Pressepapier zur Vorstellung des XVII. Tätigkeitsberichts 2003 / 2004 des Landesbeauftragten für den Datenschutz Niedersachsen am 14. Januar 2005

Der Datenschutz in den Jahren 2003 und 2004

Der XVII. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Niedersachsen zeigt äußerlich und innerlich ein **neues „Gesicht**“: An Stelle der bisherigen detailreichen Schilderung von Einzelfällen werden in der Art einer „Management summary“ in stark komprimierter Form wichtige Entwicklungen des Datenschutzes und der technischer Datensicherheit sowie bedeutsame Ergebnisse der Kontroll- und Beratungstätigkeit des LfD dargestellt und kommentiert. Damit soll eine noch bessere Grundlage für eine sachgerechte Unterrichtung und für eine problembezogene Erörterung des Tätigkeitsberichtes, insbesondere im Landtag und in seinen Ausschüssen erreicht werden. Gleichzeitig soll das Informationsangebot zu Fragen des rechtlichen und technischen Datenschutzes auf der Internetseite des LfD verdichtet und durch neue Orientierungshilfen und Handlungsempfehlungen für Bürgerinnen und Bürger, Wirtschaft und Verwaltung noch besser nutzbar gemacht werden.

Die **Gesamtbilanz** der vergangenen beiden Jahre fällt **zwiespältig** aus:
Neben erfreulichen **Fortschritten**, etwa

- in der Verabschiedung einer eindeutigen und datenschutzgerechten gesetzlichen Grundlage für die Videoüberwachung durch öffentliche Stellen,
- beim Gesundheitsdatenschutz,
- bei der Verankerung des Datenschutzes in der Steuerverwaltung,
- bei der Kooperation mit Unternehmen, Verbänden und Verwaltungen im Bereich von Internetwirtschaft und eGovernment,

gibt es fortbestehende oder neue **Problem- und Konfliktfelder**, so zum Beispiel

- in der Ausfüllung der Beratungsfunktion des LfD gegenüber dem Niedersächsischen Landtag und seinen Ausschüssen (vgl. dazu S. 8 des Tätigkeitsberichtes),
- in der übermäßigen Beschränkung individueller Freiheits- und Selbstbestimmungsrechte durch immer neue und erweiterte Überwachungs- und Ausforschungsbefugnisse insbesondere der Sicherheitsbehörden (vgl. dazu Nrn.1, 2 und 3 des Tätigkeitsberichtes)
- in der Absicherung des Rechts auf informationelle Selbstbestimmung bei kartengestützten Massenverfahren im Rahmen der Gesundheitskarte und der Job-Card (vgl. dazu Nrn. 7 und 8 des Tätigkeitsberichtes),
- bei der „Veredelung“ von Kundendaten mit Hilfe mathematisch-statistischer Methoden im Rahmen des Scorings (vgl. dazu Nr. 13 des Tätigkeitsberichtes),

Der Landesbeauftragte für den Datenschutz Niedersachsen
Brühlstraße 9 · 30169 Hannover · Telefon (05 11) 1 20–45 00 · Fax (05 11) 1 20-45 99
Internet: www.lfd.niedersachsen.de · E-Mail: burckhard.nedden@lfd.niedersachsen.de

- bei der datenschutzgerechten Ausgestaltung neuer technischer Systeme wie der Biometrie oder dem Einsatz von miniaturisierten Funkchips (RFID´s), die berührungslos ausgelesen oder beschrieben werden können (vgl. dazu Nrn. 14 und 15 des Tätigkeitsberichtes).

Zu den **Problem- und Konfliktfeldern**:

1. Nach dem Niedersächsischen Datenschutzgesetz (§ 22 Abs. 1 Satz 3 und Abs. 3 Satz 3) hat der Landesbeauftragte eine **Beratungs- und Informationsfunktion** auch gegenüber dem Landtag und seinen Ausschüssen. Diese Funktion gewinnt besonderes Gewicht bei strittigen oder konfliktbeladenen Entscheidungen, wie sie gerade im Bereich des Datenschutzes dadurch häufig auftreten, dass hier zwischen den fachlichen Anforderungen an eine (möglichst umfassende) Informationserhebung und –verarbeitung einerseits und den Anforderungen zum Schutz des Rechts auf informationelle Selbstbestimmung andererseits ein sachgerechter Ausgleich gefunden werden muss. Die praktische Wahrnehmung der Beratungs- und Informationsaufgaben wird zunehmend dadurch erschwert, dass sehr häufig die entscheidenden Weichenstellungen weit im Vorfeld der parlamentarischen Beratungen in Arbeitskreissitzungen oder anderen politischen Abstimmungsgremien getroffen werden. Etwaige Stellungnahmen des LfD im Rahmen des förmlichen parlamentarischen Verfahrens treffen dann auf bereits umfassend fixierte Positionen und kommen insofern zu spät. Ich würde mir wünschen, dass der Sachverstand des LfD und seiner Mitarbeiterinnen und Mitarbeiter, für dessen Vorhaltung das Land Jahr für Jahr Haushaltsmittel in nicht unerheblicher Höhe einsetzt, auch hier umfassender genutzt würde.

2. Im Berichtszeitraum sind im Bundes- und Landesrecht weitere **Überwachungs- und Ausforschungsbefugnisse,** vor allem für die Sicherheitsbehörden neu geschaffen oder ausgeweitet worden. Nimmt man die bereits bestehenden Befugnisse hinzu, ist aus meiner Sicht folgender Befund unausweichlich:

   Überwachung und Ausforschung der Bürgerinnen und Bürger haben insgesamt gesehen einen Umfang erreicht, der das Recht auf informationelle Selbstbestimmung und die Möglichkeiten zu freier und unbeobachteter Bewegung und Kommunikation für den Einzelnen im Übermaß einschränkt, auch mit dem Hinweis auf Terror- und Kriminalitätsgefahren nicht zu rechtfertigen und unverhältnismäßig ist.

   Ich komme zu diesem Urteil auch deshalb, weil viele der neuen oder erweiterten Überwachungs- und Ausforschungsbefugnisse auf heimliche, verdeckte Informationserhebungen und -speicherungen oder auf für den Betroffenen völlig intransparente Auswertungen ausgerichtet sind; außerdem werden sie bereits weit im Vorfeld konkreter Straftaten oder Gefahren eingesetzt und führen zu einer präventiven Erfassung völlig legaler alltäglicher Handlungen und Tätigkeiten.
   Derartige neue oder erweiterte Befugnisse sind zum Beispiel:

   a) die Einführung der präventiven Überwachung der Telekommunikation im novellierten Niedersächsischen Polizeigesetz,

b) die Ausweitung der polizeilichen Identitätsfeststellung an sogenannten gefährlichen Orten oder gefährlichen Objekten, der Befugnis zur Einrichtung von Kontrollstellen und der Regelungen zum verdeckten Einsatz technischer Mittel zur Bild- und Tonaufzeichnung im neuen Polizeigesetz,
c) die im neuen Telekommunikationsgesetz vorgesehene Berechtigung der Provider, unabhängig von der betrieblichen Notwendigkeit die Verkehrsdaten etwa für Zwecke der Auskunftserteilung an Sicherheitsbehörden bis zu 6 Monaten vorzuhalten, sowie die Pflicht, auch beim Kauf von vertragslosen (prepaid) Handys Namen, Anschrift und Geburtsdatum des Käufers zu erheben,
d) die dem Kontoinhaber verborgen bleibende automatisierte Zugriffsmöglichkeit auf die Kontostammdaten bei Banken und Sparkassen nicht nur durch das Bundesamt für Finanzen, sondern ab 1. April 2005 auch für eine Vielzahl anderer Behörden einschließlich der Finanzämter, Sozialbehörden und der Sicherheitsbehörden,
e) der gesetzlich vorgegebene Einsatz von internen Sicherungssystemen bei Banken und Sparkassen, mit denen durch eine permanente Rasterung der Kontobewegungen mögliche Geldwäschefälle erkannt werden sollen,
f) die umfassende Erhebung und Übermittlung von Flugpassagierdaten bei Flügen nach Nordamerika.

