

**Empfehlung
zum Datenschutz und Elektronik-Abfall („E-Waste“)**

45. Sitzung, 12.-13. März 2009, Sofia (Bulgarien)

-Übersetzung-

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation,

Berücksichtigend, dass die zunehmende und umfassende Nutzung elektronischer Geräte und Anlagen sowohl für private als auch für öffentliche Zwecke die Notwendigkeit mit sich bringt, solche Einrichtungen auch angemessen zu entsorgen und/oder zu recyceln;

Berücksichtigend, dass solche elektronischen Geräte und Anlagen Einrichtungen zur Kommunikation enthalten und in Anbetracht der zunehmenden technischen Konvergenz und des Vorhandenseins von Mehrzweckgeräten¹;

Berücksichtigend, dass die Europäische Union seit langem eine umweltfreundliche Politik verfolgt, die die Verminderung der Ausbeutung natürlicher Rohstoffe sowie Maßnahmen zur Verminderung der Verschmutzung umfasst; und berücksichtigend, dass solche Ziele auch seit langem in verschiedenen Nicht-EU-Staaten verfolgt werden;

Berücksichtigend, dass die angesprochenen Strategien angemessene Recycling- und Abfallbeseitigungsmaßnahmen in Bezug auf Elektro- und Elektronikabfall (E-Waste) vorsehen, wie sie mit der EG der Richtlinie 2002/96/EG² auf den Weg gebracht wurden;

Berücksichtigend, dass es einschlägigen regulatorischen Instrumenten bisher weder auf nationaler noch auf überstaatlicher Ebene gelungen ist, den Risiken, die mit dem Recycling oder der Beseitigung von Elektro- und Elektronik-Geräten insoweit einhergehen, dass solche Geräte persönliche Daten über den Nutzer des Geräts oder Dritte enthalten können, hinreichend Rechnung zu tragen;

¹ Abgesehen von und über solche Geräte und Ausstattungen hinaus, die ursprünglich für Kommunikationszwecke bestimmt waren, gibt es eine zunehmende Anzahl an Geräten, die als Datenübertragungsendgerät eingesetzt werden können, wenn sie an ein elektronisches Kommunikationsnetzwerk angeschlossen sind.

² Richtlinie 2002/96/EG des Europäischen Parlaments und des Rates vom 27. Januar 2003 über Elektro- und Elektronik-Altgeräte.

Berücksichtigend, dass es notwendig ist, die Aufmerksamkeit aller Interessenvertreter - sei es im öffentlichen oder im privaten Bereich - inklusive solcher staatlichen Stellen und Firmen, die die E-Waste recyceln oder verwerten, auf dieses Thema zu lenken, insbesondere insoweit, als dass diese Stellen, vor allem diejenigen, die sich selbst Kommunikationsgeräte und -Ausstattungen zunutze machen, als datenverarbeitende Stellen verpflichtet sind, angemessene Maßnahmen zu ergreifen, um die Sicherheit persönlicher Daten zu gewährleisten, wobei diese Maßnahmen zum Zeitpunkt des Recyclens und/oder des Beseitigens derjenigen Geräte und Ausstattungen, die zur Verarbeitung persönlicher Daten eingesetzt wurden, durchgeführt werden müssen;

Unter Bezugnahme auf generelle bestehende Leitlinien, wie sie von manchen nationalen Datenschutzbehörden in Verbindung mit der angemessenen Vernichtung und/oder Löschung von persönlichen Daten aufgestellt wurden³;

EMPFIEHLT

1. Dass die nationalen Regulierungsbehörden, in Zusammenarbeit mit den nationalen Datenschutzbehörden und allen relevanten Interessenvertretern aus der Industrie, angemessene Maßnahmen auf den Weg bringen, die den unberechtigten Zugang zu persönlichen Daten, die in zu recycelnden und/oder zu verwertenden Geräten gespeichert sind, verhindern oder begrenzen. Darüber hinaus muss sichergestellt werden, dass die entsprechenden Maßnahmen auch von den datenverarbeitenden Stellen umgesetzt werden. Solche Maßnahmen könnten zum Inhalt haben, dass Informationstechnik und/oder andere Werkzeuge und/oder Vorkehrungen - soweit als möglich als Freeware (kostenlose und lizenzfreie Software) - bereitgestellt werden,

³ Vgl. z.B.: Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe "Sicheres Löschen magnetischer Datenträger". Grundlagen, Werkzeuge und Empfehlungen aus Sicht des Datenschutzes, Stand: 7.10.2004 (<http://www.datenschutz.mvnet.de/dschutz/informat/magloe/magloe.html>); Orientierungshilfe "Datensicherheit bei USB-Geräten", Stand: November 2003 (http://www.datenschutz.mvnet.de/dschutz/informat/usb/oh_dsusb.html); Hellenic Republic Data Protection Authority, Directive 1/2005, Athens 17-10-2005, Ref. Num. 3845; Entscheidung der Italienischen Datenschutzbehörde vom 9. Dezember 2008, abrufbar unter: <http://www.garanteprivacy.it/garante/doc.jsp?ID=1583482>; siehe auch: Pressemitteilungen des Berliner Beauftragten für den Datenschutz und die Informationsfreiheit vom 24. Januar 2007 (<http://www.datenschutz-berlin.de/content/nachrichten/pressemitteilungen/pressemitteilungen-im-jahr-2007>) und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 23. Dezember 2008 (http://www.bfdi.bund.de/cln_136/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2008/PM_37_08_KeinePersoenlichenDatenAufAusrangiertenPCsVergessen.html?nn=409394).

um die Speicherung personenbezogener Daten in den entsprechenden Geräten zu begrenzen oder zu verhindern, da es sich als schwierig erweisen wird, solche Daten zu entfernen, ohne das betreffende Gerät und/oder Equipment zu zerstören⁴;

2. Dass die Maßnahmen zum Schutz personenbezogener Daten, die von den datenverarbeitenden Stellen zu ergreifen sind, den unterschiedlichen Risiken Beachtung schenken, die mit Recyclingprozessen im Gegensatz zu Abfallbeseitigungsmaßnahmen von Elektronik-Abfall einhergehen.
3. Dass mit der Einführung von Maßnahmen zum Schutz persönlicher Daten in Verbindung mit dem Recycling von Elektronik-Abfall insbesondere sichergestellt werden muss, dass die personenbezogenen Daten von magnetischen und elektronischen Medien unter Einhaltung des gegenwärtigen Stands der Technik, wie zum Beispiel durch mehrfaches Überschreiben oder Entmagnetisierung (degaussing), gelöscht werden;
4. Dass bei der Einführung von Maßnahmen zum Schutz personenbezogener Daten in Verbindung mit dem Recycling von Elektronik-Abfall die Zweckmäßigkeit der Implementierung effektiver Mechanismen zur Zerstörung magnetischer und elektronischer Medien berücksichtigt werden soll, um den unberechtigten Zugriff auf personenbezogene Daten zu verhindern;
5. Dass die zuständigen nationalen und supranationalen Stellen angemessene Aufklärungsmaßnahmen ergreifen, um die datenverarbeitenden Stellen und die Nutzer über die einschlägigen Risiken und Anforderungen zu informieren.

⁴ In dieser Hinsicht kann auf herausnehmbare Speicherkarten verwiesen werden, wie sie in Mobiltelefonen eingesetzt werden.