Richtlinie zum Einsatz von Arbeitsplatzcomputern in der Diözese Osnabrück

Kirchliches Amtsblatt für die Diözese Osnabrück, Band 50, Nr. 7, Art. 81, Seite 68
Kirchliches Amtsblatt für die Erzdiözese Hamburg vom 15.12.1995, Art. 153, Seite 140

1.0 Aufgabe und Ziel

Diese Richtlinie regelt den Einsatz von Arbeitsplatzcomputern im Generalvikariat, den sonstigen diözesanen Dienststellen, den Pfarrämtern, Kirchengemeindeverbänden und Kirchenstiftungen und den sonstigen, der kirchlichen Aufsicht unterliegenden Einrichtungen in den Bistümern Hildesheim, Osnabrück sowie im oldenburgischen Teil des Bistums Münster und im Bischöflichen Amt Schwerin. Sie ist als Ergänzung zur Anordnung über den Kirchlichen Datenschutz (KDO) und den zu ihr ergangenen bereichsspezifischen Datenschutzregelungen in ihren jeweils geltenden Fassungen anzusehen.

2.0 Arbeitsplatzcomputer

2.1 Begriffsbestimmung

Arbeitsplatzcomputer (APC) im Sinne dieser Richtlinie sind alle selbständigen Systeme der Informationstechnik, die einem Mitarbeiter zur Erfüllung seiner dienstlichen Aufgaben an seinem Arbeitsplatz zur Verfügung gestellt werden. Sie können als Einzelgerät (Stand-Alone-PC) oder in Verbindung mit anderen APC (Netzwerken) oder in Verbindung mit Anlagen der mittleren Datentechnik und Großcomputern (PC/Host-Koppelung) installiert sein.

2.2 Gefahren durch den Einsatz von Arbeitsplatzcomputern

Arbeitsplatzcomputer verfügen über eine im Wesentlichen einheitliche Systemarchitektur sowie international genormte und standardisierte Bauteile und Schnittstellen. Ihre Betriebssysteme haben als Standardsoftware eine sehr weite Verbreitung. Es handelt sich bei ihnen daher um so genannte "offene Systeme", die jederzeit einen Anschluss weiterer APC ermöglichen und heute praktisch von jedermann bedient werden können. Zum Schutz des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die auf ihnen gespeicherten personenbezogenen Daten durch besondere Vorkehrungen vor unberechtigtem Zugriff sowie vor unberechtigter Verarbeitung und Nutzung zu schützen.

3.0 Allgemeine Grundsätze

3.1 Verantwortlichkeit der Mitarbeiter

Jeder Mitarbeiter trägt die datenschutzrechtliche Verantwortung für eine vorschriftsgemäße Ausübung seiner Tätigkeit. Es ist ihm untersagt, personenbezogene Daten zu einem anderen, als in der jeweils rechtmäßigen Aufgabenerfüllung liegenden Zweck, zu verarbeiten oder zu offenbaren.

3.2 Verantwortlichkeit der Dienststellenleiter

Die Leiter der jeweiligen Dienststellen und Einrichtungen tragen die Verantwortung für eine den Grundsätzen des Datenschutzes entsprechende Ausstattung der Arbeitsplatzcomputer. Bei der Neuanschaffung von APC müssen daher Konzepte zur datenschutzgerechten Ausgestaltung der Arbeitsplätze in die Investitionsentscheidung miteinbezogen werden.

3.3 Technische und organisatorische Maßnahmen

Mit der Eingabe, Speicherung, Verarbeitung und Nutzung personenbezogener Daten auf Anlagen der elektronischen Datenverarbeitung darf erst begonnen werden, wenn die Daten verarbeitende Stelle die nach der Anlage zu § 6 KDO und die nach dieser Richtlinie erforderlichen technischen und organisatorischen Maßnahmen zum Schutz dieser Daten getroffen hat.

3.4 Mindestanforderungen

Unabhängig vom Grad der Schutzbedürftigkeit der Daten sind dabei zumindest folgende Maßnahmen zu treffen:

— Die Datenverarbeitungsanlage ist unter Verwendung des hierzu erlassenen Musterformulars beim zuständigen Bischöflichen Beauftragten für den Datenschutz zum Register der automatisch betriebenen Dateien (§ 17 Abs. 3 KDO) anzumelden.

