*Jan Fährmann[1]/Alexander Vollmar[2]/Gudrun Görlitz[3]*

# Rechtliche und technische Rahmenbedingungen für die datenschutzkonforme Verarbeitung von Ortungsdaten durch Private und die Polizei unter besonderer Berücksichtigung des Datenschutzrechts

## 1. Einleitung

Im interdisziplinären Forschungsprojekt *FindMyBike* wurde eine datenschutzkonforme Software (*FindMyBike-System*)[4] zur Übertragung von Positionsdaten gestohlener, mobiler und mit ortbaren Sendern ausgestatten Gegenstände an die Polizei konzipiert. Die Software wurde auf Basis des Wissens über Fahrraddiebstähle entwickelt (wobei auch andere Positionsdaten gestohlener Gegenstände übertragen werden können). Sobald die Besitzer*innen den Diebstahl bemerken, können sie bei der jeweiligen Trackingservice-Anbieter*in eine Uniform Ressource Locator (URL) anfordern, die durch das *FindMyBike-System* generiert und von der Trackingservice-Anbieter*in mit dem Fahrrad verknüpft wird, sodass dessen Live-Position auf einer Karte angezeigt wird. Über einen längeren Zeitraum erhobene Positionsdaten (Bewegungsdaten) können auch über die Software an die Polizei übertragen werden, müssen aber gesondert angefordert werden. Die URL mit der Live-Position können die Bestohlenen bei der Anzeigeerstellung in der Internet-Wache in das zugehörige Online-Formular kopieren. Die Polizei kann mit Hilfe dieser URL die *FindMyBike-Anwendung* aufrufen und hat damit Zugriff auf die Live-Positionsdaten des Fahrrades. Diese Positionsdaten können bei der Aufklärung von Diebstählen sehr hilfreich bzw. die wesentliche Voraussetzung zur Ermittlung der Dieb*innen sein und auch in einem zivilgerichtlichen Verfahren – z. B. auf Schadensersatz gegen die Dieb*innen – als wichtiges Beweismittel dienen.[5] Immer mehr Gegenstände

1 Dr. Jan Fährmann war in dem Projekt FindMyBike Wissenschaftlicher Mitarbeiter für die rechtlichen und kriminologischen Forschungsfragen.

2 Alexander Vollmar war in dem Projekt FindMyBike Wissenschaftlicher Mitarbeiter für die Forschungsfragen aus dem Bereich Informatik.

3 Prof. Dr. Gudrun Görlitz hat das Projekt FindMyBike für den Bereich Informatik geleitet.

4 Die Implementierung des FindMyBike-Systems ist in Vollmar/Görlitz/Kober in diesem Band, S. 227ff, dargelegt.

5 Fn. einfügen: Fährmann/Vollmar/Görlitz in diesem Band: S. 177ff.

sind ortbar, sodass zukünftig damit zu rechnen ist, dass private Anbieter zunehmend in der Lage sind, diese bei einem Diebstahl zu orten.