Nimmt man noch

g) die in der politischen Diskussion von vielen vehement geforderte und auf europäischer Ebene schon fast abgesegnete Pflicht der Provider zur langfristigen und pauschalen Speicherung sämtlicher Telekommunikations-Verkehrsdaten auf Vorrat für einen eventuellen Zugriff der Sicherheitsbehörden,
h) die Überlegungen des Bundesinnenministers für ein Sicherheitspaket III,
i) die von der Innen- und der Justizministerkonferenz übernommene Forderung nach dem Einsatz der DNA-Analyse als normalem Routineinstrument einer jeden erkennungsdienstlichen Behandlung,
j) die Auflockerungen des Trennungsgebotes zwischen Verfassungsschutz und Polizei durch Schaffung einheitlicher Dateien sowie durch die geplante Einrichtung eines gemeinsamen Informations- und Analysezentrums (GIAZ),
k) das in Hessen bereits eingeführte und auch in Niedersachsen in Vorbereitung befindliche polizeiliche Scannen und Abgleichen von Kraftfahrzeugkennzeichen aus dem laufenden Verkehr,
l) die bereits vor dem ersten Praxiseinsatz der LKW-Maut erhobene Forderung nach einem Zugriff der Sicherheitsbehörden auf die Maut-Erfassungs- und -Abrechnungsdaten

hinzu, dann wird deutlich, dass wir es mit einer schleichenden Erosion der Persönlichkeitsrechte und insbesondere des Rechts auf informationelle Selbstbestimmung zu tun haben, bei der der Kampf gegen den Terrorismus und die organisierte Kriminalität zu einem im Einzelfall kaum noch hinterfragten pauschalen Legitimationsmuster geworden ist. Auch die zeitliche Befristung mancher dieser neuen oder erweiterten Überwachungs- und Ausforschungsbefugnisse ändert nichts an diesem Befund, wenn die damit verbundenen Evaluationspflichten halbherzig, verspätet oder gar nicht ausgefüllt werden.

Mein Fazit lautet: Unser Staat wandelt sich in der Ausrichtung vom Rechtsstaat zu einem Sicherheits- oder Schutzstaat und wir sind auf dem besten Wege, Freiheitsrechte allzu bereitwillig auf dem Altar der Sicherheit zu opfern, ohne dass wir die Hoffnung haben können, dass diese Sicherheit auch nur annähernd vollständig gewährleistet werden kann.

3. Mit der zum 1. Januar 2006 einzuführenden elektronischen **Gesundheitskarte** und dem ein Jahr später vorgesehenen **JobCard-Verfahren** werden in einem bisher noch nicht praktizierten Ausmaß massenhaft Gesundheitsdaten elektronisch verfügbar gemacht bzw. millionenfach Arbeitsnehmerdaten bei einer zentralen Stelle gespeichert und zum Abruf bereitgehalten. Bei beiden Verfahren ist schon aus Gründen der Akzeptanz von überragender Bedeutung, dass Datenschutz und Datensicherheit umfassend gewährleistet werden. Zusammen mit den Datenschutzbeauftragten im Bund und in den anderen Ländern begleite ich daher die Vorbereitungen für beide Verfahren sehr intensiv.
   Bei der **Gesundheitskarte** ist noch nicht endgültig geklärt, ob die Daten vorzugsweise auf der Karte selbst oder auf einem zentralen Server gespeichert werden sollen. In jedem Fall muss die Datenhoheit und die Verfügungsbefugnis des Patienten über „seine“ Daten ebenso wie die Vertraulichkeit der Daten ohne Abstriche sichergestellt sein. Das betrifft nicht nur den Zugriff auf die gespeicherten Daten, für den eine doppelte Sicherung durch eine Freischaltung durch den Versicherten selbst sowie durch eine elektronische Authentifizierung des Zugreifenden über eine Signatur bereits gesetzlich vorgegeben ist, sondern auch die Möglichkeit des Karteninhabers, den Zugriff auf bestimmte Datenbestände im Einzelfall beschränken und auf andere sperren zu können. Um alle Optionen für die künftige Sicherheitsinfrastruktur offen zu halten, sollten alle Sicherheitsfunktionen auf der Karten-Betriebsebene und nicht nur durch Steuerungsmöglichkeiten auf den Hintergrundsystemen realisiert werden.
   Beim **JobCard-Verfahren** ist ebenfalls eine doppelte „Freischaltung“ als Voraussetzung für einen Zugriff auf die zentral gespeicherten Daten vorgesehen. Aus Datenschutzsicht ist darüber hinaus noch prüfungsbedürftig, ob durch eine Ende-zu-Ende-Verschlüsselung Zugriffsmöglichkeiten der Zentralen Speicherstelle ausgeschlossen werden müssen und die alleinige Verfügungsbefugnis des Arbeitsnehmers über seine Daten sichergestellt werden kann. Immerhin verfügt die Zentrale Speicherstelle nach der Umsetzung des JobCard-Verfahrens über Entgelt- und andere Leistungsdaten aller in Deutschland beschäftigten Arbeitnehmer und Beamten für jeweils zehn zurückliegende Jahre.

