher Meldungen und Genehmigungen, erstellt Gutachten im Zusammenhang mit gesetzgeberischen Vorschlägen, überwacht die Verarbeitung personenbezogener Daten, bietet gegebenenfalls dem privaten und öffentlichen Sektor Orientierung, gewährleistet eine gute Praxis, beobachtet Entwicklungen hinsichtlich der Verarbeitung personenbezogener Daten im eigenen Land sowie in Drittländern und stellt Informationen über diese Entwicklungen bereit.

Die Datenschutzbehörde kann einen für die Verarbeitung Verantwortlichen anweisen, eine unzulässige Verarbeitung einzustellen und bestimmte Daten, die derart verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Sie kann einem für die Verarbeitung Verantwortlichen die Nutzung bestimmter Verfahren untersagen, falls das Risiko besteht, dass Daten unter Verstoß gegen das Datenschutzgesetz verarbeitet

[24] Artikel 36 Datenschutzgesetz.

werden. Sie kann einen für die Verarbeitung Verantwortlichen anweisen, bestimmte technische und organisatorische Sicherheitsmaßnahmen durchzuführen, um Daten, die nicht verarbeitet werden dürfen, gegen Verarbeitung zu schützen bzw. um Daten gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die Änderung, die Weitergabe an unberechtigte Personen, den Missbrauch oder gegen jede andere unrechtmäßige Form der Verarbeitung zu schützen. In besonderen Fällen kann die Datenschutzbehörde gegen einen Datenverarbeiter eine einstweilige Verfügung erlassen.

Die Mitglieder und das Personal der Datenschutzbehörde haben jederzeit, auch ohne gerichtliche Verfügung, Zugang zu allen Räumlichkeiten, von denen aus verarbeitete Daten verwaltet werden oder auf zu verarbeitende Daten zugegriffen werden kann, sowie zu allen Räumlichkeiten, in denen Daten oder technische Ausrüstung aufbewahrt oder verwendet werden.

Diese Befugnisse entsprechen den Anforderungen an die Angemessenheit.

Die Jahresberichte umfassen sämtliche Aktivitäten der Datenschutzbehörde. Die Berichte sind öffentlich zugänglich und können über die Website der Datenschutzbehörde abgerufen werden.[25] Bis heute hat die Datenschutzbehörde drei Berichte veröffentlicht, und zwar für die Jahre 2002, 2003 und 2004.[26]

(b) Vorhandensein angemessener Durchsetzungsmöglichkeiten und Sanktionen

Um die Personen, die Verpflichtungen gemäß dem Datenschutzgesetz haben, zu einer guten Befolgungsrate der inhaltlichen Vorschriften zu bewegen, sieht das Datenschutzgesetz Sanktionen und Strafen für den Fall des Verstoßes gegen Vorschriften vor. Sollte jedoch gemäß anderen Rechtsvorschriften eine härtere Bestrafung vorgesehen sein, so bilden diese anderen Rechtsvorschriften die rechtliche Grundlage für die Verhängung von Sanktionen und Strafen.[27] Sanktionen und Strafen können nur von einem Gericht verhängt werden.[28]

Die Einhaltung sämtlicher wesentlicher Bestimmungen des Datenschutzgesetzes wird durch Sanktionen abgesichert. Diese Sanktionen sehen im Falle der Nichteinhaltung Geldstrafen bzw. Haft vor. Für entstandene Schäden in Hinsicht auf Sicherheitsmaßnahmen gemäß Artikel 31 ist eine Entschädigung vorgesehen. Die Haftung beschränkt sich nicht nur auf natürliche Personen, sondern kann sich auch auf juristische Personen erstrecken.