Mit der Übertragung von Positionsdaten gestohlener Gegenstände an die Polizei gehen aber auch verschiedene datenschutzrechtliche Risiken einher. Da sensible Daten von Personen betroffen sein können, die keinen Anlass zur Datenerhebung gegeben haben, sind erhöhte Anforderungen zum Schutz der Daten an die Ausgestaltung einer solchen Software zu stellen. Zwar sind sowohl Dieb*innen als auch bösgläubige Besitzer*innen wenig schutzwürdig, sodass ihre Interessen gering zu gewichten sind. Aber es ist möglich, dass (ggf. tage- oder wochenlang) Positionsdaten von gutgläubigen Besitzer*innen erhoben und ausgewertet werden, weil Fahrräder sehr schnell weitergegeben werden können. Positionsdaten – insbesondere, wenn sie über einen längeren Zeitraum erhoben werden – können ein Bewegungsbild der Person wiedergeben, die den Gegenstand bei sich führt. Daher kann es sich um sensible Daten handeln, die weitreichende Einblicke in die Privatsphäre der Betroffenen ermöglichen, gerade wenn sie mit anderen Daten kombiniert werden, was im strafrechtlichen Ermittlungsverfahren üblich ist. Grundsätzlich lassen Trackingdaten damit weitreichende Rückschlüsse auf eine Person und ihre Lebensumstände zu, etwa bezüglich des Wohnorts, besuchter Geschäfte oder Bekannter. Die Bewegungsdaten von Fahrrädern können allerdings nicht immer einer konkreten Person oder Örtlichkeit zugeordnet werden, gerade weil das Fahrrad leicht weitergegeben werden kann, was für eine geringere Schutzwürdigkeit spricht. Die Bewegungsdaten beziehen sich außerdem zumeist auf Vorgänge, die in der Öffentlichkeit ablaufen, wodurch sie auch der weniger eingriffsintensiven Sozialsphäre zugeordnet werden können. Auch ist im Regelfall ein eingeschränkter Lebensbereich betroffen, da Fahrräder meist nur zum Fortkommen oder zu sportlichen Aktivitäten verwendet werden, wobei der Bewegungsradius nicht unerheblich sein kann, zumal Fahrräder im Rahmen von Mobilitätskonzepten immer mehr an Bedeutung gewinnen. Entscheidend für die gesteigerten datenschutzrechtlichen Anforderungen ist aber der Umstand, dass die Positionsdaten für ein strafrechtliches Verfahren relevant sein können, in dem sie in eingriffsintensiver Weise verwendet werden und stigmatisierende Wirkungen bis hin zu einer (ggf. ungerechtfertigten) Verurteilung entfalten können.[6] Die Beteiligung mehrerer Akteure führt außerdem zu speziellen Risiken für das Recht auf informationelle Selbstbestimmung. Haben mehrere Personen Zugriff auf die Daten, so steigt auch das Risiko individuellen Fehlverhaltens.

Im Rahmen des Beitrages wird auf Basis dieser Risikobewertung erläutert, welche datenschutzrechtlichen Anforderungen und Pflichten bei der Konzepti-

6 Vgl. Borell/Schindler, DuD 2019, S. 772; zur Bestimmung der Sensibilität der Positionsdaten ausführlich Fährmann in diesem Band, S. 141 ff.

on der Software zu berücksichtigen sind und wie diese technisch umgesetzt wurden bzw., welche Umsetzungsmöglichkeiten es gibt. Die Konzeption der Software wurde insbesondere von den Datenschutzgrundsätzen der Datensparsamkeit sowie Privacy by Design und Default getragen, um einen wirksamen Datenschutz bereits in der Software und ihren Funktionen anzulegen. Zudem wird in diesem Beitrag auf die rechtliche Stellung und die daraus resultierenden gesetzlichen Verpflichtungen der an der Datenverarbeitung beteiligten Akteure eingegangen, die bei einer Umsetzung eines solchen Systems in der Praxis zugrunde gelegt werden müssten.

Die Software ist für die Berliner Polizei entwickelt worden. Auf Grund der hohen Datenschutzanforderungen an polizeiliche IT-Systeme konnte die Software im Zeitrahmen eines Forschungsprojektes nicht in das vorhandene IT-System integriert werden, sondern wurde als Softwareschnittstelle zur Berliner Polizei implementiert. Daraus ergibt sich der Vorteil, dass die Software auch in anderen Bundesländern ohne größeren Aufwand an die dort im Einsatz befindlichen IT-Systemen angebunden und in die polizeiliche Arbeit integriert werden kann. Wenn die Auswertung von Positionsdaten regelmäßig in die Ermittlungsarbeit einbezogen wird, dann sollte eine integrierte Implementierung in den polizeilichen Workflow und die IT-Systeme erfolgen.