— Alle bei der Verarbeitung personenbezogener Daten tätigen hauptamtlichen und ehrenamtlichen Mitarbeiter haben die Verpflichtungserklärung gemäß § 4 Abs. 2 Satz 1 KDO abzugeben. Eine Durchschrift hiervon ist dem Bischöflichen Beauftragten für den Datenschutz zuzuleiten. Den Mitarbeitern, die die Verpflichtungserklärung unterschrieben haben, ist ein Abdruck der jeweils gültigen Anordnung über den Kirchlichen Datenschutz und der in ihrem Arbeitsbereich zu beachtenden bereichsspezifischen Datenschutzregelungen (Schulen, Krankenhäuser, Friedhöfe etc.) auszuhändigen.

— Der Kreis der Nutzungsberechtigten ist schriftlich festzulegen.

— Bei Einrichtungen und Organisationen, die ständig mehr als fünf Arbeitnehmer mit der automatischen Verarbeitung personenbezogener Daten beschäftigen, soll ein Betriebsbeauftragter für den Datenschutz bestellt und dem Bischöflichen Beauftragten für den Datenschutz mit der Meldung zum Datenschutzregister benannt werden.

— Es ist sicherzustellen, daß auf dienstlich genutzten Anlagen der elektronischen Datenverarbeitung ausschließlich autorisierte Programme, zu dienstlichen Zwecken verwendet werden. Die Benutzung privater Programme ist unzulässig.

3.5 Wahrung fremder Urheberrechte

Auf Arbeitsplatzcomputern dürfen nur Originalversionen von Softwareprogrammen im Rahmen der Lizenzbedingungen des Herstellers eingesetzt werden. Die Anfertigung von Programmkopien zum Zwecke der Weitergabe an andere Dienststellen und Einrichtungen sowie zum Einsatz auf privaten PC ist aus urheberrechtlichen und strafrechtlichen Gründen strengstens untersagt (Raubkopieren). Die Stelle, die die Originalversion erworben hat, hat diese beim Hersteller ordnungsgemäß registrieren zu lassen.

3.6 Einsatz von Shareware und Public-Domain-Programmen

Die im Handel erhältlichen Shareware und Public-Domain-Programme sind keine Originalprogramme sondern Kopien der Originalversionen. Durch die häufigen Kopiervorgänge mit meist ungeprüften Disketten ist die Gefahr vor Virenbefall hier besonders groß. Darüber hinaus sind solche Programme oft unzureichend dokumentiert und ihre Kompatibilität mit anderen Programmen zweifelhaft. Aus diesen Gründen soll grundsätzlich auf den Einsatz solcher Programme verzichtet werden. Lässt sich ihr Einsatz im Einzelfall nicht vermeiden, so sind die Programme vor der Installation mit einem Viren-Scanner auf Virenbefall zu untersuchen. Ein dauerhafter Einsatz macht zudem eine Registrierung beim Hersteller erforderlich.

3.7 Weitere Maßnahmen

Die Notwendigkeit, weitere Schutzmaßnahmen durchzuführen, richtet sich nach dem Grade der Schutzbedürftigkeit der gespeicherten personenbezogenen Daten. Liegen besondere Gefahrenlagen vor, sind in der Regel weitere Maßnahmen nach Ziffer 6 erforderlich.

4.0 Datenschutzklassen

4.1 Datenschutzklasse I

Zur Datenschutzklasse I gehören Daten, deren Missbrauch keine besondere Beeinträchtigung des Betroffenen erwarten lässt. Hierzu gehören Adressangaben, Berufs-, Branchen- oder Geschäftsbezeichnungen. Für sie sind die unter Ziffer 5.1 festgelegten Maßnahmen durchzuführen.

4.2 Datenschutzklasse II

Zur Datenschutzklasse II gehören Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann. Hierzu gehören Daten über Mietverhältnisse, Geschäftsbeziehungen sowie Geburts- und Jubiläumsdaten, etc.. Für sie sind die unter Ziffer 5.2 festgelegten Maßnahmen durchzuführen.

