Prof. Dr. Friedrich von Zezschwitz
Hessischer Datenschutzbeauftragter

Arnoldshain, 9. November 2001

Datenschutz in der Justiz

I. Maßgebend für die datenschutzrechtlichen Pflichten ist das hessische Datenschutzgesetz, im Rahmen verfassungskonformer Eingrenzungen ergänzend das Grundrecht auf informationelle Selbstbestimmung. Das HDSG legt die folgenden Grundsätze für die Richterschaft fest:
   - Die materiell-rechtliche Geltung des HDSG für alle richterlichen Handlungen, einschließlich der Entscheidungsfindung und der vorausgehende Schritte (§ 3 I 1 HDSG).
   - Die Einrichtung eines – weisungsfreien - gerichtlichen Datenschutzbeauftragten zur gerichtsinternen Sicherstellung des Datenschutzes (§ 5 I HDSG). Ihm stehen allerdings keine Befugnisse zu, die die richterliche Unabhängigkeit einschränken können (Art. 97 I GG).
   - Die Beschränkung der Kontrollbefugnisse des HDSB auf Rechtsakte, die außerhalb richterlicher Unabhängigkeit liegen (§ 24 I 3 HDSG).

II. Divergenzen gegenüber den allgemeinen datenschutzrechtlichen Pflichten der Exekutive ergeben sich für Richter vor allem aus:
   - der institutionellen Garantie richterlicher Unabhängigkeit,
   - den verfahrensrechtlichen Regelungen der Prozessordnungen, insb. den dort begründeten Übermittlungs- und Benachrichtigungspflichten,
   - bundesrechtlichen Sondervorschriften der Strafprozessordnung und des Strafvollzugsgesetzes, des HGB (Handelsregister), der Insolvenzordnung (Veröffentlichung), des BGB (Vereins- und Güterrechtsregister).

III. Einzelne Problembereiche:
   1. Richterliche Tätigkeiten am PC oder im gerichtseigenen Netz (Serverbetrieb) erfolgen in *Dienstausübung* und unterstehen daher keinen grundrechtlichen Beschränkungen. Richterliche Unabhängigkeit stellt keine Individualrechtsgewährleistung dar, so dass keine persönöichen informationellen Abwehrrechte daraus herzuleiten sind. Die dienstlich bedingten *Zugriffsrechte* der einzelnen Richter sind vom Präsidium bzw. Vorsitzenden Richter des Spruchkörpers genau und vorab festzulegen. Sie sind durch informationstechnische Vorkehrungen (Passwort, Chipkarte, Biometrie) zu sichern. Eigenständige Zugriffsrechte der Geschäftsstellen, des Präsidenten/Direktors oder des Pressesprechers dürfen nicht vorgesehen werden, soweit richterliche Tätigkeiten von sonstigen ununterschieden gespeichert sind.
   2. Der richterliche Arbeitsplatz ist durch technische *Sicherheitsmaßnahmen gegen fremde Zugriffe* gesichert werden muss (§ 10 HDSG). *Passwortschutz* reicht keinesfalls aus. Bei Einzelarbeitsplätzen, die am gerichtlichen Netz hängen, ist eine Firewall zu installieren – nicht erst beim Übergang in öffentliche Netze. Erfahrungsgemäß stammen ca. 80% der unberechtigten Zugriffe von innen. - Der Rechtgrund für die Sicherheitsmaßnahmen liegt im Amtsgeheimnis (§ 203 StGB) und im Datengeheimnis (§ 9 HDSG). Ob Kenntnis Dritter über die richterliche Entscheidungsvorbereitung dessen Unabhängigkeit beeinträchtigt, ist fraglich; guter Praxis entspricht, die Parteien/Beteiligten über die maßgebenden Kriterien rechtzeitig in Kenntnis zusetzen. Betroffen ist stets das Vertrauen in das amtliche Stillschweigen. Die verfahrensrechtlichen Mitteilungspflichten legitimieren keine Zugriffe gegen den Willen des Richters.
   3. Da die Arbeit am PC oder Server „automatisierte" Datenverarbeitung (Definition: § 3 II BDSG, enger § 2 VI HDSG) darstellt, sind *Vorabkontrollen* durchzuführen und *Verfahrensverzeichnisse* zu erstellen (§§ 6, 7 VI HSDG). In die Verfahrensverzeichnisse kann jedermann einsehen; ausgenommen ist nur die Strafverfolgung (§ 6 II HDSG).
   4. *Zuständigkeitsübergreifende Zugriffe* (bspw. des leitenden Richters oder des Dienstherrn) auf den Arbeitsplatz sind unzulässig. Dahingehende Ermittlungsbefugnisse bestehen nur in Disziplinarverfahren oder zur Strafverfolgung (Rechtsbeugung, Bestechlichkeit). Nicht ausgeschlossen sind Zugriffe im Vertretungsfall, da der Vertreter den Richter uneingeschränkt ersetzt. Ist der Vorsitzende des Spruchkörpers Vertreter, so steht auch ihm das Zugriffsrecht zu.
   5. Die alltäglichen Fehler am PC (Abstürze, Programmmängel, Zugriffsverweigerung, Passwortirrtümer) zwingen zur Vorhaltung einer *professionellen Administration* der PC oder der Servers. Die Administration sollte weder durch staatliche Fernwartungsanbieter noch durch au-

ßenstehende Firmen erfolgen, da deren Verhalten im Netz nur schwer kontrollierbar ist (vgl. Mustervertrag Fernwartung). Durch Dienstanweisung müssen gerichtsinterne Administratoren auf unerlässliche Datenzugriffe beschränkt und zu besonderer Geheimhaltung verpflichtet werden.