## 2. Beteiligte Akteure an der Datenverarbeitung

An dem Prozess der Erhebung und Weiterleitung der Positionsdaten der gestohlenen Gegenstände sind folgende Personen(-gruppen) mit ihren jeweils spezifischen Interessen und rechtlichen Positionen beteiligt:

- Berechtigte zur Ortung des Diebesgutes (kurz: Tracking-Berechtigte): Berechtigt sind Eigentümer*innen der Gegenstände (hier und im Folgenden des Fahrrades). Zusätzlich kann auch aus anderen Rechtposition eine Befugnis zur Ortung folgen, etwa aus einer Anwartschaft an dem Fahrrad oder einem Fahrrad-Leasingvertrag.
- Trackingservice-Anbieter*in: Dies könnte z. B. eine Firma sein, die gegen Gebühr Tracking-Daten für die Tracking-Berechtigten verarbeitet und dafür passende Applikationen bereitstellt. Anknüpfungspunkt der Datenverarbeitung muss dabei nicht die Diebstahlsaufklärung sein, sondern kann auch – nach Entscheidung der Tracking-Berechtigten – die Auswertung gefahrener Strecken etc. sein.
- Betreiber*in des *FindMyBike-System* (kurz: System-Betreiber*in): Dies könnte ebenfalls eine Firma oder eine sonstiger Betreiber*in (z. B. ein Verein) sein. Die Aufgabe besteht speziell in der Verarbeitung und Übertragung

der Trackingdaten an die Polizei im Falle eines Diebstahls. Dieser Service muss sich nicht auf ortbare Fahrräder beschränken, sondern kann für zahlreiche Gegenstände (Autos, Mobiltelefone etc.) zur Verfügung gestellt werden. Der Trackingservice-Anbieter sowie der Betreiber eines Systems zur Übertragung von Positionsdaten an die Polizei könnten auch übereinstimmen,[7] von einem solchen Fall wird vorliegend aber nicht ausgegangen.
- Polizei
- Dieb*innen bzw. Hehler*innen.

## 3. Datenschutzrechtliche Anforderungen an die Erhebung von Trackingdaten und ihre Übermittlung an die Polizei

Die datenschutzrechtlichen Vorgaben folgen für die beteiligten Akteure aus unterschiedlichen Gesetzen. Für die privaten Trackingservice-Anbieter*innen, die Tracking-Berechtigten sowie für die Betreiber*in des FindMyBike-Systems folgen die Datenschutzgrundsätze aus Art. 5 DS-GVO, dessen Vorgaben in verschiedenen Normen konkretisiert werden. Art. 5 DS-GVO enthält die allgemeinen datenschutzrechtlichen Grundprinzipien, die zugleich Konkretisierungen der grundrechtlichen Vorgaben aus Art. 8 Abs. 2 GRCh und Art. 8 EMRK sind. Für die Polizei ergeben sich datenschutzrechtliche Grundsätze im Rahmen der strafverfolgenden Tätigkeit aus § 47 BDSG, wobei diese im Lichte der europarechtlichen Vorgaben aus der Richtlinien (EU) 2016/680 (JI-Richtlinie) auszulegen sind.[8] Auch diese Grundsätze werden teilweise durch speziellere Regelungen konkretisiert.[9] Die Grundsätze aus DS-GVO und BDSG/JI-Richtlinie weisen zahlreiche Parallelen auf,[10] auch wenn es Unterschiede im Detail gibt.[11]

Im Folgenden wird die Umsetzung der Datenschutzgrundsätze im *FindMyBike-System* und im gesamten Datenverarbeitungsvorgang von der Erhebung bis zur Übertragung an die Polizei erörtert und analysiert. Dabei konnten nicht alle möglichen technischen Funktionen im *FindMyBike-System* umgesetzt werden, da einige Spezifikationen davon abhängen, ob und inwieweit das System mit dem jeweiligen polizeilichen System verknüpft wird. Sofern eine Ver-

7 Wie etwa die Firma Ubinam; https://www.ubinam.de/ (letzter Aufruf: 20.07.2023).
8 Zur Abgrenzung von DS-GVO und BDSG Johannes/Weinhold 2018, S: 52; Schantz/Wolff-Wolff 2017, S. 75 f.; Kühling/Buchner-Schwichtenberg 2020, § 45 Rn. 3 f. m. w. N.
9 Johannes/Weinhold 2018, S. 63 f.
10 Paal/Pauly-Frenzel 2021, BDSG § 47, Rn. 3; Johannes/Weinhold 2018, S. 6; vgl. Johannes ZD-Aktuell 2017, 05852; Kühling/Buchner-Schwichtenberg 2020, § 47 Rn. 2.
11 Vgl. z. B. Johannes, ZD-Aktuell 2019, 06875; Aden/Fährmann, TATuP 2020, S. 26.