4.3 Datenschutzklasse III

Zur Datenschutzklasse III gehören Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann. Hierzu gehören Daten über kirchliche Amtshandlungen, gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen, die Mitgliedschaft in einer Religionsgesellschaft, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen, etc.. Für sie sind die unter Ziffer 5.3 festgelegten Maßnahmen durchzuführen.

4.4 Nicht zu speichernde Daten

Daten, deren Kenntnis dem Beicht- oder Seelsorgegeheimnis unterliegen sowie Daten über die Annahme einer Person an Kindes Statt (Adoptionsgeheimnis), sind in besonders hohem Maße schutzbedürftig. Ihre Ausspähung würde dem Vertrauen in die Verschwiegenheit katholischer Dienststellen und Einrichtungen schweren Schaden zufügen. Daher dürfen diese Daten nicht auf Arbeitsplatzcomputern verarbeitet werden.

4.5 Einordnung in die Datenschutzklassen

Bei der Einordnung der zu speichernden personenbezogenen Daten in die vorgenannten Schutzklassen ist auch deren Zusammenhang mit anderen gespeicherten Daten, der Zweck ihrer Verarbeitung und das anzunehmende Missbrauchsinteresse zu berücksichtigen.

4.6 Geltung der jeweils höchsten Schutzklasse

Gehören die auf einem Arbeitsplatzcomputer gespeicherten Daten unterschiedlichen Schutzklassen an, so richten sich die nach dieser Richtlinie zu treffenden Maßnahmen nach der höchsten, in der Datenverarbeitung vorkommenden Schutzklasse.

4.7 Vermeidung der Mehrfachsicherung

Schutzmaßnahmen nach den Datenschutzklassen II oder III machen die für die jeweils niedrigeren Schutzklassen vorgesehenen Maßnahmen gleicher Zielrichtung in der Regel entbehrlich.

5.0 Nach den Datenschutzklassen erforderliche Maßnahmen

5.1 Maßnahmen in Datenschutzklasse I

Zum Schutz der in die Datenschutzklasse I einzuordnenden Daten sind in der Regel folgende Maßnahmen erforderlich:

— Die Inbetriebnahme des APC ist nur nach Eingabe eines benutzerdefinierten Kennwortes möglich, das in regelmäßigen Abständen erneuert werden sollte. Das Laden des Betriebssystems kann nicht von einem der installierten Diskettenlaufwerke aus erfolgen (Boot-Schutz). Im Mehrbenutzer- oder Netzwerkbetrieb und bei einer PC/Host-Koppelung ist zudem eine Rechteverwaltung auf Unterverzeichnis- und Dateiebene erforderlich, wenn nicht alle Nutzer berechtigt sein sollen, auf die personenbezogenen Daten Zugriff zu nehmen.
— Sicherungskopien und Ausdrucke der Datenbestände sind verschlossen, im Interesse der Dienststelle möglichst in feuerfesten Stahlschränken aufzubewahren.
— Nicht mehr benötigte Dateien sind so zu löschen, dass ihre Wiederherstellung ausgeschlossen ist (physikalisches Löschen).

5.2 Maßnahmen in Datenschutzklasse II

Zum Schutz, der in die Datenschutzklasse II einzuordnenden Daten sind in der Regel folgende Maßnahmen erforderlich:

— Die auf der Festplatte gespeicherten Programme und Daten sollten dauerhaft so verschlüsselt werden, dass eine Entschlüsselung nur bezüglich solcher Programmteile und Daten stattfindet, die vom APC in den Hauptspeicher geladen werden (Online-Verschlüsselung). Der Zugang zum Entschlüsselungsprogramm ist nur nach Eingabe einer Benutzerkennung und eines Passwortes möglich, das vom Anwender in regelmäßigen Abständen zu erneuern ist. Dabei ist eine Begrenzung der Anmeldeversuche erforderlich. Das Hochfahren des APC vom Diskettenlaufwerk aus, ist auszuschließen.
— Anmeldeversuche am APC sind durch Einsatz geeigneter Programme zu protokollieren.
— bei Mehrbenutzer- und Netzwerkbetrieb ist eine abgestufte Rechteverwaltung für jeden Benutzer oder einzelne Benutzergruppen erforderlich. Der Zugang zum Betriebssystem sollte nur für den Systemverwalter möglich sein;
— Sicherungskopien sollten ebenfalls verschlüsselt und in abschließbaren, feuerfesten Schränken aufbewahrt werden; die Schnittstellen sind vor unberechtigtem Zugriff zu sichern.

