

Wie viel Datenschutz wollen Sie?

Smart Devices und Datenschutz



Bird & Bird
3. IT Law Camp

Frankfurt/M 17.3.2012

Rechtsanwältin Isabell Conrad (SSW Schneider Schiffer Weihermüller)
Rechtsanwalt Christof Höfner (Nokia Siemens Networks)

Wie viel Datenschutz soll's sein?

1 Wissen Sie eigentlich was Sie tun?

2 Apps

3 Location Based Services

4 AGB der Anbieter

Wissen Sie was Sie tun ?

Sind Sie denn schutzwürdig?



Beispiel eines aufgemalten Wegweisers auf dem Fußboden in einem Studentenwohnheim in Helsinki (Welt-Designhauptstadt 2012), SZ v. 2.1.2012, S.11

Smartphones: mehr als Mobiltelefon + Laptop

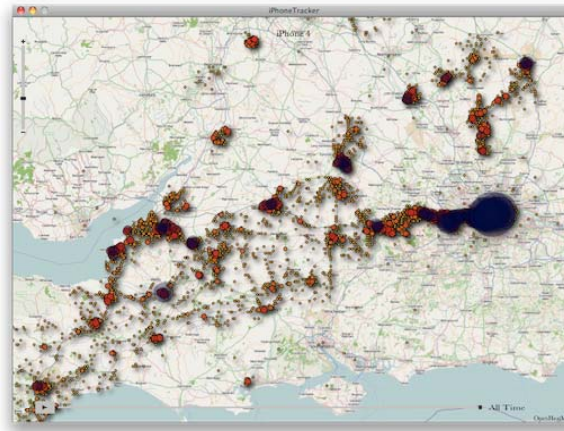
- Installation von Anwendungen (von Drittanbietern)
- metergenaue Ortung über GPS- und WLAN-Chips
- i.d.R. mehr personenbezogene Daten als frühere sog. Feature-Phones und Datenflüsse häufig unklar
 - E-Mail, Internetsurfen, Suchlisten/Favoriten, Zugangsdaten zu Online-Diensten etc.
 - Kalender, Einkaufslisten, Erinnerungsfunktionen
 - Adressbuch (nicht nur Telefonnummer und Name, sondern diverse Adressen/Kontaktdaten, Geburtstage etc.)
 - Sonstige Office-Apps (Scanner, Foto, Diktiergerät, Übersetzungshilfe)
 - Spiele, Navigationssystem etc.

Technische Risiken

Was geht?

1) Apple's „Location – Gate“

Alasdair Allan und Pete Warden, erregten großes Aufsehen, als sie einen Artikel über eine versteckte Datei in iOS 4 veröffentlichten, die regelmäßig die Position des Geräts erfasst und an Apple versendet. Alle iPhones mit iOS 4.0 oder höher legen einen log über Ihren Standort in einer Datei namens "consolidated.db" ab (eine einfache SQL-Datei), die Längen- und Breitengraden Koordinaten und einen Zeitstempel enthält. Angeblich durch iOS 5.0 abgestellt.



© ZD Net <http://www.zdnet.com/blog/apple/your-iphone-is-tracking-you-and-has-been-for-a-while/9985?tag=content;siu-container>
Siehe auch „Macworld: http://www.macworld.com/article/159352/2011/04/iphone_location.html

Technische Risiken

Was geht:

2) Verstecktes „Carrier IQ“ Root Kit auf Smart Phones

© <http://www.zdnet.com/blog/hardware/so-theres-a-rootkit-hidden-in-millions-of-cellphones/16708?tag=nl.e539>

Es scheint, daß ein Rootkit in Millionen von Android, Symbian, und sogar iOS Mobilgeräten alles aufzeichnet, was wir mit Smart Phones tun in Logs versteckt. Das Rootkit kommt von Carrier-IQ und es scheint, daß es Low-Level-Zugriff auf das System hat und es so ziemlich alles, was man mit dem Handy macht ausspioniert und an Carrier-IQ's server sendet.

Schon eine ernste Verletzung von Sicherheit, Privatsphäre und Vertrauen – oder?

Es wird anscheinend alles inkl. SMS und verschlüsselter Web-Recherchen protokolliert.

RIM, Nokia und HP haben es nie verwendet.

Apple hat das angeblich mit SW 5.01 abgestellt. Danke Apple !

