

An die
Präsidentin des Nationalrats
Mag^a Barbara PRAMMER
Parlament
1017 W i e n

GZ: BKA-353.110/0069-I/4/2014

Wien, am 27. Mai 2014

Sehr geehrte Frau Präsidentin!

Die Abgeordneten zum Nationalrat Ertlschweiger, MSc, Kolleginnen und Kollegen haben am 27. März 2014 unter der **Nr. 1159/J** an mich eine schriftliche parlamentarische Anfrage betreffend Datenmissbrauch durch Anwenderprogramme (Apps) auf Smartphones gerichtet.

Diese Anfrage beantworte ich wie folgt:

Zu den Fragen 1 und 3:

- *Ist Ihnen bzw. Ihrem Ressort die oben angeführte Studie bekannt?
Wenn ja, welche Erkenntnisse, Überlegungen und Maßnahmen wurden/werden von Ihres Ressorts aus dieser Untersuchung gewonnen?*
- *Gibt es von Seiten Ihres Ressorts Untersuchungen zur Risikoabschätzung und Risikobewertung hinsichtlich des potentiellen Datenmissbrauchs bei Installation und Anwendung von Apps auf mobilen elektronischen Geräten?
a) Wenn ja, welche Ergebnisse brachte diese Untersuchung?
b) Wenn nein, werden Sie solche in Auftrag geben?*

Diese Studie ist der zuständigen Sektion bekannt. Die Schlussfolgerungen dieser Studie hatten keinen wesentlichen Einfluss auf die IKT-Sicherheitsüberlegungen des Bundeskanzleramtes. Bereits seit Jahren wird im Bundeskanzleramt eine eigene Smartphone-Infrastruktur betrieben, welche eine sehr granulare Konfiguration der Smartphone-Apps ermöglicht. Vor dem Einsatz im behördlichen Kontext wird eine App auf die Funktionalität überprüft und mit Sicherheitselementen ausgestattet.

Zu Frage 2:

- *Gibt es von Seiten Ihres Ressorts Untersuchungen bzw. Erhebungen, die einen Überblick über Mobile Apps, die unbemerkt die Daten ihrer Nutzer sammeln, möglich machen?*
 - a) *Wenn ja, welche Ergebnisse erbrachten diese Untersuchungen und wo sind diese einsehbar?*
 - b) *Wenn nein, werden Sie eine solche in Auftrag geben?*

Das Bundeskanzleramt erhebt keine Information über die Sammeleigenschaften von Apps. Es ist auch nicht geplant, einen Auftrag dazu zu vergeben.

Zu den Fragen 4 und 5:

- *Erachten Sie die bestehenden Regelungen zum Schutz der Konsumenten vor Datenmissbrauch durch Anwendungsprogramme auf mobilen elektronischen Geräten für ausreichend?*
Wenn nein, welche Maßnahmen zur Verbesserung der Situation wurden bzw. werden von Ihnen getroffen?
- *Welche rechtlichen Möglichkeiten sehen Sie, um die unerlaubte bzw. unerkannte Weitergabe von Handy-Daten einzuschränken bzw. völlig zu unterbinden?*

Soweit Handy-Daten „unerlaubt“, d.h. entgegen rechtlicher Verbotsnormen weitergegeben werden, kommt nur eine nachträgliche Sanktionierung im Falle der Aufdeckung in Frage. Diesbezüglich verweise ich auf die einschlägigen Strafbestimmungen des DSG 2000 (§§ 51 ff). Die allfällige „unerkannte“ Weitergabe von Handy-Daten spricht die Frage der Transparenz gegenüber den Betroffenen an. Grundsätzlich sind Auftraggeber, d.h. insbesondere Anbieter von Kommunikationsdienstleistungen sowie Internetdiensteanbieter schon nach dem DSG 2000 (§ 24) zu einer ausreichenden Information verpflichtet. Hier stellt sich primär die Frage der effektiven Verfolgung mangelhafter Informationstätigkeit durch die Aufsichtsbehörde bzw. – bei nachteiligen Folgen im Nachhinein – durch Betroffene vor Zivilgerichten. Die völlige Einschränkung bzw. Unterbindung solcher unerkannten Weitergaben kann insofern nicht unmittelbar mittels einer legitimen Maßnahme bewerkstelligt werden, sondern hängt vom entsprechenden Bewusstsein und der sozialen Interaktion aller Beteiligten ab.

Zu Frage 6:

- *Welche Möglichkeiten nutzt Ihr Ressort, um auf die Gefahren von Handy-Apps hinsichtlich der persönlichen Datensicherheit der User, unter besonderer Berücksichtigung der Gruppe der Jugendlichen, hinzuweisen bzw. konkret zu informieren?*

Im Rahmen der Cyber Security-Aktivitäten betreibt das Bundeskanzleramt gemeinsam mit dem Bundesministerium für Finanzen das Web-Portal onlinesicherheit.gv.at. Dieses Portal bietet Benutzern die Möglichkeit, sich über das Thema Datensicherheit auf mobilen Endgeräten zu informieren.

Zu Frage 7:

- *Welche Möglichkeiten sehen Sie, um dem beschriebenen Gefahrenpotential auf EU bzw. internationaler Ebene zu begegnen?*
- Welche diesbezügliche Maßnahmen, Vorhaben bzw. Veranlassungen sind Ihrem Ressort dazu bekannt?*
 - An welchen von diesen ist Österreich aktiv in welcher Form beteiligt?*
 - Welche Ergebnisse hat dieses Engagement bisher gebracht?*

Das Bundeskanzleramt ist bestrebt, im Rahmen seiner Beteiligung am Rechtsetzungsverfahren im EU-Rat betreffend die Datenschutz-Grundverordnung auf eine klare Regelungen hinzuwirken, welche die Informationsmindestfordernisse für Auftraggeber insbesondere auf dem Feld der Internetdienste so definiert, dass eine wirksame Anwendung in der künftigen Praxis erwartbar ist. Die Einzelheiten dieser Transparenzanforderungen sind sich nach wie vor im Stadium der Diskussion.

Mit freundlichen Grüßen

FAYMANN

	1001ABXXECP-AuftragserfassungWnl/aIDpROrOXiZR4U6R WrRzYKcbH7DV/SMRhLl85LCbpAzYekuFWzBFhlo3hK8jbS6mREbd8F2XlniRFLcilGK l9knaogcizWnsBEJqHcrrCPTCUD83hZOhiohAcPvl/NNcVlijF3zklbb8pfBq7NjedD uWzgnn9N2J0xEa9Bw3x3zvHEwcEsl8Z4fDF57BGkE9/dE2lFMrSjGBGiMUu9lKhodmb ruHUhDlz4BGZKu+zYHi6WIjtDIWRsm3u7/Qd2ORVnHUNtJ5um0s8iz0X9oJ9LFQwE0w DJC947w==	
	Unterzeichner	serialNumber=812559419344,CN=Bundeskanzleramt,C=AT
	Datum/Zeit-UTC	2014-05-27T12:23:35+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	1026761
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bka.gv.at/verifizierung	