

Ing. Dr. iur. Eike Wolf

Kommentar zum Polizeilichen Staatsschutzgesetz (PStSG)

Dass der polizeiliche Staatsschutz auf eine solide rechtliche Basis zu stellen ist, steht außer Zweifel. Der Entwurf ist allerdings mit zu vielen Unbestimmtheiten (absichtlich?) ausgestaltet, die weit mehr der Überwachung der Bürger dienen als ihre Freiheit schützen. Warum die Regierung und im Besonderen das BMI die Überwachung der Freiheit der Bürger vorzieht, ist nicht verständlich. Das BMI drückt damit eine offensichtliche Hilflosigkeit aus, die es durch intensivere Überwachung verdecken und kompensieren will. Denn die meisten Bestimmungen sind so unbestimmt abgefasst, dass der Sicherheitsbeamte im Verfassungsdienst sich nicht mehr den Kopf darüber zerbrechen muss, ob eine Überwachungsmaßnahme noch verhältnismäßig und gerechtfertigt ist. Bei dieser unbestimmten Rechtslage ist seine Entscheidung immer verhältnismäßig und gerechtfertigt.

Dabei wird aber völlig ignoriert, dass der Staat auf Grund der Verfassung und der zwar oft zitierten EMRK aber deren fast immer unbeachteten Geist und auch anderer verfassungsrechtlichen Nebengesetzen, die staatliche Verwaltung die Freiheit der Bürger genauso zu schützen hat, wie deren Sicherheit.

Der Entwurf vernachlässigt auch einige grundlegende psychologische Eigenschaften des Menschen und damit auch der Sicherheitsbeamten. Je mehr Material aus Ermittlungsergebnissen man zur Verfügung hat, das aber immer unvollständig ist, umso leichter fällt man auch ein Vorurteil auf Grund der Interpretation des Ermittlungsmaterials. Dabei sollte die Behörde auf Grund vergangener Ermittlungsergebnisse und deren Fehlinterpretation bereits gewarnt sein.

Durch die Aufnahme von Ermittlungsmaßnahmen durch die Sicherheitspolizei oder dieser gleichgestellten Verfassungsschutz wird ein Verfahren begonnen, das gemäß Art 6 EMRK (Verfassungsrang) fair ablaufen soll und für das gemäß Art 6 Abs 2 der Betroffene als unschuldig zu gelten hat, bis zum gesetzlichen Nachweis seiner Schuld. Durch diesen Entwurf würde dieses Verfahren nicht mehr fair sein und außerdem die Unschuldsvermutung dauernd verletzt. Es wird nämlich in keiner Bestimmung auch nur erwähnt, dass auch zu Gunsten des Betroffenen Ermittlungsmaßnahmen zu setzen sind. Die Objektivität des Verfassungsdienstes ist damit grundlegend verletzt.

Somit enthält der vorliegende Entwurf viele gravierende Mängel und Unbestimmtheiten und Ungereimtheiten, die im Folgenden aufgezeigt werden. In der vorgeschlagenen Form ist der Entwurf jedenfalls abzulehnen.

Zu §2 des Entwurfs:

Warum ist zu den Landesämtern keine Leitung und keine Geschäftsordnung festgelegt? Wer bestimmt diese? Da auf Grund Art 10 Abs 1 Z6 der „Staatsschutz“, Z7 und Z14 die Kompetenz dem Bund zugeordnet ist, müsste der Entwurf auch die Leitung und Organisation und die Geschäftsordnung der Landesämter regeln.

Ing. Dr. iur. Eike Wolf

Zu §4 des Entwurfs:

Um Lesbarkeit der Paragraphen mit der Zitierung einer Vielzahl von Gesetzesstellen aus anderen Gesetzen zu erhöhen, wird vorgeschlagen, dass jeweils nach der Anführung eines Paragraphen eines fremden Gesetzes auch in Klammer die kurze Inhaltsangabe angeführt wird, zB