Risiken

Die Realität / die größte Fehlerquelle im IT Bereich

Der Nutzer !!

Smart phones sind klein und begehrt.

Ergo: enormes Verlustrisiko durch Dummheit oder Diebstahl.

Dann sind alle Daten weg / in falschen Händen.

60% aller Unternehmensdaten liegen auf ungeschützten PCs oder mobilen Endgeräten

1 von 10 Laptops wird innerhalb eines Jahres gestohlen oder geht verloren

66% aller USB-Sticks gehen verloren.

Technische Risiken

Vermeidbarkeit:

3) allgemeine technische Risiken:

Virenschutz

ungesicherte WLANs

Verschlüsselung

Codes

Sperren

Technische Risiken

Was kann man technisch besser machen?

Beispiel: Intel

Lange hatte Intel die Nutzung von iPhone / iPad durch Intel MA verboten.

Nun verwendet eine Intel eine Exchange basierende Mail App und eine „mobile iron“ Mobile Device Management Lösung, mit der Intel die Geräte überwachen, steuern und die gesamten Daten ggf. löschen kann. Zusätzlich ist nur über VPN Tunnel Zugriff auf die Firmensysteme möglich.

Seither ist die Nutzung von Apple Handhelds erlaubt.

Wie viel Datenschutz soll's sein?

1 Wissen Sie eigentlich was Sie tun?

2 Apps

3 Location Based Services

4 AGB der Anbieter

Was sind Apps? (1)

- Apps = Application = Anwendungsprogramm
- Begriff von Apple im Zusammenhang mit Smartphones geschaffen



- Zunehmend herstellerübergreifende Verwendung für Anwendungen auf Smartphones, Tablet-Computern und nun auch PC's
- Apps können auf die Daten anderer Anwendungen zugreifen (z.B. Adressbuch)

Was sind Apps? (2)

- Klassische Software mit oder ohne Online-Funktionalität



Betrachter für Webseiten des ZDF



Brockhaus multimedial mobil 2010

Verhältnis von Smartphone-Betriebssystem zu Apps

- Wer bestimmt, welche Apps wann auf die Daten anderer Anwendungen zugreifen können (z.B. Adressbuch)?

iPhone Facebook-App



- **Betriebssystem bestimmt**, welche Berechtigungen Apps haben können (Zugriff auf Betriebssystemfunktionen, GPS-Sensor, WLAN, Adressbuch etc)
- Grds. können nur **Hersteller der Smartphone-Betriebssysteme für ausreichende Abschottung von Apps sorgen**
- Apple apps nur über itunes app store – dh Kontrollmöglichkeit durch Apple

Smartphone-Betriebssystem Android

Android Sandbox

- Default: Deny All, kein Zugriff auf App-fremde Daten und kein Zugriff auf Gerätefunktionen
- Erteilen weiterer Rechte über *Permissions*
- Permissions, die eine App einfordert kann sich der Nutzer vor Installation anzeigen lassen.

(P) Informierte Entscheidung durch den Nutzer wohl oft nicht möglich

- Apps im **Android Market** unterliegen keiner Kontrolle durch Android-Hersteller Google.
- Apps sind auch aus Quellen außerhalb Android Market installierbar.



Wie viel Datenschutz soll's sein?

