

## MERKBLATT: ÜBERMITTLUNG VON DATEN AN STRAFVERFOLGUNGSBEHÖRDEN

### MISSBRÄUCLICHE INTERNETNUTZUNG

Beim Einsatz der IT-Systeme der RUB sind einschlägige Gesetze, Vorschriften und Dienstvereinbarungen einzuhalten. Diese regeln unter anderem die Bereitstellung von Daten unter Gesichtspunkten des Datenschutzes, des Urheber- und Markenrechts und belegen die Verbreitung oder Verschaffung rechtswidriger Inhalte mit Strafe.

Besteht der Verdacht, dass IT-Systeme der Ruhr-Universität missbräuchlich genutzt werden, so sind keine Ermittlungen auf eigene Faust anzustellen, sondern

- es sollten Beweise gesichert werden (Ausdruck und Speicherung der Dateien, Ermittlung von Zeugen etc.).
- der Verstoß ist zeitnah zu melden, damit die Daten entfernt oder der Zugang zu ihnen gesperrt werden kann. Dies ist insbesondere besonders dann wichtig, wenn auf IT-Systemen gespeicherte personenbezogene Daten oder urheberrechtlich geschützte Inhalte von Unberechtigten eingesehen werden können oder rechtswidrige Inhalte auf IT-Systemen der RUB abgelegt sind oder über diese verbreitet werden.
- bei der Meldung sind die offiziellen Meldewege einzuhalten. Eine Beschreibung der Meldewege findet sich unter der am Ende angegebenen Internetadresse.

### VORGEHENSWEISE BEI AUSKUNFTSERSUCHEN DRITTER

Häufig werden Auskunftersuchen an Einrichtungen der Ruhr-Universität gerichtet, um Informationen über Benutzer des Internets zu ermitteln. Dabei müssen die datenschutzrechtlichen Belange der Hochschulangehörigen berücksichtigt werden. Grundsätzlich sind ausschließlich Strafverfolgungsbehörden befugt, derartige Auskünfte unter bestimmten gesetzlichen Vorgaben einzuholen.

Werden Anfragen von Sicherheitsbehörden gestellt, so sollte nicht übereilt gehandelt werden und die folgenden Leitlinien berücksichtigt werden:

- **Die Übermittlung von Daten ist mit der Beauftragten für Informationssicherheit der RUB abzustimmen. Diese wird gegebenenfalls das Justitiariat und den Datenschutzbeauftragten einschalten.**
- Erfolgt das Auskunftersuchen telefonisch, so sollte um eine schriftliche Bestätigung der Anfrage gebeten werden. Dies dient in erster Linie dazu, im Nachhinein Vorwürfe über datenschutzrechtliche Verstöße von Seiten der Nutzer auszuräumen.
- In der Anfrage muss die Rechtsgrundlage für die Auskunft genannt sein. Daraus ergibt sich, welche Daten überhaupt übermittelt werden dürfen (siehe unten).
- Vorhandene Daten sollten gesichert und nicht gelöscht werden.
- Gegenüber den betroffenen Nutzern und Dritten ist Stillschweigen zu wahren.

## RECHTSGRUNDLAGEN

Bei Auskunftersuchen der Strafverfolgungsbehörden ist zwischen Bestands-, Nutzungsdaten (Verkehrsdaten) und Inhalten der Kommunikation zu unterscheiden:

- Bestandsdaten sind personenbezogene Daten wie Name und Anschrift eines Benutzers oder fest vergebene IP-Adressen. Gemäß § 174 TKG (Telekommunikationsgesetz) sowie § 22 TTDSG (Telekommunikation-Telemedien-Datenschutzgesetz) besteht eine Auskunftspflicht gegenüber den Ermittlungsbehörden auch ohne vorherige richterliche Anordnung, soweit dies zur Verfolgung von Straftaten, Ordnungswidrigkeiten oder zur Gefahrenabwehr erforderlich ist. Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden. Benutzern darf gemäß § 174 TKG nicht mitgeteilt werden, dass eine Auskunftserteilung stattgefunden hat. Ergänzend sind gemäß § 161 StPO alle öffentlichen Einrichtungen bei staatsanwaltlichen Ermittlungen verpflichtet, auf Verlangen Bestandsdaten an die Strafverfolgungsbehörden zu übermitteln.
- Nutzungsdaten (Verkehrsdaten) sind Daten, die bei der Bereitstellung und Erbringung eines Dienstes erhoben werden: beispielsweise Zeitpunkt des Beginns oder Endes einer Internetverbindung. Nach § 100g StPO können Strafverfolgungsbehörden über einen Kommunikationsvorgang Auskunft verlangen. Es muss eine schriftliche richterliche Anordnung oder bei Gefahr im Verzug eine staatsanwaltliche Anordnung vorgelegt werden. Die staatsanwaltliche Anordnung bei Gefahr im Verzug tritt nach drei Tagen außer Kraft, wenn sie nicht vom Gericht bestätigt wird.
- Bei Vorliegen einer besonders schweren Straftat besteht gemäß §23 TTDSG auch eine Auskunftspflicht über die als Bestandsdaten erhobenen Passwörter oder andere Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen möglich ist. Es muss eine schriftliche richterliche Anordnung vorliegen.
- Inhalte der Kommunikation, beispielsweise Inhalte von Emails, unterliegen dem Fernmeldegeheimnis. Wichtigste Rechtsgrundlage für eine Überwachung und Aufzeichnung der Inhalte einer Telekommunikation wird durch § 100a StPO begründet. Die formale Voraussetzung für ein Auskunftersuchen setzt den konkreten Verdacht einer schweren Straftat voraus. Es muss ferner eine schriftliche richterliche Anordnung oder bei Gefahr im Verzug eine staatsanwaltliche Anordnung vorgelegt werden. Die staatsanwaltliche Anordnung bei Gefahr im Verzug tritt nach drei Tagen außer Kraft, wenn sie nicht vom Gericht bestätigt wird.

## WELCHE SPEICHERPFLICHT BESTEHT?

Es besteht *keine generelle Pflicht zur Erhebung und Speicherung von Daten* für eine mögliche Auskunftserteilung an Strafverfolgungsbehörden. § 176 TKG begründet nur eine Speicherpflicht für Anbieter öffentlich zugänglicher Telekommunikationsdienste. Jedoch werden Bestandsdaten nach § 172 TKG zulässigerweise gespeichert, die nach § 174 TKG von Strafverfolgungsbehörden angefragt werden können. §12 TTDSG erlaubt unter strengen Auflagen die kurzzeitige Speicherung von Verkehrsdaten zur Beseitigung von Störungen und zur Gefahrenabwehr. Bei der Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten sind die datenschutzrechtlichen Bestimmungen einzuhalten (DSGVO Datenschutz-Grundverordnung). Erst nach einer richterlichen Anordnung besteht im Einzelfall eine Pflicht zur Vorratsdatenhaltung für die Übermittlung an Sicherheitsbehörden.

## Referenzen:

„Internetrecht“, Prof. Dr. Hoeren, Universität Münster, <https://www.itm.nrw/lehre/materialien/>  
Forschungsstelle Recht des DFN, <https://www.dfn.de/rechtimdfn/>  
Meldewege: <http://www.itsb.rub.de/themen/meldewege.html>