„1. Operative Koordinierungsstelle für jede Form von Angriffen auf Computersysteme von verfassungsmäßigen Einrichtungen (§ 22 Abs. 1 Z 2 SPG, *Vorbeugender Schutz von verfassungsmäßigen Einrichtungen*) sowie kritischen Infrastrukturen (§ 22 Abs. 1 Z 6 SPG, *Vorbeugender Schutz von kritischen Infrastrukturen*) nach den §§ 118a (*Widerrechtlicher Zugriff auf ein Computersystem*), 119 (*Verletzung des Telekommunikationsgeheimnisses*), 119a (*Missbräuchliches Abfangen von Daten*), 126a (*Datenbeschädigung*), 126b (*Störung der Funktionsfähigkeit eines Computersystems*) und 126c (*Missbrauch von Computerprogrammen oder Zugangsdaten*) Strafgesetzbuch (StGB), BGBl. Nr. 60/1974;“

Diesen Vorschlag hat bereits *Schönherr*, Sprache und Recht, 1985, Regel 19, S14 gemacht, um das lästige Nachschlagen oder Aufsuchen der genannten Bestimmungen zu vermeiden. Dieses Büchlein ist sicher in der Amtsbibliothek vorhanden und ist für die Verfassung von legislativen Vorhaben dringend zu empfehlen.

Völlig unbestimmt sind jedoch die verfassungsmäßigen Einrichtungen. Der Verweis auf §22 Abs 1 Z2 geht ins Leere, weil dort auch nur die „verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit“ genannt werden. Daher wäre es dringend notwendig, diese zu definieren.

Zu §5 des Entwurfs:

Dass das SPG gilt, ist ja evident. Gemeint ist wohl, dass es immer dann anzuwenden ist, wenn das PStSG nichts Abweichendes festlegt. Sprachlich schöner und deutlicher wäre daher die folgende Formulierung:

„§5. *Soweit dieses Bundesgesetz nicht Abweichendes bestimmt, ist das Sicherheitspolizeigesetz anzuwenden.*“

Es ist jedoch völlig offen, welchen Kompetenzumfang der Staatsschutzbeamte hat, den erweiterten gemäß §12 Abs 1 PStSG oder nur den des SPG. Diese Unbestimmtheit ist gemäß Art 18 B-VG verfassungswidrig.

Zu §6 des Entwurfs:

Um Lesbarkeit dieses Paragraphen mit der Zitierung einer Vielzahl von Gesetzesstellen aus anderen Gesetzen zu erhöhen wird wie zu §4 vorgeschlagen in Klammer ein knappe Inhaltsangabe des zitierten Gesetzes einzufügen. Darüber hinaus ist der „*vorbeugende Schutz vor wahrscheinlichen Angriffen*“ ein sprachlicher Pleonasmus, weil der „Schutz vor“ bereits die Vorbeugung enthält.

Ing. Dr. iur. Eike Wolf

Es ist weiters nicht nachvollziehbar, warum die Störung einer Versammlung (§285 STGB) gleich ein verfassungsgefährdender Angriff sein soll, der den Staatsschutz aktiviert. Das ist schon nach dem Versammlungsgesetz 1953 §17 der normalen Sicherheitspolizei zugewiesen.

Die in §6 aufgelisteten Strafbestände des STGB sollten sorgfältiger gelistet und abgespeckt werden.

Zu §7 des Entwurfs:

Die Beratung hinsichtlich „Cybersicherheit“ ist grundsätzlich zu begrüßen. Jedoch entsteht dabei ein Interessenkonflikt, denn einerseits sollen einzelne Computer und Computersysteme von Behörden und Unternehmen sicher gemacht werden. Andererseits hat gerade der Staatsschutz ein vitales Interesse in fremde Computer und Computersysteme unbemerkt einzudringen. Wie will der Staatsschutz diesen internen Konflikt lösen? Der Entwurf enthält nicht einen einzigen Hinweis zu diesem Konflikt und dadurch auch keine Rechtsgrundlagen, die diesen Konflikt transparent machen und ein Lösung andeuten. Auf die moralischen und ethischen Eigenschaften der eingesetzten Beamten kann man sich nicht verlassen, weil wenn dem so wäre, bräuchte man den ganzen Entwurf nicht.

Zu §9 des Entwurfs:

Diese Bestimmung ist eine Generalklausel und enthält keine Einschränkung hinsichtlich der Verhältnismäßigkeit der Ermittlung und Verwendung der Daten. Dadurch wird aber §1 Abs 2 2. Absatz (Verfassungsbestimmung) verletzt, der die Verhältnismäßigkeit auch für Behörden vorschreibt.