1 Wissen Sie eigentlich was Sie tun?

2 Apps

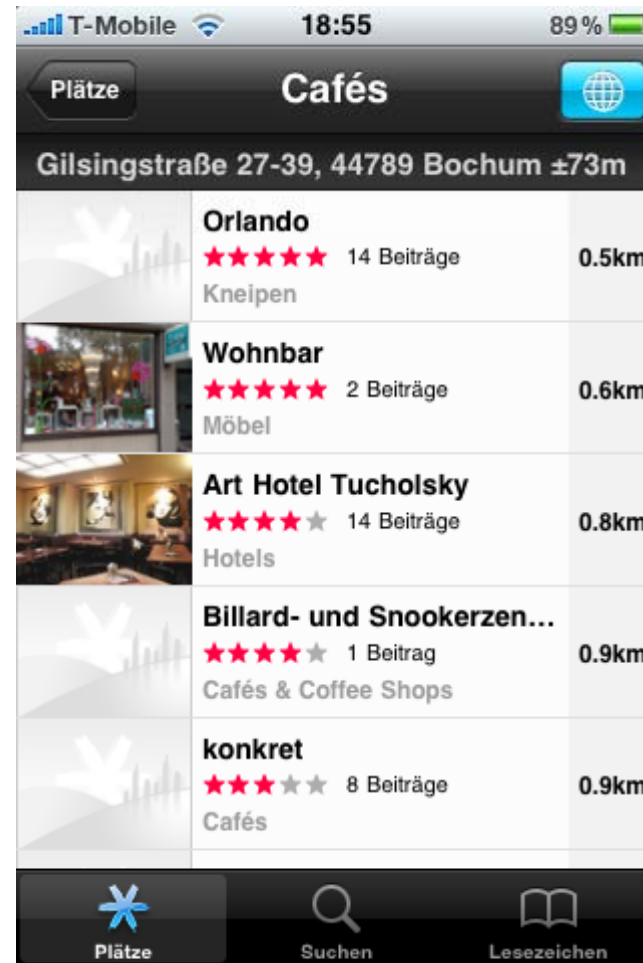
3 Location Based Services

4 AGB der Anbieter

Location Based Services (LBS)



iPhone Find my Friends-App



iPhone Qype-App

Beispiele für Einstellmöglichkeiten



**Kontrolle durch den Nutzer:
Anzeige einer
Ortung durch das
Betriebssystem**

**Kontrolle von Apps im
Rahmen des
Zulassungsprozesses bei
geschlossenen
Plattformen, sog. walled
gardens**

Datenschutzaspekte von LBS

- Bereitstellung von Diensten in Abhängigkeit vom aktuellen Aufenthaltsort des Nutzers.
- Erfordert in vielen Fällen die Übermittlung des Aufenthaltsorts an den Anbieter des Dienstes
 - Bsp.: Der Landkartenausschnitt, der die aktuelle Position des Nutzers anzeigen soll, muss erst vom Server des Diensteanbieters heruntergeladen werden muss, da das Kartenmaterial nicht vollständig auf dem Smartphone vorgehalten wird.
- Eine Speicherung der Ortsdaten über die reine Erbringung des Dienstes hinaus ist regelmäßig ohne Einwilligung des Nutzers nur auf Basis von § 15 TMG zulässig.
- Unterrichtung über Verwendung von Positionsdaten entspr. oft nicht § 13 TMG.
- Erstellung von Langzeitprofilen möglich über IMEI etc.

1 Consumerization der IT: „i“ statt „I“ – die elektronische Leine

2 Apps

3 Location Based Services

4 AGB der Anbieter

Wie viel Datenschutz wollen Sie denn?

Die Realität:

- a) Microsoft
- b) Apple
- c) Google

Wie viel Datenschutz wollen Sie denn?

Die Realität:

a) Microsoft © MS Online Privacy Statement download Nov '11

Erfassung persönlicher Daten

**§ 13 TMG
allgemein verständlich..**

MS erfasst zusätzliche Daten zu Ihren Interaktionen mit MS-Websites und -Diensten, wobei personenbezogene Daten ausgeschlossen werden. So werden auf unseren Websites zum Beispiel Daten von Ihrem Browser mithilfe von Websiteanalysetools abgerufen. Dazu zählen Daten wie die Website, von der aus Sie auf die Website gelangt sind, die Suchmaschine(n) und die Schlagwörter, mit denen Sie nach der betreffenden Website gesucht haben, die Seiten der Website, die Sie betrachtet haben, Ihre Browser-Add-Ons sowie die Breite und Höhe Ihres Browserfensters. MS verwendet weiterhin Technologien wie Cookies oder Webbeacons (Erkennungstags) um Informationen zu den von Ihnen angezeigten Seiten, zu den Links, auf die Sie klicken, und zu anderen Aktionen, die Sie auf den Websites oder Diensten durchführen, zu sammeln. Darüber hinaus erhalten wir einige Standarddaten, die Ihr Browser an die von Ihnen besuchten Websites sendet, z. B. IP-Adresse, Browsertyp und -sprache, Zugriffszeiten sowie die Adressen der Websites, durch die Sie auf diese Websites weitergeleitet wurden

**EUGH IP Adresse
= persbez. Datum**

Wie viel Datenschutz wollen Sie denn?

