

Bonn, den 28.03.2022

Allgemeine Positionierung

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Thema:

Einschaltung Dritter bei eingriffsintensiven Maßnahmen wie Quellen-Telekommunikationsüberwachung und Online- Durchsuchung



In den Medien wird verschiedentlich darüber berichtet, dass deutsche Polizeibehörden IT-Produkte für heimliche Ermittlungseingriffe bei Drittherstellern beschafft hätten. Im parlamentarischen Raum wird über die Grenzen des Einsatzes von Spionagesoftware diskutiert. Diese allgemeine Positionierung soll aufzeigen, wo die rechtlichen und rechtspolitischen Grenzen in denkbaren Fällen des Einsatzes Dritter im Kontext der Durchführung eingriffsintensiver Maßnahmen – wie Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und Online-Durchsuchung – verlaufen.

- Die rechtliche Beurteilung hängt maßgeblich davon ab, welche Dienstleistungen im Einzelfall von welcher Stelle und wie erbracht werden. Insofern ist auf die Umstände des Einzelfalls abzustellen.
- Die Durchführung von IT-gestützten eingriffsintensiven Maßnahmen gehört zum genuinen Bereich staatlicher Verantwortung. Bei Einbeziehung Dritter ist deshalb größte Zurückhaltung geboten. Eigenentwicklungen sind den von privaten Dritten entwickelten Software-Lösungen vorzuziehen (vgl. z.B. 28. Tätigkeitsbericht des BfDI, S. 57).
- Die Verarbeitung personenbezogener Daten im Auftrag des Verantwortlichen im Kontext der Durchführung derart eingriffsintensiver Maßnahmen sollte auf ein Mindestmaß begrenzt sein. Die Möglichkeit einer unkontrollierten Speicherung oder sonstigen missbräuchlichen Verwendung personenbezogener Daten ist auszuschließen.
- Entscheidungsbefugnisse hinsichtlich des „Ob“ und „Wie“ der Durchführung einzelner Überwachungsmaßnahmen dürfen nicht auf private Dritte übertragen werden. Vorbereitende Hilfstätigkeiten sind in engen Grenzen möglich.
- Soweit eingesetzte IT-Produkte nicht von der verantwortlichen Stelle selbst hergestellt bzw. entwickelt wurden, dürfen die verarbeiteten Daten nicht ihrem Einfluss und der Kontrolle entzogen sein. Derartige Überwachungsmittel müssen allen in Deutschland geltenden datenschutzrechtlichen Anforderungen gerecht werden. Der Verantwortliche muss über alle Informationen verfügen, die zum Zweck der Durchführung einer Datenschutzkontrolle, inklusive der relevanten Beschaffenheitsmerkmale der Hard- und Software, notwendig sind und er muss die Beherrschbarkeit der Hard- und Software vollumfänglich gewährleisten.
- Bei eingriffsintensiven Maßnahmen wie zum Beispiel der Quellen-TKÜ und der Online-Durchsuchung sind an die Sicherheit der Datenverarbeitung strenge



Anforderungen zu stellen (vgl. § 49 Abs. 2 BKAG, ergänzend § 64 BDSG). So setzt die Einschaltung von Auftragsverarbeitern voraus, dass bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau gewährleistet ist (§§ 62 Abs. 2, 64 Abs. 1 BDSG). Angesichts der hohen Eingriffsintensität von Maßnahmen wie Quellen-TKÜ und Online-Durchsuchung ist der Einsatz von Auftragsverarbeitern in diesem Bereich de facto an hohe Hürden geknüpft.

- Die Einschaltung (privater) Dritter darf die Kontrollbefugnisse der Datenschutzaufsichtsbehörden nicht einschränken. Angesichts der umfassenden Informations- und Mitwirkungspflichten der öffentlichen Stellen (vgl. z.B. § 16 Abs. 4 BDSG) muss der Verantwortliche über alle Informationen verfügen, die zur Beurteilung der datenschutzrechtlichen Rechtmäßigkeit der Maßnahme, inklusive – um bei diesem Beispiel zu bleiben – der relevanten Beschaffenheitsmerkmale etwaiger Software, notwendig sind. Soweit Dritte einbezogen sind, wäre etwa nicht hinnehmbar, wenn die Einsicht in die Unterlagen davon abhängig gemacht wird, dass die Aufsichtsbehörde beispielsweise eine gesonderte Geheimhaltungsvereinbarung, Serviceklauseln, „Gebühren“ für fachliche Begleitung oder dergleichen unterzeichnet oder begleitet (24. Tätigkeitsbericht Nr. 7.4.1, S. 94). Im Bereich der Auftragsdatenverarbeitung nach dem BDSG hat die verantwortliche Stelle nach § 62 Abs. 5 Nr. 5 BDSG sicherzustellen, dass alle für die Datenschutzkontrolle erforderlichen Informationen ohne zusätzliche Anforderungen verfügbar sind.