Zu §10 des Entwurfs:

Es ist offensichtlich, dass der Staatsschutz auch personenbezogene Daten erfassen und verwenden können soll. Es gilt aber auch für ihn das DSG2000, dass als Staatsgrundgesetz nicht nur den Staat (wie die anderen Staatsgrundgesetze) beschränkt, sondern auch die Bürger und Personengemeinschaften und juristische Personen vor allzu ausführlichen und detaillierten Datensammlungen schützen soll. Um dem Rechnung zu tragen, sollte daher der **§10 Abs1** mit einer Einschränkung versehen werden wie folgt:

„§10. (1) Das Bundesamt und die Landesämter dürfen personenbezogene Daten für

- 1. die erweiterte Gefahrenforschung (§ 6 Abs. 1 Z 1);*
- 2. den vorbeugenden Schutz vor wahrscheinlichen verfassungsgefährdenden Angriffen (§ 6 Abs. 1 Z 2);*
- 3. den Schutz vor verfassungsgefährdenden Angriffen aufgrund von Informationen von Dienststellen inländischer Behörden oder ausländischer Sicherheitsbehörden (§ 6 Abs. 1 Z 3);*
- 4. die Information verfassungsmäßiger Einrichtungen (§ 8)*

Ing. Dr. iur. Eike Wolf

im Rahmen der §1 und der §§6 - 9 DSG2000 ermitteln und verwenden, wobei sensible Daten gemäß §4 Z2 DSG2000 nur insoweit ermittelt und verwendet werden dürfen, als diese für die Ermittlung gemäß Z1 – 4 unbedingt notwendig sind.“

Absatz 3 dieses Paragraphen betrifft die Amtshilfe, die bereits im B-VG Art 22 festgelegt ist. Dabei ist jedoch eine wesentliche Einschränkung zu beachten, denn anerkannte Kirchen gelten als Körperschaften öffentlichen Rechts, sie sind aber keine Staatsorgane. Von denen Auskünfte im Rahmen der Amtshilfe zu verlangen, geht über die Amtshilfe, die hier gemeint ist, wohl hinaus. Daher wäre eine Präzisierung der zur Amtshilfe verpflichteten Organe notwendig.

Absatz 5 kann ohne Beschränkung des Inhalts vereinfacht werden zu:

„(5) Abgesehen von den Fällen der Abs. 2 bis 4 sowie den Ermittlungen nach § 12 sind das Bundesamt und die Landesämter für Zwecke des Abs. 1 berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten, zu ermitteln und weiterzuverarbeiten.“

Der durchgestrichene Satzteil ist überflüssig, weil veröffentlichte Texte und Bilder im Internet für Zwecke der öffentlichen Sicherheit und Verwaltung immer gemäß §41 UrhG frei verwendbar sind.

Allerdings ist dazu anzumerken, dass der Abs 5 in dieser Formulierung die Rasterfahndung gem §141 Abs 2 STPO ohne Ermächtigung durch den Rechtsschutzbeauftragten möglich macht, was sicher zu weit geht.

Zu §11 Abs1 des Entwurfs:

Die Erlaubnis zum „Zwecke der Bewertung der Wahrscheinlichkeit einer Gefährdung“ geht weit über die Datenanwendungen der Sicherheitsbehörden (§53a SPG) hinaus. Damit erhielte der Staatsschutz eine unbeschränkte Befugnis zum Datensammeln und –verwenden, weil die Wahrscheinlichkeit durch keinerlei begleitende Kriterien definiert ist. Der Staatsschutz bestimmt allein ohne Aufsicht durch den Rechtsschutzbeauftragten, wann und wie viel und welche Daten er erfasst und verwendet. Dh. Die Wahrscheinlichkeit muss durch begleitende Kriterien eingegrenzt werden, um eine nachprüfende Kontrolle solcher Datenanwendungen sicherzustellen. Zudem ist diese Datensammlung unter die Kontrolle des Rechtsschutzbeauftragten zu stellen.