Die Realität:

a) Microsoft: (II)



§ 11 BDSG
§ 13 TMG ?

Verwendung Ihrer persönlichen Daten

Die vom Microsoft erfassten und verwendeten persönlichen Daten werden für den Betrieb und die Verbesserung der Websites und Dienste von Microsoft verwendet.

Die Verwendung umfasst möglicherweise das Bereitstellen eines effizienteren Kundenservices;

die Vereinfachung der Nutzung der Websites oder Dienste, indem dafür gesorgt wird, dass dieselben Informationen nicht wiederholt eingegeben werden müssen;

die Durchführung Von Untersuchungen und Analysen, die auf die Optimierung von Produkten, Diensten und Technologien abzielen;

und das Anzeigen von Inhalten und Werbeinformationen,

die auf Ihre Interessen und Präferenzen abgestimmt sind. Weitere Informationen zur Verwendung von Informationen zu Werbezwecken finden Sie unten im Abschnitt

Microsoft verwenden Ihre persönlichen Daten möglicherweise auch, um mit Ihnen zu kommunizieren. Sie erhalten möglicherweise notwendige Servicenachrichten, ...

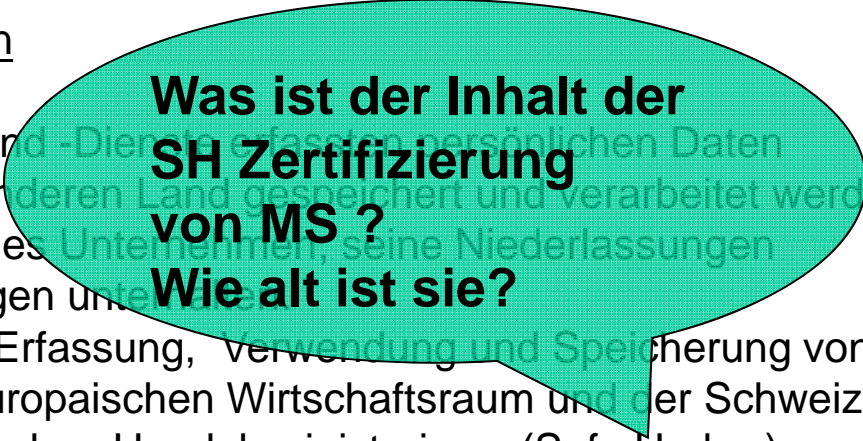
Wie viel Datenschutz wollen Sie denn?

Die Realität:

a) Microsoft: (III)

Verwendung Ihrer persönlichen Daten

Die [über] Ober 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 Dienstleister Einrichtungen unterhalten. Microsoft hält solch in Bezug auf die Erfassung, Verwendung und Speicherung von Daten aus der Europäischen Union, dem Europäischen Wirtschaftsraum und der Schweiz an die Bestimmungen des amerikanischen Handelsministeriums (Safe Harbor).



**Was ist der Inhalt der
SH Zertifizierung
von MS ?
Wie alt ist sie?**

Wie viel Datenschutz wollen Sie denn?

Die Realität:

a) Microsoft (IV)

Weitergabe Ihrer persönlichen Daten

Mit Ausnahme der in dieser Datenschutzerklärung genannten Fälle werden Ihre persönlichen Daten ohne Ihre Einwilligung nicht an Unternehmen außerhalb von Microsoft oder seine Niederlassungen und verbundenen Unternehmen weitergegeben.

Was gilt dann?

Einige Dienste von MS weisen ein Cobranding von MS und einem anderen Unternehmen auf. In manchen Fällen werden sowohl die Datenschutzbestimmungen von Microsoft als auch die des anderen Unternehmens angezeigt.

In diesen Fällen werden die von Ihnen beispielsweise auf den Anmeldeformularen angegebenen Informationen sowohl von Microsoft als auch dem anderen Unternehmen erfasst.

MS beauftragen gelegentlich andere Firmen, in begrenztem Umfang Dienste bereitzustellen, z. B. für das Verarbeiten und Verschicken von Direktwerbungen für das Beantworten von Kundenanfragen, für das Hosting von Webseiten, für die Analyse von Transaktionen oder für das Erstellen einer statistischen Analyse bezüglich der Dienste von MS. Diesen Diensteanbietern werden nur die persönlichen Daten übermittelt, die für die Bereitstellung des jeweiligen Dienstes erforderlich sind. Diese Firmen verpflichten sich, die Daten vertraulich zu behandeln.