Unterstützung betroffener Personen bei der Wahrnehmung ihrer Rechte **bedeutet, dass der Einzelne seine Rechte rasch und wirksam ohne überhöhte Kosten durchsetzen können muss. Dafür muss es ein Verfahren geben, das eine unabhängige Überprüfung von Beschwerden ermöglicht.**

---

25 Artikel 41 Datenschutzgesetz.

26 Die Berichte befinden sich auf der Website der Datenschutzbehörde auf Färöisch. http://www.datueftirlitid.fo/index.asp?pID={6A552A7B-263D-4D06-B468-F966DDAD0A15}

27 Artikel 44 Absatz 1 Datenschutzgesetz.

28 Dänische Verfassung vom 5. Juni 1953, Artikel 3 und 63.

Die Rechte einer betroffenen Person sind in Kapitel 7 des Datenschutzgesetzes aufgeführt.[29] Artikel 30 regelt, wie eine betroffene Person ihre Rechte durchsetzen kann, und zwar geht dies mittels einer Beschwerde bei der Datenschutzbehörde. Alternativ dazu kann eine betroffene Person direkt vom allgemeinen Recht der Beschwerde beim Bezirksgericht Gebrauch machen.

Gegen eine von der Datenschutzbehörde getroffene Entscheidung kann weder beim Justizministerium noch bei einer anderen Verwaltungsbehörde Beschwerde eingelegt werden. Eine solche Beschwerde muss vor Gericht eingelegt werden.

Eine der Aufgaben der Datenschutzbehörde besteht darin, bei der Auslegung des Datenschutzgesetzes Unterstützung zu leisten. Die Datenschutzbehörde ist eine ansprechbare Institution, die Beschwerden von betroffenen Personen anhört und über behauptete Rechtsverletzungen des Datenschutzgesetzes entscheidet. Bürger können insbesondere verlangen, dass die Datenschutzbehörde eine Beurteilung erstellt. Dadurch erhält eine Person bei den zu behandelnden Fragestellungen institutionelle Unterstützung. Das Verfahren zur Erstellung einer Beurteilung ist ausführlich auf der Website der Datenschutzbehörde beschrieben und ist kostenlos.

Die Gewährleistung einer angemessenen Entschädigung bei Verstoß gegen das Datenschutzgesetz ist ein Schlüsselelement, das eine unabhängige Schieds- oder Schlichtungsinstanz voraussetzt, das die Zahlung von Entschädigungen oder auch die Auferlegung von Sanktionen ermöglicht.

Gemäß Artikel 46 des Datenschutzgesetzes muss der für die Verarbeitung Verantwortliche sämtliche Schäden entschädigen, die bei einer unter Verstoß gegen die Bestimmungen des Datenschutzgesetzes durchgeführten Verarbeitung personenbezogener Daten entstanden sind, es sei denn, es wird nachgewiesen, dass ein solcher Schaden nicht durch die bei der Verarbeitung personenbezogener Daten erforderliche Sorgfalt und Umsicht hätte abgewendet werden können.

Artikel 44 und 45 erlegen bei einem Verstoß gegen das Datenschutzgesetz Sanktionen auf, die aus Geldstrafen bzw. Haft bestehen. Personen, die geschäftlich tätig sind, kann das Recht auf geschäftliche Betätigung entzogen werden, falls sie wegen eines Vergehens gemäß dem Datenschutzgesetz verurteilt werden.

Die Gruppe ist der Auffassung, dass das färöische Recht eine angemessene Entschädigung für Personen gewährleistet, die durch eine Verletzung der Datenschutzbestimmungen geschädigt wurden.

3. ERGEBNIS

Wenn auch das färöische Recht nicht sämtliche Anforderungen erfüllt, die die Datenschutzrichtlinie den Mitgliedstaaten auferlegt, ist sich die Gruppe doch bewusst, dass unter Angemessenheit nicht eine vollständige Übereinstimmung mit dem von der Richtlinie festgelegten Schutzniveau zu verstehen ist.

[29] Artikel 26 bis 30 Datenschutzgesetz.

Ausgehend von den obigen Feststellungen und den von den Färöern zur Verfügung gestellten zusätzlichen Informationen kommt die Gruppe daher zu dem Schluss, dass die Färöer ein angemessenes Schutzniveau im Sinne von Artikel 25 Absatz 6 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr gewährleistet.

Brüssel, den 9. Oktober 2007

Für die Datenschutzgruppe
Der Vorsitzende
Peter SCHAAR