Datenanwendungen, insbesondere in lit k) „Lebensverhältnisse“ ist so allgemein, dass darunter alles subsumiert werden kann. Es widerspricht daher dem Verhältnismäßigkeitsgebot des §1 Abs 2 DSG2000 (Verfassungsbestimmung). Abs1 muss daher insoweit eingeschränkt werden, dass sensible Daten gemäß §4 Z2 DSG2000 mit Ausnahme der politische Meinung, religiöse oder philosophische Überzeugung nicht erfasst werden dürfen. Der letzte Absatz von Abs 1 muss daher lauten:

„sowie tat- und fallbezogene Informationen und Verwaltungsdaten verarbeiten, auch wenn es sich um besonders schutzwürdige Daten eingeschränkt auf politischen Meinung oder religiöse oder philosophische Überzeugung im Sinne des § 4 Z 2 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr.

Ing. Dr. iur. Eike Wolf

165/1999, handelt.“ Sensible Daten wie Ethnik oder Gesundheit oder Sexualleben können wohl kaum etwas über die Gefährlichkeit eines möglichen Angriffs beitragen. Wenn dies doch einmal der Fall sein sollte, dann müsste die erweiterte Erlaubnis des Rechtsschutzbeauftragten eingeholt werden.

Zu §11 Abs1 Z3 des Entwurfs:

Die „Kontakt- oder Begleitpersonen“ ist ein zu allgemeiner Begriff und müsste präzisiert werden.

Zu §11 Abs4 des Entwurfs:

Die Protokollaufzeichnungen dürfen erst nach der Löschung gemäß Abs 2 gelöscht werden, sonst ist der Löschvorgang nach Abs 2 nicht protokolliert, was der Logik der Protokolldateien widerspricht. Gleiches gilt für §13 Abs 3 und §14 Abs 2. Darüber hinaus muss für die Protokolldateien sichergestellt sein, dass sie entweder durch eine sichere und qualifizierte Signatur gesichert und damit unveränderbar oder zumindest nur durch ein Vieraugenprinzip zugänglich sind. Sonst könnten sie von einem Systemadministrator jederzeit manipuliert werden.

Zu §12 des Entwurfs:

Der Begriff „aussichtslos“ muss hinsichtlich Ermittlungsmaßnahmen präzisiert werden, weil ein zu unbestimmter Begriff.

Falls bei den Observationen und versteckten Ermittlungen auch sogenannte IMSI-Catcher verwendet werden sollten, dann muss hier darauf hingewiesen werden, dass ein IMSI-Catcher in Richtung Mobilfunkgerät wie eine Basisstation wirkt, in Richtung Mobileswitchingcenter (MSC) jedoch wie ein Mobilfunkgerät, wobei jedoch eine Eigenschaft kritisch ist, dass gemäß GSM-Standards die Basisstation den Funkverkehr entschlüsselt und in damit abhörbar macht. Das bedeutet, dass der Einsatz von IMSI-Catchern nicht nur die Routineüberwachung eines Mobilgerätes, sondern auch dieses abhörbar macht. Dazu müsste aber die Genehmigung eines Gerichts eingeholt werden. Verschweigt man diese Möglichkeit des IMSI-Catchers, hört man illegal ab und verletzt eine Verfassungsbestimmung.

Zu Abs1 Z7:

Diese Bestimmung geht weit über §53 Abs 3a SPG hinaus und ist nach herrschender Meinung (OGH und Literatur) ein Eingriff in das Kommunikationsgeheimnis (§93 TKG 2003) und bedarf der gerichtlichen Zustimmung. Über die Verkehrsdaten sind in der Regel Schlüsse auf den Inhalt der Kommunikation möglich, können aber auch irreführend sein. Die „Verkehrsdaten“ müssen dahergestrichen werden.

Zu §13 des Entwurfs:

Die Beschäftigung staatlich bezahlter V-Leute ist ein besonders kritischer Bereich, weil einerseits die Zuverlässigkeit dieser Personen sehr eingeschränkt ist, wenn sie aus dem Umfeld der zu beobachtenden Organisation oder eines potentiellen Täters stammt. Und weiters ist die Ladung vor

F:\eigproj\Datenschutzrat\Stellungnahmen\Kommentar zum Polizeilichen Staatsschutzgesetz.doc

Ing. Dr. iur. Eike Wolf

Gericht als Zeuge wegen Preisgabe der Identität oft nicht möglich und daher sind die dadurch verschafften Beweismittel nicht im Rahmen eines fairen Verfahrens (Art 6 Abs 3 lit d EMRK) und damit für den Beschuldigten nicht überprüfbar und hinterfragbar. Da in dieser Bestimmung und auch in den Erläuterungen all diese Bedenken nicht einmal angedacht wurden, sollte man diese Bestimmung besser streichen. Überdies ist die Speicherung der so ermittelten Daten für 10 Jahre wohl zu lang und es gibt auch keine Begründung für diese lange Speicherung. Sie würde sich auch gemäß §6 Abs 1 Z 4 DSG2000 als besonders aufwendig und teuer gestalten.

