Schleswig-Holsteinischer Landtag
Umdruck 16/1992

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

ULD ▪ Postfach 71 16 ▪ 24171 Kiel

Ân den Vorsitzenden des Finanzausschusses
des Schleswig-Holsteinischen Landtages
Günter Neugebauer, MdL
Landeshaus
24105 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Dr. Johann Bizer
Durchwahl: 988-1286

Aktenzeichen:
LD7-65.02/07.001

Kiel, 30. April 2007

Einsatz einer zentralen Serverlösung für die Bewährungshilfe
Sitzung des Finanzausschusses vom 3. Mai 2007
LT-Umdrucke 16/1844, 1895, 1947

Sehr geehrter Herr Vorsitzender,

Die Fraktion der FDP hat für die Erörterung der Sitzung des Finanzausschusses am 3. Mai 2007 zum Tagesordnungspunkt 4 „Software für Bewährungshilfe, Gerichtshilfe und Führungsaufsicht“ eine Stellungnahme des ULD erbeten, die ich Ihnen als Anlage übersende.

Mit freundlichen Grüßen

gez. Dr. Johann Bizer
(Stellv. Landesbeauftragter für den Datenschutz)

Anlage

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

ULD • Postfach 71 16 • 24171 Kiel

Ân den Vorsitzenden des Finanzausschusses
des Schleswig-Holsteinischen Landtages
Günter Neugebauer, MdL
Landeshaus
24105 Kiel

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Dr. Johann Bizer
Durchwahl: 988-1286

Aktenzeichen:
LD7-65.02/07.001

Kiel, 30. April 2007

Stellungnahme zum Einsatz
einer zentralen Serverlösung für die Bewährungshilfe
LT-Umdrucke 16/1844, 1895, 1947

Rechtsgrundlage der Datenverarbeitung in der Bewährungshilfe ist § 12 des Bewährungs- und Gerichtshilfegesetzes vom 31. Januar 1996 in Verbindung mit der Landesverordnung für den bereichsspezifischen Datenschutz in der Bewährungs- und Gerichtshilfe vom 30. April 1996. Letztere verweist in § 3 Abs. 2 für die elektronische Datenverarbeitung auf das LDSG sowie die Datenschutzverordnung. Ferner ist die Anordnung über die Organisation der Bewährungs- und Gerichtshilfe (OrgBG) vom 15. November 1996 zu beachten, in der u.a. die Grundsätze der Aufgabenwahrnehmung (§ 2) sowie die Vertraulichkeit der Akten und Register (§ 21) zu entnehmen sind.

1. Unter Gesichtspunkten des Datenschutzes und der Datensicherheit bietet eine zentrale Serverlösung eines Windows-Terminal Servers (WTS) für zahlreiche Anwender an unterschiedlichen Stanorten wie der Bewährungshilfe den Vorteil, dass die dezentralen Stellen von Aufgaben der Administration und der Programmpflege (bspw. dem Einspielen von Updates) entlastet und diese kompetent an einer zentralen Stelle gebündelt und professionell von einem Dienstleister übernommen werden können. Dezentrale Systemlösungen haben demgegenüber den Nachteil, dass die Administration vor Ort durch kompetentes und regelmäßig zu schulendes Personal erfolgen muss. Zudem ist erfahrungsgemäß die Qualitätssicherung und Kontrolle der Administration an verteilten Standorten erheblich aufwändiger als bei einer zentralen Serverlösung. Unterbleibt sie, weil die hierfür erforderlichen Ressourcen nicht vorhanden sind, dann sind die Sicherheitsrisiken bei einer dezentralen Lösung höher als bei einer zentralen Serverlösung.

   Für eine zentrale Serverlösung spricht, dass die Administration kompetent an einem Standort revisionssicher durchgeführt werden kann.

2. Eine zentrale Serverlösung ist unter dem Gesichtspunkt der Datensicherung gegen Verlust (Verfügbarkeit) einer dezentralen Lösung vorzuziehen. Bei einer dezentralen Lösung müssen die gespeicherten Daten nicht nur lokal durch die erforderlichen technischen (bspw. Festplattenverschlüsselung) und baulichen (bspw. neue Türen, Fenster, Schlüsselmanagement) Maßnahmen abgesichert werden, sondern auch die Backup-Daten selbst müssen gegen den Fall eines Diebstahl gesondert gesichert werden. Da die Bewährungshilfe aus funktionalen Gründen teilweise in Wohnungen untergebracht ist (LT-Umdruck 16/1844, Anlage 2 zu 13.), werden erhebliche Aufwendungen erforderlich sein, um ein angesichts der erheblichen Sensibilität der Betroffenendaten angemessenes Schutzniveau zu erreichen. Demgegenüber bietet ein zentrales Rechenzentrum ein deutlich höheres Maß an Datensicherheit gegen externe Angriffe sowie gegen einen Ausfall der Systeme. Bei einem (teilweisen) Ausfall der Systeme ist zudem in einem professionellen Betrieb eines Rechenzentrums eine schnellere Wiederherstellung über ein deutlich längeres Wartungsfenster möglich als es aus Ressourcengründen bei einer lediglich lokalen Administration über mehrere Standorte der Fall sein kann.

   Mit einer zentralen Serverlösung kann die Verfügbarkeit der Daten besser gewährleistet werden als bei einer dezentralen Lösung.