4. Immer mehr Unternehmen versuchen, über ihre Kunden mit Hilfe statistisch-mathematischer Verfahren mehr zu erfahren und insbesondere Informationen über deren finanzielle Leistungsfähigkeit oder künftige Zahlungsbereitschaft zu erhalten. Damit soll die Einschätzung des eigenen Ausfallrisiko etwa bei Abschluss einer Versicherung, eines Kreditvertrages oder eines längerfristigen Mietverhältnisses ermöglicht werden. Dazu werden sogenannte **Scoring-Verfahren** eingesetzt, bei denen Bewertungen, die über zu dem Kunden passende statistische Vergleichsgruppen vorhanden sind (etwa zur Zahlungsmoral der verschiedenen Berufsgruppen, zur Unfallhäufigkeit von Verkehrsteilnehmern der einzelnen Altersgruppen oder zum Freizeitverhalten der Bewohner von Gemeinden unterschiedlicher Größenklassen), für den Kunden übernommen und zu einem kundenbezogenen Gesamtscorewert zusammengeführt werden. Die Einordnung eines Kunden in eine bestimmte Vergleichsgruppe und die Übernahme des dieser Vergleichsgruppe zugeordneten Wertes ist aus mei-

ner Sicht ein Bearbeitungsvorgang mit Personenbezug, für den daher zu fragen ist, inwieweit er die rechtlichen Voraussetzungen erfüllen muss, die auch sonst für die Verarbeitung personenbezogener Daten gelten. Von Seiten der Wirtschaft wird diese Einordnung häufig noch bestritten. Dabei wird aber übersehen, dass mit der Zuordnung des Kunden zu einer bestimmten Vergleichsgruppe und der Übernahme des dafür ausgebrachten Scorewertes für diesen Kunden eine sehr konkrete personenbezogene Bewertung getroffen wird, die ja auch gerade vom Unternehmen als Entscheidungshilfe angestrebt wird. Meine datenschutzrechtlichen Anforderungen an Scoring-Verfahren sind daher

a) es darf keine automatisierten Entscheidungen „nach Tabelle“ geben,
b) für den Betroffenen muss transparent gemacht werden, dass ein Scoring-Verfahren durchgeführt wird und welche Bewertungsvorgänge damit verbunden sind,
c) es dürfen keine Persönlichkeitsmerkmale oder Daten, deren Bewertung diskriminierenden Charakter haben kann (z.B. Gesundheitsdaten, Daten zur politischen Meinung, Religionszugehörigkeit oder zum Sexualleben), in ein Scoring-Verfahren einbezogen werden,
d) dem Betroffenen muss das Ergebnis des Scoring-Verfahrens in einer Weise mitgeteilt werden, dass er die vorgenommenen Bewertungen nachvollziehen und ggf. gegen das Bewertungsergebnis oder dagegen, dass er einer bestimmten, auf ihn möglicherweise nicht zutreffenden statistischen Vergleichsgruppe zugeordnet worden ist, Gegenvorstellungen erheben kann.

Ich werde den Problembereich im Rahmen eines Kooperationsprojektes mit großen niedersächsischen Unternehmen im nächsten Jahr noch weiter aufarbeiten.

5. Mit der vom Rat der EU beschlossenen Verordnung zur Speicherung der biometrischen Merkmale „Gesicht“ und „Fingerabdruck“ in maschinenlesbarer Form in Reisepässen erhält die Diskussion um die notwendigen Sicherheitsmaßnahmen, Datenmissbrauch und zentrale Referenzdateien bei der **Biometrie** neuen Zündstoff. Der deutsche Gesetzgeber, der sich die Entscheidung über die Auswahl der geeigneten biometrischen Merkmale im Pass- und Personalausweisgesetz ausdrücklich vorbehalten und bisher nur die Speicherung eines Merkmals zugelassen hatte, ist damit vor vollendete Tatsachen gestellt worden. Die Vorgaben der EU sind für die maschinenlesbaren Gesichtsbilder innerhalb von 18 Monaten (also bis Mitte 2006) und für die Fingerabdrücke bis Anfang 2008 umzusetzen. Aus Datenschutzsicht sind bei der Ausgestaltung der technischen Komponenten und bei dem Verfahren folgende Eckpunkte unverzichtbar:

   a) eine Nutzung der biometrischen Merkmale darf nur zur Personenverifikation, nicht zur –identifikation stattfinden,
   b) die biometrischen Merkmale dürfen zur Vermeidung von Überschussinformationen nicht als Rohdaten, sondern nur als mathematisches Komprimat (Template) auf dem Ausweispapier abgespeichert werden,
   c) eine Hinterlegung der Merkmale in einer zentralen Referenzdatei muss gesetzlich ausgeschlossen bleiben,
   d) für das Auslesen der biometrischen Merkmale aus dem Ausweispapier müssen Verfahren vorgegeben werden, die eine aktive Mitwirkung des Betroffenen erfordern; ein verdecktes Auslesen und Erfassen muss streng untersagt werden.

   Bei der ebenfalls von der EU vorgegebenen Abspeicherung auf einem mit dem Ausweispapier verbundenen elektronischen und von außen über ein Lesegerät

ansprechbaren Funk-Chip (RFID), ergeben sich weitere Anforderungen zur Gewährleistung der Datensicherheit: Es muss verlässlich verhindert werden, dass beim Auslesevorgang die Übermittlung der Daten zwischen Speicherchip und Lesegerät kompromittiert werden kann, d.h. dass die Daten von außen verfälscht werden oder dass ein „Identitätsdiebstahl“ stattfindet. Dies kann zum Beispiel durch eine hochwertige Verschlüsselung der Biometriemerkmale erreicht werden.

Die vom Europäischen Parlament und vom Bundestag geforderte umfassende Risikoanalyse und Folgenabschätzung, bei der sowohl die technische Zuverlässigkeit der verschiedenen Verfahren (Fehlerrate!) als auch die gesellschaftlichen Auswirkungen der Aufnahme biometrischer Merkmale in Ausweispapiere zu bewerten wären, ist durch die vorschnelle Entscheidung der EU umgangen worden. Und auch der Nachweis der Geeignetheit und Erforderlichkeit für Zwecke der Terrorismusbekämpfung bleibt wohl ebenso auf der Strecke wie die Beantwortung der Frage nach den Kosten und eine seriöse Kosten-Nutzen-Analyse.

6. **Radio-Frequency-Identification (RFID)** bezeichnet ein Verfahren, bei dem miniaturisierte IT-Systeme (RFID-Chips, RFID-Tags), die mit einem Gegenstand (oder als Implantat auch unmittelbar mit einer Person) fest verbunden sind, über Funksignale mit geeigneten Lesegeräten kommunizieren. Je nach Ausstattung können die auf dem Chip gespeicherten Informationen lediglich ausgelesen oder aber auch inhaltlich verändert und Verarbeitungsprozesse auf dem Chip von außen angestoßen werden. Die Einsatzfelder reichen von der Warenlogistik, der Diebstahlssicherung und der Produktionsautomation bis zu Kundenbindungssystemen und – durch Abspeicherung von biometrischen Merkmalen auf dem RFID-Chip – zur Personenverifikation. Die Kommunikation wird in allen Fällen von außen durch ein von einem Lesegerät ausgehendes Signal angestoßen; anders als bei den bisher üblichen Barcodes muss der Chip/Tag dabei dem Lesegerät nicht mehr ausdrücklich präsentiert werden, vielmehr wird die Kommunikation automatisch ausgelöst, wenn der Chip/Tag in die Nähe eines Lesegerätes kommt. Wenn der Chip und/oder das Lesegerät nicht erkennbar oder bewusst verborgen sind, kann die Kommunikation auch verdeckt und für den Betroffenen unbewusst erfolgen. Die Übertragungsweite kann dabei zwischen wenigen Zentimetern und mehreren Metern liegen. Es wird sogar berichtet, dass besonders hoch entwickelte Chips über GPS aktiviert werden können und damit eine Kommunikation über sehr weite Entfernungen ermöglichen.
   Datenschutzrechtlich ergeben sich bereits dann Probleme, wenn auf diese Weise eindeutig gekennzeichnete Waren, Gebrauchsgegenstände oder Papiere einer bestimmten Personen zugeordnet und diese Zuordnungen auf dem Chip selbst oder in Hintergrundsystemen abgespeichert werden (z.B. bei elektronischen Bezahlverfahren oder Kundenbindungssystemen) oder wenn der Chip zur Speicherung und zum Auslesen personenbezogener Daten (wie etwa biometrischer Merkmale) dient.
   Für den Einsatz von RFID-Systemen bei der Warenkennzeichnung und beim Warenverkauf bestehen folgende allgemeine datenschutzrechtliche Anforderungen:
   - die Betroffenen müssen umfassend über Einsatz und Verwendungszweck informiert werden,