6. Der Umfang elektronischer Kommunikation *innerhalb der Gerichte* hängt vom Willen der Teilnehmenden ab und stellt deswegen keine Gefahr für die richterliche Unabhängigkeit dar. Die Grenze liegt daher im Datenschutz: Soweit personenbezogene Daten Parteien/Beteiligte weitergegeben werden, handelt es sich um eine Übermittlung, die dem Zweckbindungsgebot nach § 13 I HDSG unterliegt. Sie darf nur ausnahmsweise durchbrochen werden (§§ 13 II, 12 II HDSG). Regelmäßig darf nur innerhalb des Spruchkörpers und des Instanzenzuges übermittelt werden. Eine „Beiziehung" zu anderen Verfahren muss über § 12 II HDSG legitimiert werden. - Wie der richterliche Arbeitsplatz technisch zu sichern ist, muss auch die Kommunikation unter Richtern und deren Hilfskräften sicher (verschlüsselt) ablaufen.
7. Elektronische Kommunikation *mit Parteien/Beteiligten* setzt deren ausdrückliche Zustimmung voraus. Sie wird durch die Angabe einer e-mail-Adresse nicht erteilt. Zugangsfragen werden derzeit beraten. Alle Datenschützer fordern, auch hier die 3-Tagesfrist gelten zu lassen. Die Kommunikation bedarf aus datenschutzrechtlichen Gründen der Verschlüsselung. Außerdem ist bei verfahrensbestimmenden Verfügungen und Entscheidungen mit elektronisch zertifizierter Signatur zu arbeiten. Einfacher ist allerdings die nachfolgende Versendung in Papierform.
8. *Speicherungen vor Verkündung* der Entscheidung berühren neben datenschutzrechtlichen Fragen auch die richterliche Unabhängigkeit. Eine Einsichtnahme durch Dritte erlaubt diesen, den Entscheidungsprozess nachzuvollziehen und ggfs. zu beeinflussen. Der Zugriff des Vertreters auf vorbereitende Überlegungen setzt die Einwilligung des eigentlich Zuständigen voraus, denn der Vertreter entscheidet aus eigener Beurteilung; im übrigen kann er zugreifen.
9. *Speicherungen nach Rechtskraft* der Entscheidung berühren nur noch Datenschutz. Grundsätzlich ist der Weg der Anonymisierung zu gehen. Die Wiederauffindung wird durch Schlagworte besser geleistet als durch Namen. Der Einwand zu hohen Arbeitsaufwands ist nicht begründet, da mit einfachen PC-Befehlen („Ersetzen") Namen getilgt und durch A,B,C ersetzt werden können. Ausdrucke auf Papier sind nach Anonymisierung zu erstellen – das gilt auch für die gerichtsinterne Information und Bibliothek. Die personenbezogenen Daten sind zu löschen, sobald feststeht, dass sie nicht mehr benötigt werden (§ 19 III HDSG). Sofern neben dem Urteilsausdruck auf Papier elektronische Dokumente mit Personenbezug aufbewahrt werden sollen, ist die Verwendung von Disketten oder CD-ROM vorzuziehen.
10. Eine *organisationsrechtlich begründete Auswertung* von Speicherungen in Einzel-PCs und Servern (bspw. durch das Präsidium) ist generell unzulässig, soweit die betreffenden Daten auf richterliche Tätigkeiten zurückgehen. Insoweit besteht hinsichtlich der Inhalte keine dienstaufsichtliche Zuständigkeit. Straftaten oder vermuteter Missbrauch des Internetzugangs dürfen nur disziplinarrechtlich verfolgt werden, nicht durch formlose Einsichtnahme. Im Straf- oder Disziplinarverfahren sind nur solche Zugriffe als „erforderlich" i.S.v. § 11 I HDSG anzusehen, mit denen Dienstvergehen bewiesen werden sollen, die sich aus dem Vorgang der Entscheidungsfindung herleiten oder aus anderen Dienst.
11. *Internet-Nutzung und e-mails* von PC oder Server erzeugen wiederkehrende Gefahren, da unberechtigte Zugriffe von außen nicht mit Sicherheit abgewehrt werden können (Firewall, IDS, biometrische Abschirmung). Zweckmäßig ist der Einsatz besonderer PCs, auf denen sich keine zu schützenden Daten befinden. Besondere Gefahren entstehen bei der Öffnung von „Anhängen" zu e-mails, da sie Schadprogramme enthalten können. Auch deswegen ist die Verwendung gesonderter PCs ohne Verbindung zum inneren Netz zu empfehlen.
12. *Private Mitnutzung* dienstlicher Internet-Anschlüsse führt zu kaum überwindbaren Telekommunikationsproblemen, denn die Dienststelle wird damit Diensteanbieter und darf nach TDDSG und TKG nur auf die Verbindungsdaten (zur Abrechnung und Funktionssicherung) zugreifen, die Inhalte hingegen nicht zur Kenntnis nehmen. Das aber ist für dienstliche e-mails unerlässlich (vgl. dazu 29. TB. 22.2.2 - Neufassung 11/2001).
13. Die *neu gefasste StPO (§§ 474 – 495)* enthält erstmals eigenständiges Datenschutzrecht für das Strafverfahren und ein länderübergreifendes Verfahrensregister. Es erfasst weit mehr Daten und ergänzt das BZRG. Außerdem werden die Übermittlungsbefugnisse zwischen StA und Polizei und die (gelockerte) Zweckbindung bei repressiven und präventiven Zwecken geregelt.