Bundesministerium
des Innern

Bundesministerium des Innern, 11014 Berlin

[redacted]

HAUSANSCHRIFT
Alt-Moabit 101 D
10559 Berlin

POSTANSCHRIFT
11014 Berlin

TEL +49(0)30 18 681-1519
FAX +49(0)30 18 681-55038

ZI4@bmi.bund.de
www.bmi.bund.de

Betreff: Informationsfreiheitsgesetz
hier: Handlungs- und Dienstanweisungen zur Nutzung von Verschlüsselungstechniken im BMI. (z.B. zu Kryptophones, PGP, GNUPG, Gpg4win, S/MIME)

Bezug: Ihr Antrag vom 16. Januar 2015
Aktenzeichen: ZI4-13002/4#516
Berlin, 29. Januar 2015

Anlage: - 1 -

Sehr geehrt[redacted]

mit E-Mail vom 21. Januar 2015 beantragen Sie auf Grundlage des Informationsfreiheitsgesetzes (IFG) die Übersendung von Handlungs- und Dienstanweisungen zur Nutzung von Verschlüsselungstechniken im BMI (z.B. zu Kryptophones, PGP, GNUPG, Gpg4win, S/MIME).

Generelle Handlungsanweisungen zur Nutzung von Verschlüsselungstechniken gibt es nur in Form einzelner Absätze in der IT-Sicherheitsrichtlinie (Hausanordnung Gruppe 3 Blatt 4.1). Dort ist im Absatz 4.4 der "Umgang mit mobiler Informationstechnik" beschrieben:

> *"Mobile IT-Geräte (Laptop, MDA etc.) sind grundsätzlich verschlossen aufzubewahren. Ausgehändigte Schlüsselmittel (z.B. USB-Token für Laptops) sind hiervon getrennt verschlossen aufzubewahren.*
> *Bei Verlust eines mobilen IT-Geräts ist unverzüglich der Benutzerservice zu informieren. Außerhalb der Servicezeiten ist das Referat Z II 1 über das Lagezentrum zu informieren. Bei einem Diebstahl ist zusätzlich Anzeige bei einer*

Polizeidienststelle zu erstatten. Sofern Schlüsselmittel (z.B. Zertifikate auf MDAs, USB-Token für Laptops) von dem Verlust (mit-)betroffen sind, ist das Zertifikat über die RA-Stellen (Registration Authorities) im Referat Z II 3 (Innerer Dienst; Bibliothek; Sicherheitsbeauftragter des BMI) oder durch den Nutzer selbst unter Verwendung des bei der Zertifikatsausstellung festgelegten Sperrkennworts gegenüber der Zertifizierungsstelle zu sperren.
Bei Verlust eines dienstlich zur Verfügung gestellten Mobiltelefons ist unmittelbar der Benutzerservice zu informieren. Außerhalb der Servicezeiten ist das Referat Z II 1 über das Lagezentrum zu informieren. Die notwendige Sperrung der SIM-Karte wird durch das Referat Z II 1 beim Mobilfunkprovider veranlasst.
Mobiltelefone verfügen systembedingt nur über schwache Sicherheitsmechanismen. Sensible Informationen, insbesondere VS-Daten, Personalaktendaten oder „besondere Arten" personenbezogener Daten (siehe Ziffer 4.3.3) dürfen grundsätzlich weder auf dem Gerät selbst, noch auf einer damit verwendeten Erweiterungskarte (z.B. SD-Card) gespeichert oder - etwa per Kurznachrichten (SMS) - verarbeitet und versandt werden. Der Austausch von Daten mit einer Einstufung bis VS-NfD zwischen Kryptohandys (siehe Ziffer 2.2 und Ziffer 4.7) ist mit entsprechender Verschlüsselung zulässig."

Eine weitergehende Beschreibung, wie mit der Hardware und der Verschlüsselungstechnik umzugehen ist, existiert nur für die Kryptohandys (Blackberry-Geräte) und ist als Anlage beigefügt. Der Umgang mit Laptops bzw. den zugelassenen USB-Sticks erfolgt nur mit mündlicher Einweisung, hierfür existieren keine schriftlichen Anweisungen. Der Nutzer bestätigt jedoch durch Unterschrift die geltenden Regelungen, einschließlich der Einhaltung der o.g. Hausanordnung.

Ich hoffe, Ihnen hiermit geholfen zu haben.

Mit freundlichen Grüßen
Im Auftrag
[redacted]
Menz