



Commission nationale pour la protection des données, 1, avenue du Rock'N'Roll L-4361 Esch-sur-Alzette

Frau [REDACTED]
[REDACTED]
A-1100 Wien

Esch-sur-Alzette, den 15. November 2013

Betrifft : Ihr Antrag auf Einhaltung Ihrer Grundrechte als Nutzer von Microsoft

Sehr geehrte Frau [REDACTED],

Die nationale Kommission für den Datenschutz bezieht sich hiermit auf Ihren Antrag auf Einhaltung Ihrer Grundrechte als Nutzer von Microsoft, hinsichtlich der von der britischen Tageszeitung „The Guardian“ enthüllten möglichen Zusammenarbeit zwischen der Firma Microsoft Luxembourg S.à r.l. (im folgenden „Microsoft Luxembourg“) und der amerikanischen „National Security Agency“ (NSA) im Rahmen des „Prism“ Programms.

Aus Ihrer Anfrage geht hervor, daß Sie von einer Verarbeitung Ihrer Microsoft Daten nicht nur durch Microsoft Luxembourg, sondern von weiteren Auftragverarbeitern innerhalb des Microsoft Konzerns ausgehen, aber auch daß Sie den Verdacht hegen, daß diese Daten durch einen „Massenzugriff“ der NSA auf Microsoft an erstere überlassen werden. Desweiteren bitten Sie uns auch um eine Überprüfung der Rechtskonformität des „Safe Harbor“. Ihr Antrag ist gemäß Artikel 32 Abschnitt 2 Buchstabe a) des abgeänderten Gesetzes vom 2. August 2002 zum Schutz personenbezogener Daten bei der Datenverarbeitung demnach zulässig, da sich Ihr Antrag auf die Einhaltung ihrer Grundrechte und Freiheiten in Bezug auf eine Datenverarbeitung bezieht. Unsere Behörde hat demnach den angesprochenen Hotmail (bzw live.com/outlook.com) und die angegliederten Dienste von Microsoft eingehend überprüft, durch Vor-Ort-Kontrollen sowie durch Hinterfragungen von zusätzlichen juristischen und technischen Aspekten.

Da obengenannte Microsoft Firma ihren Sitz in Luxemburg hat, ist gemäß Artikel 3 Abschnitt 2 Buchstabe a) des Gesetzes, welches Artikel 4 Abschnitt 1 Buchstabe a) der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr umsetzt, das luxemburgische Recht auf alle Verarbeitungen personenbezogener Daten durch besagte Firma anwendbar, die im Rahmen ihrer Tätigkeiten in Luxemburg ausgeführt werden.

Auf Ihren Antrag hin haben wir uns die Rolle von Microsoft Luxemburg bei der Datenverarbeitung innerhalb der komplexen Infrastruktur des Microsoft Konzerns überprüft. Unseren Erkenntnissen zufolge, sowie angesichts den von Microsoft Luxemburg an uns formell erklärten Informationen ergibt sich, daß Microsoft Luxembourg die Gesellschaft ist, welche vertraglich als Anbieterin der Online Dienste für die Europäischen Nutzer gilt und sich diesbezüglich gemäß des Microsoft Services Agreement (Dienste wie Outlook.com, SkyDrive usw.) rechtlich verpflichtet. Sie ist demnach die verantwortliche Stelle für die personenbezogenen Daten im Rahmen dieser Dienste.

Sie werfen desweiteren die Frage auf, ob Ihre Microsoft Daten überhaupt in die USA (vor allem an Microsoft Corporation USA) übermittelt werden können. Eine solche Übermittlung muß vor allem zulässig im Sinne von Artikel 5 des luxemburgischen Datenschutzgesetzes sein, d.h. daß sie eine der im Gesetz aufgeführten Bedingungen erfüllen muß. Im Falle von Microsoft ist eine solche Übermittlung *„erforderlich für die Ausführung eines Vertrages, an dem die betroffene Person beteiligt ist“* (Artikel 5 Abschnitt 1 Buchstabe c) des Datenschutzgesetzes welches Artikel 7 Buchstabe b) der Richtlinie 95/46/EG entspricht).

