



LDI NRW, Postfach 20 04 44, 40102 Düsseldorf

31. Juli 2013

Seite 1 von 4

Frau
Carina Gödecke MdL
Präsidentin des Landtags
Nordrhein-Westfalen
Postfach 101143
40002 Düsseldorf



Datenschutz bei Datenverarbeitungen mit Auslandsbezug und Datensicherheit

Sehr geehrte Frau Landtagspräsidentin,

zu Ihrer Unterrichtung erlaube ich mir, Ihnen den Abdruck meines
Schreibens an die Mitglieder der Landesregierung zuzuleiten.

Mit freundlichen Grüßen


(Ulrich Lepper)

Dienstgebäude und
Lieferanschrift:
Kavalleriestraße 2 - 4
40213 Düsseldorf
Telefon 0211 38424-0
Telefax 0211 38424-10
poststelle@ldi.nrw.de
www.ldi.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 704, 709, 719
Haltestelle Poststraße



LDI NRW, Postfach 20 04 44, 40102 Düsseldorf

31. Juli 2013

Seite 1 von 4

An die
Mitglieder der Landesregierung
des Landes Nordrhein-Westfalen

Datenschutz bei Datenverarbeitungen mit Auslandsbezug und Datensicherheit

Sehr geehrte Damen und Herren,

aus Anlass der Berichte über Überwachungsmaßnahmen ausländischer Geheimdienste wende ich mich mit der Bitte an Sie, die nachfolgende Darstellung über rechtliche Anforderungen an Datenübermittlungen öffentlicher Stellen mit Auslandsbezug sowie damit im Zusammenhang stehende Hinweise zur Datensicherheit aufzugreifen und die Empfehlungen Ihren weiteren Überlegungen zugrunde zu legen. Ferner bitte ich mein Schreiben an die Behörden Ihres Geschäftsbereiches weiterzuleiten. Mit gleichlautendem Schreiben habe ich mich an die Kommunen in Nordrhein-Westfalen sowie an die kommunalen Spitzenverbände bereits unmittelbar gewandt.

I.

Das Datenschutzgesetz des Landes Nordrhein-Westfalen verlangt für Übermittlungen an öffentliche und nicht-öffentliche Stellen ins außereuropäische Ausland, dass beim Empfänger der Daten ein **angemessenes Datenschutzniveau gewährleistet** ist, § 17 DSGVO NRW. Soweit für die Übermittlung personenbezogener Daten durch öffentliche Stellen ins außereuropäische Ausland besondere gesetzliche Regelungen bestehen, gehen diese dem Datenschutzgesetz des Landes vor.

Dienstgebäude und
Lieferanschrift:
Kavalleriestraße 2 - 4
40213 Düsseldorf
Telefon 0211 38424-0
Telefax 0211 38424-10
poststelle@ldi.nrw.de
www.ldi.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 704, 709, 719
Haltestelle Poststraße

Die Europäische Kommission hat in mehreren Entscheidungen Grundsätze des „sicheren Hafens“ („Safe Harbor“) zum Datentransfer an Unternehmen in den USA (2000) und Standardvertragsklauseln zum Datentransfer auch an Unternehmen in anderen Drittstaaten (2004 und 2010) festgelegt. Die Beachtung dieser Vorgaben soll gewährleisten, dass personenbezogene Daten, die in die USA oder andere Drittstaaten übermittelt werden, dort einem angemessenen Datenschutzniveau unterliegen.

Nach den Berichten, nach denen ausländische Dienste umfassend und anlasslos ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung auf personenbezogene Daten zugreifen, die von Deutschland an Stellen in den USA übermittelt werden, muss beim gegenwärtigen Erkenntnisstand allerdings von einer hohen Wahrscheinlichkeit ausgegangen werden, dass Schutzanforderungen verletzt sind.

Das gilt auch bei Inanspruchnahme von Cloud-Diensten, bei denen sich wegen des Sitzlandes und/oder der Belegenheit der dem anbietenden Unternehmen zur Verfügung stehenden Server ein Zugriff auf personenbezogene Daten der Bürgerinnen und Bürger durch Stellen in Drittstaaten nach Art und Umfang gegenwärtig nicht einschätzen lässt. Auf Angebote nichtdeutscher Unternehmen an Schulen und Schulträger zur Verarbeitung von Daten der Schule sei in diesem Zusammenhang besonders hingewiesen.