3. Eine zentrale Serverlösung erfordert, dass von den Clients (an den Standorten der Bewährungshilfe) über elektronische Netze auf die auf dem zentralen Server gespeicherten personenbezogenen Daten der Mandanten zugegriffen werden muss. Eine solche elektronische Übermittlung bedeutet unter Gesichtspunkten des Datenschutzes gegenüber einer lokalen Datenverarbeitung prinzipiell eine Risikoerhöhung, die aber durch technische Maßnahmen minimiert werden kann. Erfolgt der Datentransfer über das Landesnetz, so ist dieses durch das ULD bereits geprüft und im Sommer 2006 erfolgreich einem Datenschutz-Audit unterzogen worden. Ob zusätzliche Sicherheitsbedürfnisse angesichts der Sensibiltät der Betroffenendaten durch eine Verschlüsselung auf Applikationsebene abgesichert werden müssen, ist von den verantwortlichen Stellen zu prüfen.

   Die sich aus einer zentralen Serverlösung ergebenden Transportrisiken über elektronische Netze können durch den Einsatz des Landesnetzes ggf. auch zusätzlicher Verschlüsselungsmaßnahmen datenschutzkonform abgesichert werden.

4. Die Verantwortung für die Rechts- und Ordnungsmäßigkeit der Datenverarbeitung der personenbezogenen Daten liegt bei den Trägern der Bewährungshilfe, d.h. den bei den Landgerichten nach § 4 Abs. 1 BGG eingerichteten Dienststellen. Wird die Datenverarbeitung durch einen Dienstleister technisch unterstützt wird, dann ist dies nach § 17 LDSG nur unter Beachtung der Vorgaben der Auftragsdatenverarbeitung möglich, d.h. insbesondere durch entsprechende schriftliche Weisungen und Kontrollmaßnahmen. Die einzelne Dienststelle der Bewährungshilfe kann ihrer gesetzlichen Datenverantwortung nur nachkommen, wenn Konzept und Implementierung der zentralen Serverlösung

gewährleisten, dass die Betroffenendaten der einzelnen Dienststellen der Bewährungshilfe von einander getrennt verarbeitet werden (getrennte Mandantenhaltung). Die Mandantenfähigkeit der zentralen Serverlösung ist datenschutzrechtliche Voraussetzung, damit die einzelnen Dienststellen die Vertraulichkeit ihrer Akten gewährleisten können und die Weitergabe der Betroffenendaten nur in den vom Gesetz vorgeschriebenen Fällen kontrolliert erfolgt.

Eine zentrale Serverlösung muss eine getrennte Mandantenhaltung der Daten der Betroffenen gewährleisten, damit die einzelnen Dienststellen der Bewährungshilfe ihrer Datenverantwortung nach § 17 LDSG nachkommen können.

5. Ein Vorteil einer zentralen Serverlösung ist, dass die einzelnen Dienststellen der Bewährungshilfe ihrer Datenverantwortung nachkommen können, indem sie sich auf ein vom Ministerium zentral erstelltes oder veranlasstes IT-Konzept (§ 4 f. DSVO) sowie ein entsprechendes Sicherheitskonzept (§ 6 DSVO) stützen, das durch Standard-Sicherheitsmaßnahmen für die lokalen Client-Arbeitsplätze lediglich zu ergänzen ist. Voraussetzung ist allerdings, dass die entsprechenden Konzepte und ihre Implementierung den gesetzlichen Anforderungen entsprechen. Vorsorglich weisen wir darauf hin, dass das uns bislang vorliegende Sicherheitskonzept für den ABS-Arbeitsplatz von Dataport mit Dattum vom 1.1.2004 für das geplante Verfahren SoPart noch angepasst werden muss und zur Erfüllung der gesetzlichen Anforderungen noch grundlegend zu überarbeiten ist. Das ULD unterstützt dies gerne beratend.

Einführung und Betrieb einer zentralen Serverlösung können sich auf zentral erstellte IT- und Sicherheitskonzepte stützen. Allerdings entsprechen die dem ULD bislang vorliegenden Unterlagen noch nicht den Anforderungen des LDSG/DSVO und sind grundlegend zu überarbeiten.

6. Die Dienststellen der Bewährungshilfe können in der Wahrnehmung ihrer Datenverantwortung nach § 17 LDSG bei Einführung und Betrieb einer zentralen Serverlösung durch das Ministerium unterstützt werden, indem die zentrale Implementierung des Verfahrens SoPart bei Dataport, der entsprechenden Standardarbeitsplätze der Bewährungshilfe sowie die erforderlichen Kontrollmaßnahmen durch ein Datenschutz- und Sicherheitsmanagement einer Datenschutz-Auditierung nach § 43 Abs. 2 LDSG unterzogen werden. Ziel einer solchen Auditierung ist die Bestätigung einer datenschutzkonformen Gestaltung der zentralen Serverlösung, damit die Dienststellen der Bewährungshilfe sich ohne weiteren Aufwand ihre Datenverantwortung erfüllen können. Das ULD bietet vorbereitende Gespräche zur Durchführung einer solchen Auditierung an.

Die datenschutzkonforme Gestaltung der zentralen Serverlösung sollte durch ein Datenschutz-Audit des ULD bestätigt werden.

gez. Dr. Johann Bizer
(Stellv. Landesbeauftragter für den Datenschutz)