Auch erfolgt unserer Meinung nach die Übermittlung durch Microsoft nach Treu und Glauben und auf rechtmäßige Weise, da der Nutzer unmißverständlich in den Microsoft Datenschutzrichtlinien darauf hingewiesen wird (*„Microsoft Online Privacy Statement“* : *“die über Microsoft-Websites und -Dienste erfassten persönlichen Daten können in den USA sowie in jedem anderen Land gespeichert und verarbeitet werden, in dem Microsoft oder ein verbundenes Unternehmen, seine Niederlassungen oder seine Dienstanbieter Einrichtungen unterhalten“*)¹) und da besagter Nutzer diesen Richtlinien auch zustimmen muß und somit sein Einverständnis gegeben hat sobald er die Microsoft Dienste benutzt.

Hat Microsoft in Luxemburg die vom Datenschutzgesetz vorgeschriebenen Formalitäten ohnehin erfüllt, wird eine Verarbeitung der Microsoft Nutzerdaten durch Microsoft Corporation, vor allem bei Gebrauch der globalen Onlinedienste wie Hotmail, welche eine internationale Übermittlung der Daten erfordern, von unserer Behörde also nicht als unlaut angesehen.

Was die Weitergabe von Nutzerdaten an Drittländer angeht, kann eine solche Übertragung von personenbezogenen Informationen gemäß der Richtlinie 95/46/EG außerhalb der europäischen Union durch einen für die Verarbeitung verantwortliche Stelle nur dann durchgeführt werden, wenn das Land des Empfängers als ein Land anerkannt worden ist, das einen angemessenen Schutz gewährleistet.

Im spezifischen Fall von Microsoft Luxemburg (als Tochterunternehmen von Microsoft Corporation) steht fest, daß besagtes Mutterhaus in den USA dem „Safe Harbor“ beigetreten ist, welches den Schutz personenbezogener Daten beim Transfer aus der EU in die USA sicherstellen soll (*“Microsoft Corporation and its Controlled U.S. Subsidiaries“* Zertifikat vom 29. Juni 2001).

„Safe Harbor“ erhielt mit der Kommissionsentscheidung 2000/520/EG vom 26. Juli 2000 [gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA]

¹ <http://privacy.microsoft.com/en-gb/fullnotice.mspx>

rechtliche Gültigkeit. Den Datenverarbeitungen der Unternehmen, die sich dem Safe Harbor anschließen, wird dann ein angemessenes Schutzniveau eingeräumt.

Die in Luxemburg für die Verarbeitung verantwortliche Stelle muß gemäß Artikel 18 Abschnitt 2 des luxemburgischen Datenschutzgesetzes sicherstellen, daß der Empfänger der Daten (im Drittland) ein angemessenes Schutzniveau für die übermittelten Daten bietet. Hat sich dieser (US) Empfänger dem „Safe Harbor“ verpflichtet, erlaubt die Angemessenheitsentscheidung der Kommission gemäß Artikel 25. Abschnitt 6 der Richtlinie ohne weiteres eine Übermittlung der Daten in dieses Land. „Safe Harbor“ ermöglicht es demnach rechtlich zulässig personenbezogene Daten aus der EU in die USA zu exportieren.

Microsoft Luxemburg leitet nach diesem Prinzip in Europa gesammelten Nutzerdaten an Microsoft Corporation in die USA weiter, so wie es auch in dessen Onlinedatenschutzbestimmungen vorgesehen ist [(„Microsoft hält sich in Bezug auf die Erfassung, Verwendung und Speicherung von Daten aus dem Europäischen Wirtschaftsraum und der Schweiz an die Bestimmungen des amerikanischen Handelsministeriums (Safe Harbor)“].²

Microsoft hat nach den diversen Veröffentlichungen vom *“The Guardian”* angegeben daß : *„We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the [American] government has a broader voluntary national security program to gather customer data we don't participate in it.“*³