Zu §14 Abs1 des Entwurfs:

§6 Abs 1 Z4 DSG2000 schreibt die Aktualisierung von personenbezogenen Daten vor. Dies wird hier korrekt wiederholt, wäre aber an sich überflüssig. Die Zitierung des §6 1 Z4 DSG2000 wäre ausreichend. Jedoch enthält der letzte Satz von Abs 1 die sehr unbestimmte Formulierung „..., es sei denn, für ihre Löschung wäre eine besondere Regelung getroffen worden.“ Da keine Kriterien für die „besondere Regelung“ angegeben sind, kann diese Regelung beliebig ausfallen. Das widerspricht aber eindeutig §6 Abs 1 Z5 DSG2000. Dort wird verlangt, dass nur gesetzliche Archivbestimmungen die Löschung von personenbezogenen Daten nach Erfüllung ihres Zwecks die Löschung verhindern können. Diese Regelung des §6 Abs 1 Z5 ist die Konkretisierung des §1 Abs 2 DSG2000 (Verfassungsbestimmung). Damit §14 Abs 1 letzter Satz der Verfassungsbestimmung des DSG2000 entspricht, müssen daher die „besonderen Regelungen“ durch bestimmende Kriterien ergänzt werden, damit diese Regelungen überprüf- und kontrollierbar werden.

Zu §14 Abs2 des Entwurfs:

In gleicher Weise enthält der 2. Absatz 2. Satz die unbestimmte Formulierung „aufgrund bestimmter Tatsachen“. **Welche Tatsachen?** Der Entwurf verwendet immer wieder solche unbestimmten Formen, damit er personenbezogene Daten und Ermittlungshandlungen nach Belieben und ohne Kontrolle und Überprüfbarkeit verwenden kann. Das widerspricht aber eindeutig Art 18 Abs 1 B-VG. Daher ist auch hier unbedingt eine Konkretisierung durch ergänzende Kriterien einzufügen, sonst wäre diese Bestimmung verfassungswidrig und damit würde sich der Staatsschutz außerhalb der Verfassung stellen.

Unklar und völlig unbegründet ist auch die lange Speicherzeit von 6 Jahren im letzten Satz. Die Zweckbestimmung des §6 Abs 1 Z5 begrenzt die Speicherzeit auf die Zweckerfüllung. Danach sind sie zu löschen. Das bedeutet, dass diese lange Speicherzeit einer gesetzlichen Begründung bedarf, die aber völlig im Entwurf und in den Erläuterungen fehlt. Ohne Kriterien für die erweiterte Speicherzeit ist dieser Satz verfassungswidrig.

Zu §15 Abs 1 des Entwurfs:

Der 1. Abs ist sprachlich verunglückt. Gemäß §6 ABGB und der herrschenden Meinung (Rechtsprechung und Lehre) muss ein Gesetz zunächst nach der eigentümlichen Bedeutung der

Ing. Dr. iur. Eike Wolf

Worte und ihres Zusammenhangs ausgelegt werden. Wendet man dies hier an, dann steht der Rechtsschutzbeauftragte unter dem besonderen Rechtsschutz der Aufgaben nach §6 Abs 1 Z1 und Z2. Denn die Wortfolge „kommt zu“ bedeutet gemäß Österreichisches Wörterbuch 42. Auflage 2012 (zukommen) unter anderem „jemandem eine Unterstützung zuteil werden lassen“. Ausführlicher ist WAHRIG, Deutsches Wörterbuch, Jubiläumsausgabe 1991 und neben den direkten Bedeutungen gibt es die übertragenen Bedeutungen von „schenken“, eine „Vergünstigung gewähren“. Das ist aber hier sicher nicht gemeint. Richtig gestellt müsste der 1. Absatz also lauten:

„(1) Dem Rechtsschutzbeauftragten (§91aSPG) obliegt die Ermächtigung zu und Kontrolle der Aufgaben gemäß §6 Abs 1 Z1 und Z2.“

Zu §15 Abs 2 des Entwurfs:

„Verlängerung ist zulässig“ ist zu unbestimmt und muss präzisiert werden hinsichtlich der Dauer und der maximalen Anzahl der Verlängerungen.