Zwar enthalten die für Übermittlungen in die USA geltenden Safe-Harbor-Grundsätze eine Regelung, die die Geltung des „sicheren Hafens“ begrenzt, sofern es die nationale Sicherheit erfordert oder Gesetze solche Ermächtigungen vorsehen. Im Hinblick auf das Ziel eines wirksamen Schutzes der Privatsphäre darf jedoch von diesen Eingriffsbefugnissen nur im Rahmen des tatsächlich Erforderlichen Gebrauch gemacht werden. Ein umfassender und anlassloser Zugriff auf personenbezogene Daten kann demgegenüber durch Erwägungen zur nationalen Sicherheit nicht gerechtfertigt werden.

Somit kann für Datentransfers über Safe Harbor in der Regel ein angemessenes Datenschutzniveau derzeit nicht angenommen werden.

Fehlt es an einem angemessenen Datenschutzniveau, so ist, vorbehaltlich spezialgesetzlicher Erlaubnisnormen, nach § 17 Absatz 2 DSGVO eine Übermittlung nur unter den dort bezeichneten **engen** und in jedem Einzelfall zu prüfenden Voraussetzungen möglich.

Dementsprechend besteht für alle öffentlichen Stellen im Land die Verpflichtung, vor Übermittlung personenbezogener Daten im Rahmen der ihnen obliegenden Vorabkontrolle zu prüfen, ob - zunächst unabhängig von einem Datentransfer mit Auslandsbezug - auf einer ersten Stufe die Voraussetzungen für eine Übermittlung überhaupt erfüllt und - auf einer zweiten Stufe - die Voraussetzungen speziell für einen Transfer mit Auslandsbezug im jeweiligen Einzelfall gegeben sind. Dabei sind auch angemessene Vorkehrungen zur Datensicherheit zu treffen. Für bereits laufende Datentransfers empfehle ich eine erneute Risikobewertung.

II.

Sicherheitskonzepte zur Datensicherheit in den öffentlichen Stellen in Nordrhein-Westfalen bedürfen (ohnehin) einer regelmäßigen Überprüfung. Daher ist es aktuell naheliegend, bereits bei den hier im Lande von den verantwortlichen und von ihnen beauftragten Stellen vor Ort getroffenen Vorkehrungen zur Datensicherheit anzusetzen und diese einer flächendeckenden und umfangreichen Überprüfung darauf hin zu unterziehen, ob sie gegenwärtig vorstellbaren Gefährdungsszenarien standhalten. Ich empfehle daher, soweit noch nicht geschehen, in eine grundlegende Überprüfung sämtlicher für die Datensicherheit wesentlicher Komponenten einzutreten und im Bedarfsfall gebotene Nachbesserungen vorzunehmen.

III.

Unabhängig von der Frage des Datenzugriffs ausländischer Geheimdienste kann, je nach Ausgestaltung des jeweiligen Datenverarbeitungsprozesses, das Recht auf informationelle Selbstbestimmung bereits dann verletzt sein, wenn öffentliche Stellen zur Erfüllung öffentlicher Aufgaben auf private Diensteanbieter im Netz zurückgreifen und jene Anbieter - aufgrund welcher internen Verarbeitungsprozesse auch immer - personenbezogene Daten der Bürgerinnen und Bürger auch ins außereuropäische Ausland transferieren, ohne dass die Frage der Angemessenheit des Datenschutzniveaus zuvor geprüft worden ist und ohne dass die Bürgerinnen und Bürger von dem Transfer oder von dem Zweck der weiteren Verwendungen ihrer Daten beim Diensteanbieter oder bei Dritten zuvor in Kenntnis gesetzt werden.

So müssen z.B. der Online-Abruf von Informationen bei einer Behörde oder die Online-Kommunikation der Bürger mit der Behörde weiterhin möglich sein, ohne dass die Bürgerinnen und Bürger dafür bei privaten Stellen gleichsam mit ihren Daten bezahlen und über die weitere Verarbeitung ihrer Daten keine Kenntnis haben.

Daher kann ich nur mit Nachdruck dazu raten, z.B. Informations- oder Kommunikationsplattformen für die Bürgerinnen und Bürger oder für einzelne Gruppen, z.B. für Schüler und Lehrer, ausschließlich in eigener, **öffentlicher** Regie zu betreiben. Wegen weiterer Einzelheiten darf ich auf meinen 21. Datenschutz- und Informationsfreiheitsbericht verweisen (dort insbesondere S. 27/28 und 99).

Mit freundlichen Grüßen

./.
(Ulrich Lepper)