Dies wiederum ist im Einklang mit Microsofts Datenschutzrichtlinie, welche besagt daß: *„Microsoft kann zu folgenden Zwecken persönliche Informationen teilen oder offenlegen, einschließlich der Inhalte Ihrer Nachrichten“, sowie „um dem Gesetz nachzukommen, im Rahmen eines Prozesses zu erwidern oder legale Forderungen zu erfüllen, wie etwa von Strafverfolgungsbehörden und staatlichen Organisationen.“*⁴

Microsoft Luxemburg hat unserer Datenschutzbehörde formell zugesichert daß :

- *“Neither Microsoft Luxembourg nor its U.S.-based parent company Microsoft Corp. (collectively, “Microsoft”) has granted the U.S. National Security Agency mass access to customer data. Until it was reported by the media, Microsoft did not have any knowledge of PRISM ;*
- *As noted above, Microsoft did not have any knowledge of PRISM until it was reported in the media. Microsoft is obligated to comply with applicable law. Except as described below, Microsoft only discloses customer data in response to valid legal demands, and even then, we only comply with legal demands for information about specific accounts or identifiers ;*
- *In the ordinary course of events, Microsoft only responds to legal government demands (order or subpoenas) pursuant to applicable local law, and we only comply with orders for requests about specific*

² <http://privacy.microsoft.com/DE-DE/fullnotice.msp>

³ <http://www.microsoft.com/en-us/news/press/2013/jun13/06-06statement.aspx>

⁴ <http://www.microsoft.com/privacystatement/de-de/core/default.aspx?Componentid=pspOtherInformationModule&View=Description>

accounts or identifiers. Microsoft may, in limited circumstances, disclose customer data to criminal law enforcement agencies where we believe the disclosure is necessary to prevent an emergency involving danger of death or serious physical injury to a person. Microsoft requires that law enforcement agencies submit emergency requests in writing on official letterhead, and signed by a law enforcement authority. The request must contain a summary of the emergency, along with an explanation of how the information sought will assist law enforcement in addressing the emergency. Each request is carefully evaluated by Microsoft Global Criminal Compliance team before any data is disclosed, and the disclosure is limited to the data that we believe would enable law enforcement to address the emergency.”

Microsoft streitet also ausdrücklich ab, der NSA Zugriff auf ihren gesamten Datenbestand zwecks einer Massenauswertung zu gewähren. Microsoft versichert, daß nur erhebliche individualisierte Daten im Einzelfall übermittelt werden.

Desweiteren hat Microsoft Corporation, ungeachtet der möglichen Anwendung des sogenannten „Gag Orders“, in ihrer Pressemitteilung vom 11. Juli 2013 („*Responding to government legal demands for customer data*“⁵), folgende Aussage gemacht : „ *we only ever comply with orders about specific accounts or identifiers, and we would not respond to the kind of blanket orders discussed in the press over the past few weeks, as the volumes documented in our most recent disclosure clearly illustrate. To be clear, Microsoft does not provide any government with blanket or direct access to SkyDrive, Outlook.com, Skype or any Microsoft product*“. Auch kürzlich, am 27. September 2013, hat Microsoft Corporation ihren „*January-June 2013 Law Enforcement Requests Report*“ veröffentlicht, welcher die genaue Zahl von Anfragen (Anforderungen für Daten in Bezug auf alle Microsoft Online- und Cloud-Services, darunter Skype) weltweiter Strafverfolgungsbehörden umfaßt, und wie Microsoft dementsprechend auf diese Anforderungen reagiert hat.