5.3 Maßnahmen in Datenschutzklasse III

Zum Schutz, der in die Datenschutzklasse III einzuordnenden Daten sind in der Regel folgende Maßnahmen erforderlich:

— Die auf der Festplatte gespeicherten Programme und Daten sind dauerhaft zu verschlüsseln (Online-Verschlüsselung). Eine Entschlüsselung findet nur bezüglich solcher Programmteile und Daten statt, die vom APC in den Hauptspeicher geladen werden. Der Zu-

gang zum Entschlüsselungsprogramm ist nur nach Eingabe einer Benutzerkennung und eines zumindest achtstelligen Passwortes möglich, das vom Anwender in regelmäßigen Abständen zu erneuern ist. Trivialpasswörter (z.B. 4711, 12345, Gast, master) dürfen nicht verwendet werden. Dabei ist programmseitig eine Begrenzung der Anmeldeversuche auf höchstens drei Fehlversuche vorzusehen. Das Hochfahren des APC vom Diskettenlaufwerk aus, ist auszuschließen.

— im Mehrbenutzer- und Netzwerkbetrieb sind für jeden Benutzer abgestufte Rechte für den Zugriff auf Programme, Daten und Peripheriegeräte (insbes. Laufwerke, Schnittstellen) durch einen Systemverwalter zu vergeben; Systemaktivitäten sind durch eine hierfür geeignete Software zu protokollieren, deren Auswertung durch eine Person erfolgen sollte, die selbst nicht Systemverwalter ist.
— Sicherungskopien sind zu verschlüsseln und in verschlossenen, möglichst feuerfesten Stahlschränken aufzubewahren.

6.0 Maßnahmen für besondere Gefahrenlagen

Über die in den Ziffern 3, 4 und 5 genannten Anforderungen hinaus können im Einzelfall, bei Vorliegen besonderer Gefahrenlagen, weitere Maßnahmen erforderlich sein.

6.1 Virenschutz

Bei Einsatz von APC in öffentlichen Fernkommunikationsnetzen (Telefax, Teletex u.ä.) sowie beim Anschluss von APC an externe Datenbanken ist ein ausreichender Schutz vor Virenbefall zu installieren. Aus Kosten- und Sicherheitsgründen ist hierfür in der Regel eine Hardwareerweiterung erforderlich. Sollte diese Möglichkeit wegen des Fehlens freier Steckplätze auf dem APC nicht gegeben sein, kann ausnahmsweise ein Softwareprogramm eingesetzt werden (Viren-Scanner), das regelmäßig auf den neuesten Stand zu bringen ist.

6.2 Schutz von Fernkommunikationsanlagen

APC, die an Einrichtungen der Fernkommunikation angeschlossen sind und mit deren Hilfe Daten der Schutzklasse III übertragen werden können, sind auch gegen Ausspähung durch Abhören des Leitungsnetzes zu sichern. Hierzu stehen abschirmsichere Kabel zur Verfügung. Die Daten sind zudem in verschlüsselter Form zu übertragen. Das zur Entschlüsselung benötigte Passwort darf nicht auf dem gleichen Wege an den Empfänger übermittelt werden.

6.3 Fernwartung

Eine Fernwartung von APC durch betriebsfremde Firmen schafft besondere Gefahren hinsichtlich der Ausspähung von Daten. Sie darf daher nur erfolgen, wenn zuvor durch Rückruf bei dem Fremdunternehmen die Berechtigung zur Vornahme von Wartungsarbeiten geklärt worden ist. Die Standleitung ist anschließend durch den für das System verantwortlichen Mitarbeiter zu aktivieren. Der Ablauf der Wartungsarbeiten und der dabei übermittelten Daten ist möglichst durch eine geeignete Software automatisch zu protokollieren und durch den Leiter der Dienststelle zu kontrollieren.

