



Der Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,  
Postfach 1468, 53004 Bonn

**Bundesnetzagentur**  
**Referat 416**  
**Canisiusstr. 21**  
**55122 Mainz**

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn  
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799- [REDACTED]

TELEFAX (0228) 997799- [REDACTED]

E-MAIL [REDACTED]@bdi.bund.de

BEARBEITET VON [REDACTED]

INTERNET [www.datenschutz.bund.de](http://www.datenschutz.bund.de)

DATUM Bonn, 04.11.2013

GESCHÄFTSZ. VIII-190-2/025#0257

Bitte geben Sie das vorstehende Geschäftszeichen bei  
allen Antworten treiben unbedingt an.

BETREFF **Schnittstellen an Netzabschlusspunkten**

BEZUG **Mitteilung 395/2013**

Sehr geehrte Damen und Herren,

ich möchte zu den datenschutzrechtlichen Aspekten der Lage des Netzabschlusspunktes Stellung nehmen. Dies betrifft in erster Linie Frage 9 (*Sehen Sie Gefahren im Hinblick auf den Schutz privater Daten und im Hinblick auf die Einschränkung der Funktionsherrschaft des Endnutzers über seine private Infrastruktur?*) in Mitteilung 395/2013. Hier ist jedoch nicht nur die Endbenutzerfreundlichkeit betroffen, wie Sie dies in der Überschrift des Fragenkomplexes nahelegen, sondern auch die Verpflichtungen der Netzbetreiber.

Wenn sich der Netzabschlusspunkt hinter einer „Box“ befindet, ist diese „Box“ als Teil des Telekommunikationsnetzes zu bewerten. Somit sind die datenschutzrechtlichen Anforderungen zur Speicherung von Verkehrsdaten einzuhalten. Dies betrifft – je nach Funktionsumfang – Telefongespräche, IP-Adressen oder Verbindungen zu WLAN-Clients. Viele Router mit Telefonfunktion haben Anruflisten als Komfortfunktion und Logfiles (z. B. als „Ereignisse“ bezeichnet) zur Fehlersuche. Diese müssten entweder auf explizite Veranlassung und unter der Kontrolle des Teilnehmers gespeichert werden oder, wenn sie auf Veranlassung des Telekommunikationsanbie-



ters für Zwecke des § 100 Abs. 1 TKG gespeichert werden, nach 7 Tagen gelöscht werden (siehe „Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten“). Dabei ist auch die Erforderlichkeit zu prüfen, wenn z. B. keine Entstörung für die WLAN-Nutzung durchgeführt wird, sind hier auch keine Daten zu speichern.

Wenn eine „Box“ Teil des Telekommunikationsnetzes ist, ist der Telekommunikationsanbieter auch für die Sicherheit verantwortlich, muss also für die gesamte Lebensdauer des Gerätes diese gewährleisten (siehe Katalog von Sicherheitsanforderungen, Punkt 9.9). In der Vergangenheit wurden z. B. für DSL-Router häufiger Sicherheitsmängel bekannt. Diese wären unverzüglich durch den Telekommunikationsanbieter zu beheben. In der Praxis dürfte es erforderlich sein, für die zeitnahe Bereitstellung einer aktuellen Firmware bei sicherheitskritischen Fehlern eine vertragliche Vereinbarung mit dem Hersteller der „Box“ abzuschließen.

Besondere rechtliche Herausforderungen ergeben sich bei dem Modell B3. Daher möchte ich auf einige Aspekte hinweisen:

- Die Funkschnittstellen an der „Box“ sind noch dem Netzbetreiber zuzurechnen. Daraus kann geschlossen werden, dass diese nach Stand der Technik gesichert werden müssen, also etwa WLAN- und DECT-Verbindungen immer sicher verschlüsselt werden müssen (s. § 109 Abs. 1 TKG). Die Verbindung zu einem DECT-Gerät ohne Verschlüsselung oder einem veralteten WLAN-Gerät mit WEP-Verschlüsselung dürfte also nicht mehr hergestellt werden.
- Wenn hausinterne Telefonate (wenn die „Box“ als Telefonanlage arbeitet) oder Datenverkehr verschiedener angeschlossener Endgeräte (z. B. von einem NAS zu einem Smart-TV) über die „Box“ geführt werden, könnte dieser Verkehr als Telekommunikation in der Verantwortung des Netzbetreibers betrachtet werden, für die er auch verantwortlich ist. Gleichzeitig dürfte dies dem berechtigten Interesse vieler Nutzer widersprechen, die ihr lokales Netz als eigenen „Hoheitsbereich“ empfinden, in den keine Eingriffe des Netzbetreibers zu erfolgen haben. Die Administration der „Box“ durch den Netzbetreiber muss einerseits so weit gehen, dass die Sicherheit gewährleistet werden kann, andererseits sind unangemessene Eingriffe durch den Anbieter (z. B. Einrichtung einer VPN-Verbindung durch den Anbieter, also ein Zugang von außen in das LAN) technisch zu verhindern.
- Ein Anrufbeantworter, der auch in manchen Routern integriert ist, wäre ggf. nach den Regelungen des § 107 TKG zu beurteilen, einschließlich der Pflichten zur Sicherung der Nachrichten (siehe § 107 Abs. 2 TKG).
- Die Informationspflichten des § 93 TKG sind zu beachten, etwa wenn Komfortfunktionen eine Datenübermittlung an Dritte erfordern. Dies wäre bei DynDNS-



Diensten der Fall, bei denen die IP-Adresse an den Anbieter des DynDNS-Dienstes übermittelt wird. Weiterhin sind die Teilnehmer über die in der „Box“ gespeicherten Daten zu informieren, etwa für eine Entstörung.

Bei einer Verlagerung der Netzabschlusspunkte sind also neben den in der Anhörung genannten Aspekten, wie z. B. wettbewerbsrechtlichen oder Verbraucherschutzrechtlichen Fragen, auch Fragen zum Datenschutz, Fernmeldegeheimnis und zur Sicherheit zu berücksichtigen, für die der Netzbetreiber die Verantwortung übernimmt, wenn die Schnittstelle hinter eine „Box“ verlagert wird. Weiterhin bestehen dann auch Kontrollbefugnisse bzw. -verpflichtungen für den BfDI und die BNetzA.

Mit freundlichen Grüßen  
Im Auftrag