Hinzu kommt daß auch die Bestimmungen des „Safe Harbor“ es den US-Firmen ermöglichen, die Daten an Ihre Behörden weiterzuleiten : „*Die Geltung dieser [Safe Harbor] Grundsätze kann begrenzt werden a) insoweit, als Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Rechnung getragen werden muss, b) durch Gesetzesrecht, staatliche Regulierungsvorschriften oder Fallrecht, die unvereinbare Verpflichtungen oder ausdrückliche Ermächtigungen schaffen, vorausgesetzt, die Organisation kann in Wahrnehmung dieser Ermächtigungen nachweisen, dass die Nichteinhaltung der Grundsätze sich auf das Ausmaß beschränkte, das die Einhaltung übergeordneter berechtigter Interessen aufgrund eben dieser Ermächtigung erforderte (...)*“.⁶

Den Erkenntnissen unserer Behörde zufolge liegen uns demnach keine konkreten Elemente eines Verstoßes gegen das Luxemburgische Datenschutzgesetz vor, weder bei der Verarbeitung der Daten noch bei der Übermittlung dieser Daten, die man Microsoft Luxemburg nach Luxemburgischen Recht vorwerfen könnte.

Es konnte also in keinster Weise eine aktive Verwicklung von Microsoft in Luxemburg an einer Massenübermittlung („freiwillige Zusammenarbeit“) an die

⁵ <http://www.microsoft.com/en-us/news/press/2013/jul13/07-11statement.aspx>

⁶ eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF

NSA nachgewiesen werden. Desweiteren gibt es keinerlei Hinweise, daß deren Geschäftsführer Kenntnis hatten von einer solchen Übermittlung. Wurden die Daten einmal (rechtmäßig) an Microsoft Corporation übermittelt, ist unsere Behörde rechtlich nicht mehr zuständig um zu überprüfen, ob auf US-amerikanischen Staatsgebiet diese Daten, rechtmäßig oder nicht, weitervermittelt werden.

Es sei auch daran erinnert, daß der Angemessenheitsbeschuß der europäischen Kommission bezüglich des „Safe Harbor“ geltendes Recht in Luxemburg ist und die Datenübertragungen zu den beigetretenen Unternehmen weiterhin per se zulässig sind, es sei denn, die Europäische Kommission unterzieht diese Entscheidung einer Revision. Wir nehmen allerdings zur Kenntnis, daß die EU eine Arbeitsgruppe von der EU-Kommission mit Prüfung des „Safe Harbor“ Abkommens angesichts der heutigen technologischen Entwicklung und neuer Risiken für die Privatsphäre beauftragt hat.

Hinsichtlich Ihrer Vermutung, ob Ihre eigenen Daten seitens Microsoft Luxemburg an staatliche Sicherheits- oder Polizeibehörden einschließlich Nachrichtendienste weitergeleitet oder überlassen worden sind, können wir Ihnen mitteilen, daß Ihr Hotmail Konto ([REDACTED]) oder Ihre Microsoft Daten nach Wissen von Microsoft nie Gegenstand oder Ziel einer staatlichen Nachfrage unter irgendeiner Gerichtsbarkeit oder einer sonst uns bekannten Überwachung wurden. In diesem Sinne wurde uns von von Microsoft Luxemburg ausdrücklich zugesichert daß : *„We want to report that Microsoft Corp.'s investigation into [REDACTED] Hotmail account revealed her account has never, to Microsoft Corp.'s knowledge, been the subject or target of any government demand or legally authorized surveillance. As such, Microsoft Corp. has not pulled or produced her personal data to any governmental entity in any jurisdiction.“*

Abschließend möchten wir bemerken, daß unsere Behörde die Bemühungen der EU-Kommission und des Parlaments zur genaueren Aufklärung der von Ihnen angesprochenen angeblichen Überwachungsvorgänge der Geheimdienste im Internet begrüßt, welche wir auch weiterhin mit höchster Aufmerksamkeit verfolgen werden. Auch die Artikel-29 Arbeitsgruppe der europäischen Datenschutzbehörden wird ihren Beitrag zur Bewertung des eventuellen Handlungsbedarf in den kommenden Monaten leisten.

Mit freundlichen Grüßen,

Für die nationale Kommission für den Datenschutz,



Gérard Lommel
Vorsitzender



Thierry Lallemand
Ordentliches Mitglied



Marc Hemmerling
Ersatzmitglied