6.4 Wartungsarbeiten in der Dienststelle

Bei der Durchführung von Wartungsarbeiten innerhalb der Dienststelle, ist in der Regel die ständige Anwesenheit des für das System verantwortlichen Mitarbeiters erforderlich. Dabei wird ein Zugriff auf Datenbestände durch den Wartungsdienst normalerweise nicht erforderlich sein. In diesen Fällen ist, je nach Datenschutzklasse durch Passwortschutz und/oder Verschlüsselung sicherzustellen, dass der Wartungsdienst in diese Bereiche keinen Einblick erhält. In den anderen Fällen ist mit besonderer Sorgfalt darauf zu achten und nach Möglichkeit auch technisch sicherzustellen, dass keine Kopien der Datenbestände gefertigt werden können. Muss dem Wartungsdienst bei Vornahme der Arbeiten ein Passwort mitgeteilt werden, ist dieses sofort nach deren Beendigung zu ändern.

6.5 Wartungsarbeiten außerhalb der Dienststelle

Die Durchführung von Wartungsarbeiten in den Räumen eines Fremdunternehmens kann nur in besonderen Ausnahmefällen gestattet werden. Die Gründe und die Art und Weise ihrer Durchführung sind schriftlich zu dokumentieren. Vor Herausgabe des APC ist dessen Festplatte zu verschlüsseln und eine Rechteverwaltung zu installieren, die der Werkstatt keine Zugriffsrechte auf sensible Datenbestände gestattet.

6.6 Sicherung der Integrität der Datenbestände

Bei dem Einsatz von Datenbankprogrammen entstehen besondere Gefahren, wenn verschiedene Dateien miteinander verknüpft werden. In diesen Fällen hat eine Änderung von Datensätzen innerhalb einer Datei nicht immer auch eine Änderung in der mit dieser verknüpften Datei zur Folge. Hierdurch können sich in Bezug auf die gleiche Person Datenbestände unterschiedlichen Inhaltes ergeben. Von den Mitarbeitern wird in diesen Fällen besondere Aufmerksamkeit verlangt, um eine gleichmäßige Änderung des Datenbestandes an allen Stellen zu gewährleisten. Daher ist bei der Neuanschaffung von Datenbanken solchen Softwareprodukten der Vorzug zu geben, die eine Änderung von Datensätzen nur dann zulassen, wenn gleichzeitig auch die mit diesen verknüpften Datensätze geändert werden (referentielle Integrität).

6.7 Verbot privater Datenverarbeitung

Unabhängig von der Einordnung der zu verarbeitenden Daten in die Datenschutzklassen der Ziffern 4.1, 4.2, und 4.3, ist eine private Erhebung, Verarbeitung und Nutzung dienstlicher Daten unzulässig.

6.8 Nutzung privater Datenverarbeitungssysteme zu dienstlichen Zwecken

Die Nutzung privater Datenverarbeitungssysteme, Datenträger und Programme zu dienstlichen Zwecken ist nur erlaubt, wenn dieses zur Erfüllung der dem Anwender obliegenden dienstlichen Aufgaben unabweislich oder zwingend geboten ist. Hierfür bedarf es der schriftlichen Genehmigung der speichernden Dienststelle. Die Genehmigung darf nur erteilt werden, wenn der Eigentümer der Datenverarbeitungsanlage folgende schriftliche Erklärung abgegeben hat:

"Ich verpflichte mich, bei der Verarbeitung personenbezogener Daten auf meinem privaten Datenverarbeitungssystem, bzw. auf einem Datenverarbeitungssystem in meinen Privaträumen die Anordnung über den Kirchlichen Datenschutz - KDO - nebst Durchführungsbestim-

mungen und die Richtlinie zum Einsatz von Arbeitsplatzcomputern in den Bistümern Hildesheim, Osnabrück, im oldenburgischen Teil des Bistums Münster und im Bischöflichen Amt Schwerin einzuhalten. Eine Ausfertigung der KDO und der Richtlinien ist mir heute übergeben worden. Gleichzeitig unterstelle ich mich der Aufsicht des Bischöflichen Beauftragten für den Datenschutz und übernehme die der speichernden Dienststelle obliegenden Verpflichtungen nach § 17 Abs. 2 KDO. Ich verpflichte mich weiter, der Dienstelle auf Anforderung die für die dienstlichen Zwecke verwendeten Datenträger sowie Ausdrucke aller gespeicherten Daten zur Verfügung zu stellen. Nach Beendigung der Zusammenarbeit werde ich nach Kräften an der Übertragung des Datenbestandes auf ein anderes dienstliches Datenverarbeitungssystem mitwirken. In diesem Falle werde ich auch alle dienstlich benötigten Datenträger und Ausdrucke an die Dienststelle herausgeben und dafür Sorge tragen, dass die Daten auf meiner Anlage vollständig so gelöscht werden, dass eine Wiederherstellung des Datenbestandes nicht mehr möglich ist."