- die RFID-Systeme sind so weiter zu entwickeln, dass RFID-Chips ohne Verarbeitungsfunktion eine Löschung aller Daten durch den Betroffenen ermöglichen,
- im Endkundengeschäft sind geeignete Geräte für eine Löschung der auf dem RFID-Chip gespeicherten Daten bei Verlassen der Verkaufsräume kostenfrei bereitzuhalten,
- für RFID-Systeme mit Verarbeitungsfunktion ist sicherzustellen, dass eine Kommunikation zwischen Lesegerät und RFID-Chip nur mit Kenntnis und Einwilligung des Betroffenen erfolgt,
- die Vertraulichkeit der Kommunikation sowie der auf dem RFID-Chip gespeicherten Daten ist durch geeignete technische Maßnahmen verlässlich sicherzustellen,
- Betroffene müssen kostenfrei Gelegenheit erhalten, sich Kenntnis über die auf einem RFID-Chip gespeicherten Informationen zu verschaffen,
- es sind RFID-Systeme anzubieten, die auf der Anwendungsebene nicht über eine eindeutige Kennzeichnung identifizierbar sind.

Auf diese Weise wird verhindert, dass verdeckte Nutzungs- oder Bewegungsprofile von Kunden entstehen.

Handlungsschwerpunkte 2005

Im Jahr 2005 steht die Diskussion über die richtige Gewichtung zwischen der Gewährleistung von Sicherheit einerseits und dem Recht auf informationelle Selbstbestimmung andererseits weiterhin auf der Tagesordnung. Ich erwarte, dass hierzu durch die Entscheidung des Bundesverfassungsgerichts über die Verfassungsbeschwerde zur präventiven TKÜ im Niedersächsischen Polizeigesetz neue datenschutzrechtliche Maßstäbe gesetzt werden.

Neben den vorstehend bereits erörterten Bereichen werden weitere Handlungsschwerpunkte meiner Tätigkeit in folgenden Feldern liegen:

- datenschutzgerechte Ausgestaltung der Verfahren beim elektronischen Meldewesen,
- Datenschutz und Datensicherheit an Schulen,
- Schutz der Gesundheitsdaten in Krankenhäusern,
- Beratung kleiner und mittelständischer Unternehmen bei Datentransfers in Drittländer und beim Einsatz von Videotechnik,
- Entwicklung datenschutzrechtlicher Leitplanken für Geo-Informationssysteme,
- Neuordnung des Datenschutzrechts für Tele- und Mediendienste,
- Datenschutzrechtliche Anforderungen an den Einsatz von Dokumenten-Management-Systemen in der Verwaltung,
- Schulung der behördlichen und betrieblichen Datenschutzbeauftragten,
- Herausgabe einer leicht verständlichen, praxisgerechten Handlungsanleitung für den häuslichen PC-Einsatz.

Nachdem nunmehr in den Bundestag der Entwurf für ein **Informationszugangsgesetz** für die Bundesverwaltung eingebracht worden ist, wird auch in Niedersachsen die Diskussion zur Schaffung entsprechender landesrechtlicher Vorschriften verstärkt zu führen sein. Ich habe mich seit langem für einen freien Informationszugang der niedersächsischen Bürgerinnen und Bürger zu den Dokumenten der Verwaltung eingesetzt. Für die dabei entstehenden Zielkonflikte mit dem Schutz von Betriebs- und Geschäftsgeheimnissen oder mit dem Schutz personenbezogener Daten gibt es praxisgerechte und erprobte Lösungen.

Für den **25. Januar 2005 um 10.00 Uhr** lade ich zu einem **Pressefrühstück** in meine Dienststelle Brühlstraße 9 ein, bei dem die angesprochenen und weitere Themen des Tätigkeitsberichtes und der Entwicklungen im Datenschutz vertieft erörtert werden können.