Zu §16 Abs 1 des Entwurfs:

Der zweite Satz dieses Absatzes schränkt die Befugnisse des Rechtsschutzbeauftragten ein für *„Auskünfte und Unterlagen über die Identität von Personen oder über Quellen, deren Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde, und für Abschriften (Ablichtungen), wenn das Bekanntwerden der Information die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde.“*

Eine ähnliche Einschränkung findet sich auch schon in §91d Abs 1 SPG. Beide Einschränkungen unterstellen damit dem Rechtsschutzbeauftragten Unzuverlässigkeit bei seiner Tätigkeit. Diese Unterstellung wird in den Erläuterungen zum PStSG nicht begründet. Woher kommt dieses Misstrauen? Oder soll damit ein Weg aus der Kontrolle und Überwachung durch den Rechtsschutzbeauftragten gefunden werden? Angeblich soll der Rechtsschutzbeauftragte die Funktion der Gerichte gemäß STPO übernehmen, weil dies im Vorverfahren von Ermittlungen angeblich schneller und weniger formalistisch abläuft. Wenn man dies so einrichten wollte, dann müsste man aber dem Rechtsschutzbeauftragten auch das Vertrauen und die Kompetenzen wie einem Gericht zuerkennen. Insoweit sind beide Beschränkungen (in SPG und PStSG) nicht nachvollziehbar und enthalten ein unbedründetes Misstrauen der Sicherheitsbehörden und des Staatsschutzes gegenüber dem Rechtsschutzbeauftragten. Es bleibt daher der begründete Verdacht, dass mit dieser Beschränkung der Befugnisse des Rechtsschutzbeauftragten für den Staatsschutz nur eine Möglichkeit geschaffen wird, durch die Behauptung, dass deren *„Bekanntwerden die nationale Sicherheit oder die Sicherheit von Menschen gefährden würde.“*, beliebige Ermittlungsverfahren zu starten und Datensammlungen anzulegen.

Das ergibt einen Freibrief für beliebige Ermittlungsverfahren ohne Kontrolle. Daraus folgt eine teilweise Verfassungswidrigkeit, die durch Streichung dieses 2. Satzes des Abs 1 behoben wäre.

Ing. Dr. iur. Eike Wolf

Wie weit die Unabhängigkeit des Rechtsschutzbeauftragten trotz seiner gesetzlichen Weisungsfreiheit reicht, ist gemäß Art 6 Abs 1 EMRK zweifelhaft. Denn schon die ebenso weisungsfrei gestaltete Datenschutzkommission wurde zu Recht von der EU-Kommission und dem EuGH gerügt und führte letztlich zu einer eigenen wirklich unabhängigen Behörde. Ähnliches könnte hier auch passieren. Man könnte sich aber die Rügen und Auflagen des EGMR sparen.

Zu den Änderungen im SPG:

Zu §53 Abs 3b des Entwurfs:

Durch den Einsatz von sogenannten IMSI-Catcher können auch Inhaltsdaten erhoben werden. Siehe oben zu §12 PStSG. Zudem ist ein IMSI-Catcher nicht zur genauen Lokalisierung eines Mobilfunkgerätes geeignet. Dazu müssten mehr als einer eingesetzt werden, um eine genaue Peilung des Mobilfunkgerätes zu erzielen. Daher ist diese Änderung des SPG ohne Ermächtigung durch den Rechtsschutzbeauftragten oder eines Gerichtes ein illegaler Eingriff in ein Grundrecht.

Ich ersuche um die Berücksichtigung meiner Kommentare und Verbesserungsvorschläge.

Wien, 6. Mai 2015

MfG

Ing. Dr. iur. Eike Wolf

Konsulent und

EuroPriSe zertifizierter Datenschutzexperte

Bechardgasse 15/8

1030 Wien

Tel: +431 367 85 26

Mobil: +43 664 421 52 35

E-Mail: eike.wolf@wolf-telecom.at