**Wer sind diese,
wo sitzen diese?**

Wie viel Datenschutz wollen Sie denn?

Die Realität:

a) Microsoft (V)

Änderungen an diesen Datenschutzbestimmungen

Diese Datenschutzbestimmungen werden *von Zeit zu Zeit aktualisiert, um Änderungen bei Diensten und Feedback von Partnern und Kunden zu berücksichtigen*. Wenn Änderungen an den Bestimmungen vorgenommen wurden, können Sie das anhand des geänderten Datums unter "Letzte Aktualisierung" am Anfang der Datenschutzbestimmungen erkennen.

Bei grundlegenden Änderungen oder bei Änderungen in Bezug auf die Verwendung Ihrer persönlichen Daten durch Microsoft wird entweder vor der Implementierung dieser Änderungen an hervorgehobener Stelle ein Hinweis angezeigt, oder Sie erhalten von MS eine direkte Benachrichtigung. Sie sollten daher diese Datenschutzbestimmungen regelmäßig überprüfen, damit Sie In Bezug auf den Schutz Ihrer persönlichen Daten durch MS stets aktuell informiert sind.

Wie viel Datenschutz wollen Sie denn?

Die Realität:

b) Apple © Apple Datenschutzrichtlinie - download Jan 2012

Wie wir personenbezogene Daten nutzen:

Die personenbezogenen Daten, die wir erheben, erlauben uns, dich über die neuesten Apple Produktankündigungen, Softwareupdates und andere Informationen zu informieren. Du hilfst uns auch dabei, unsere Dienste zu verbessern. Wenn du nicht in unserem Verteiler sein möchtest, kannst du dich abmelden, indem du deine Einstellungen änderst. Wir nutzen personenbezogene Daten auch als Unterstützung für unsere Produkte, Dienste, Inhalte und Werbung zu entwickeln, anzubieten und zu verbessern. Von Zeit zu Zeit können wir personenbezogene Daten nutzen, um wichtige Mitteilungen zu versenden, wie Mitteilungen über Änderungen unserer Geschäftsbedingungen und Richtlinien. Während diese Informationen für die Beziehung zu Apple wichtig sind, kann man sich für den Erhalt dieser Informationen nicht abmelden. Wir können personenbezogene Daten auch für interne Zwecke nutzen, wie zur Buchprüfung, Datenanalyse und Forschung, um Apples Produkte, Dienste und die Kommunikation mit Kunden zu verbessern.

was macht Apple denn genau mit „deinen“ Daten

was macht Apple denn

aha: faule Äpfel kann man

„dir“ immer in den Korb

Legen!

Kurz: gelten § 11 BDSG und § 13 TMG noch ?

Wie viel Datenschutz wollen Sie denn?

Die Realität:

b) Apple (II)

Erheben und Nutzen von nicht-personenbezogenen Daten

Wir erheben auch nicht-personenbezogene Daten - Daten in einer Form, die keinen direkten Bezug zu einer bestimmten Person erlauben. Wir können nicht-personenbezogene Daten für jeden Zweck weitergeben und offenlegen.
Nachfolgend sind einige Beispiele für nicht-personenbezogene Daten aufgeführt, welche wir erheben und wie wir sie nutzen können:

Wir erheben Daten, wie namentlich Beruf, Sprache, Postleitzahl, Vorwahl, individuelle Geräteidentifizierungsmerkmale sowie Ort und Zeitzone, wo Apple Produkte verwendet Werden, damit wir das Verhalten unserer Kunden besser verstehen und unsere Produkte, Dienste und Werbung verbessern können.

Hallo!! EuGH zu
IP Adressen

was macht Apple denn
genau mit „deinen“ Daten?

Wie viel Datenschutz wollen Sie denn?