Der genehmigte Antrag und die schriftliche Verpflichtungserklärung sind in drei Stücken auszufertigen, von denen eines bei der Dienststelle und eines bei dem Verpflichteten verbleibt. Die dritte Ausfertigung ist dem Bischöflichen Beauftragten für den Datenschutz zur Kenntnisnahme zuzuleiten.

7.0 Maßnahmen zur Datensicherung

Zum Schutz des Datenbestandes vor dessen Verlust sind regelmäßige Datensicherungen erforderlich.

7.1 Sicherungskopien der verwendeten Programme

Die mit dem APC angelegten Datenbestände sind in der Regel nur mit den eingesetzten Softwareprogrammen wieder lesbar zu machen. Die Datensicherung muss sich daher auch auf diese Programme erstrecken. Aus diesem Grunde sind vor Beginn der Verarbeitung Sicherungskopien der verwendeten Programme anzulegen und möglichst von den Originaldisketten der Programme und den übrigen Datenträgern getrennt aufzubewahren.

7.2 Zeitabstände bei der Datensicherung

Der aktuelle Datenbestand sollte mindestens einmal täglich, bei Ende der Arbeit mit dem Datenverarbeitungssystem gesichert werden. Darüber hinaus sollte monatlich einmal eine Sicherung der gesamten Festplatte durchgeführt werden.

Kann der Verlust von Daten den Betroffenen in seinen Rechten beeinträchtigen (z. B. Personaldaten, kirchl. Amtshandlungsdaten), so ist die Zahl der Datensicherungen auf angemessene Abstände zu erhöhen. In diesen Fällen sind auch Zweitkopien der jeweiligen Sicherungskopien anzufertigen.

Bei dem Neuerwerb von Programmen zur Verarbeitung personenbezogener Daten soll nach Möglichkeit solchen Programmen der Vorzug gegeben werden, die eine automatische Sicherung des Datenbestandes durchführen.

7.3 Ausdruck von Datenbeständen in Abwesenheit des zuständigen Mitarbeiters

Sollen umfangreiche Ausdrucke von personenbezogenen Daten aus organisatorischen Gründen während der Abwesenheit des hierfür zuständigen Mitarbeiters erfolgen, so ist in geeigneter Weise dafür Sorge zu tragen, dass andere Mitarbeiter sowie betriebsfremde Personen während der Zeit, in denen die Ausdrucke unbeaufsichtigt sind, keinen Zugang zu den Räumen haben, in denen sich der APC und der Drucker befinden.

7.4 Vernichtung von EDV-Ausdrucken und Datenträgern

EDV- Ausdrucke mit personenbezogenen Daten sind durch Zerreißgeräte oder durch andere geeignete Maßnahmen, die die Lesbarkeit oder Wiederherstellbarkeit ausschließen, zu vernichten. Datenträger (Disketten, Festplatten, Datenbänder, etc.), die nicht mehr benötigt werden, sind vor ihrer Beseitigung so zu löschen, bzw. zu behandeln, dass die Wiederherstellung, der auf ihnen gespeichert gewesenen Daten, ausgeschlossen ist. Dieses kann durch Neumagnetisierung der Datenträger, durch physikalisches Löschen der Dateien, Unterverzeichnisse und Verzeichnisse oder in anderer Weise geschehen.

8.0 Schlussbestimmungen

Diese Richtlinien sind von den Leitern der speichernden Stellen den hiervon betroffenen Mitarbeitern/innen auszuhändigen oder sonst in geeigneter Weise bekannt zu machen.

Diese Richtlinien treten am 1.8.1994 in Kraft.
Osnabrück, 27. Juli 1994