Die Realität:

b) Apple (III)

Standortbezogene Dienste

Um Standortbezogene Dienste auf Apple Produkten anzubieten können Apple und unsere Partner und Lizenznehmer präzise Standortdaten erheben, nutzen und weitergeben, einschließlich des geographischen Standorts deines Apple Computers oder Geräts in Echtzeit. **Apple hat aber die Geräte ID !!** Diese Standortdaten werden in anonymisierter Weise erhoben, durch die du nicht persönlich identifiziert wirst. Diese werden von Apple und unsere Partner und Lizenznehmer verwendet, um dir standortbezogene Produkte und Dienste anzubieten und um diese zu verbessern. Wir geben zum Beispiel deinen geographischen Standort an Anwendungsdienstleister weiter, wenn du deren Standort Dienste auswählst.

© Apple Datenschutzrichtlinie - download Jan 2012

Wie viel Datenschutz wollen Sie denn?

Die Realität:

b) Apple (IV)

Internationale Nutzer

Die von Dir zur Verfügung gestellten Daten sind Unternehmen auf der ganzen Welt zugänglich und können von diesen weitergegeben werden, so wie dies in dieser Datenschutzrichtlinie beschrieben ist. Apple hält sich an die vom US- Handelsministerium aufgestellten Safe Harbor – Grundsätze über das Erheben, Verwenden und Speichern personenbezogener Daten von Organisationen aus dem Europäischen Wirtschaftsraum und der Schweiz.

**Interessanter
Lösungsansatz**

Bitte beachte, daß die verantwortliche Stelle für personenbezogene Daten von Personen mit Wohnsitz in Mitgliedsstaaten des Europäischen Wirtschaftsraumes gemeinsam, Apple Sales International in Cork, Irland, und Apple UK Limited in Uxbridge, England sind. Verantwortliche Stelle für personenbezogene Daten, die im Europäischen Wirtschaftsraum durch die Benutzung von iTunes erhoben werden, ist iTunes Sarl in Luxemburg.

© Apple Datenschutzrichtlinie - download Jan 2012

Wie viel Datenschutz wollen Sie denn?

Die Realität:

c) Google (März 2012)

Protokolldaten

Wenn Sie unsere Dienste nutzen oder von Google bereitgestellte Inhalte aufrufen, erfassen und speichern wir bestimmte Daten gegebenenfalls in Serverprotokollen.

Diese Protokolle können Folgendes enthalten:

Einzelheiten zu der Art und Weise, wie Sie unsere Dienste genutzt haben, beispielsweise Ihre Suchanfragen.

Telefonieprotokollinformationen wie Ihre Telefonnummer, Anrufernummer, Weiterleitungsnummern, Datum und Uhrzeit von Anrufen, Dauer von Anrufen, SMS-Routing-Informationen und Art der Anrufe, IP-Adresse.

Daten zu Geräteereignissen wie Abstürze, Systemaktivität, Hardware-Einstellungen, Browser-Typ, Browser-Sprache, Datum und Uhrzeit Ihrer Anfrage und Referral-URL. Cookies, über die Ihr Browser oder Ihr Google-Konto eindeutig identifiziert werden können.

© Google Datenschutzrichtlinie – veröffentlicht März 2012

Wie viel Datenschutz wollen Sie denn?

Die Realität:

c) Google (II)

Standortbezogene Informationen

Bei der Nutzung standortbezogener Google-Dienste erheben und verarbeiten wir möglicherweise Informationen über Ihren tatsächlichen Standort, wie z.B. die von Einem Mobilfunkgerät gesendeten GPS-Signale. Darüber hinaus verwenden wir zur Standortbestimmung verschiedene Technologien, wie zum Beispiel Sensordaten Ihres Geräts, die beispielsweise Informationen über nahegelegene WLAN-Zugänge oder Sendemasten enthalten können.

© Google Datenschutzrichtlinie – veröffentlicht März 2012

Conclusio / Confusio

Der Schutz personenbezogener Daten ist elementar.

Die geltenden Gesetze fordern von „verantwortlichen Stellen“ und deren Datenverarbeitern bei der Verarbeitung personenbezogener Daten ein hohes Maß an Schutz und Verantwortung.

Schützen natürliche Personen ihre eigenen personenbezogenen Daten im gleichen Maß?

Ist natürlichen Personen ihrer eigenen personenbezogenen Daten wichtig?

Ist der immer noch geltende Datenschutzansatz richtig?

RA Christof Höfner, Country Counsel,

Nokia Siemens Networks GmbH & Co. KG

christof.hoefner@sns.com

RAin Isabell Conrad

SSW Schneider Schiffer Weihermüller

isabell.conrad@ssw-muc.de