knüpfung erforderlich ist, werden diesbezüglich Vorschläge formuliert. Auch bzgl. der Erhebung der Positionsdaten durch Trackingservice-Anbieter*innen werden Vorschläge erarbeitet, um ein hohes Datenschutzniveau sicherzustellen. Hinsichtlich des *FindMyBike-Systems*, welches losgelöst von den polizeilichen Datenverarbeitungssystemen funktioniert, sind die Funktionen zur Umsetzung der Datenschutzgrundsätze alle in der im Forschungsprojekt konzipierten Software implementiert.

Im Folgenden werden die Datenschutzgrundsätze zunächst beschrieben und danach erläutert, wie diese in dem *FindMyBike-System* umgesetzt wurden, bzw. wie sie bei der Trackingservice-Anbieter*in und bei einer Verknüpfung mit dem polizeilichen IT-System umgesetzt werden könnten.

### *3.1 Privacy bei Design and Default*

Zunächst ist auf die Grundsätze „Privacy by Design" und „Default" einzugehen. „Privacy by Design" bedeutet nach Art. 25 Abs. 1 DS-GVO bzw. 71 BDSG,[12] dass technische Anwendungen so ausgestaltet werden müssen, dass die Datenschutzgrundsätze effektiv umgesetzt werden.[13] Dazu müssen nicht nur zum Zeitpunkt der eigentlichen Verarbeitung, sondern bereits bei der Einrichtung der Datenverarbeitungssysteme geeignete technische und organisatorische Maßnahmen getroffen werden, um eine datenschutzrechtskonforme Datenverarbeitung zu unterstützen oder zu ermöglichen. Damit soll erreicht werden, dass die Einhaltung datenschutzrechtlicher Grundsätze möglichst nicht von Entscheidungen der Nutzer*innen abhängt, sondern das IT-System bereits im Design nur eine rechtskonforme Nutzung zulässt.[14] Privacy by Default bedeutet, dass Datenverarbeitungsprozesse so voreinzustellen sind, dass ein möglichst optimaler Datenschutz gewährleistet wird (z. B. im Sinne der Datenminimierung so wenig Daten wie möglich erhoben werden), die Nutzer*innen sich also nicht erst aktiv für datenschutzfreundliche Einstellungen entscheiden müssen, Art. 25 Abs. 2 DS-GVO.[15]

Im *FindMyBike-System* wird durch technische Voreinstellungen und Funktionen sichergestellt, dass die Datenschutzgrundsätze soweit wie möglich automatisch umgesetzt werden, indem Daten nur über einen gewissen Zeitraum an die Polizei übertragen, Positionsdaten im System nur übergangsweise und nicht

12 BT-Drs. 18/11325, S. 118.

13 Baumgartner/Gausling, ZD 2017, S. 310; Auernhammer-Kramer/Meints 2020, Art. 24 Rn. 1.

14 Anwendungsbeispiele bei Fährmann, MMR 2021, S. 778 ff.; Bosch/Fährmann/Aden, ZKKW 2021, S. 206 ff.

15 Schenk/Mueller-Stöfen, GWR 2017, S. 177; Auernhammer-Brüggemann 2020, Art. 25 Rn. 23; Gola/Heckmann-Nolte/Werkmeister 2022, Art. 25 Rn. 27.

dauerhaft gespeichert, Bewegungsdaten nur auf Anforderungen an die Polizei übertragen und Daten im System pseudonomisiert und verschlüsselt werden. Auf die genaue Umsetzung wird bei dem jeweiligen Datenschutzgrundsatz eingegangen.

### *3.2 Zweckbindung*

Der Zweckbindungsgrundsatz, der bereits in den 1980er Jahren durch das Bundesverfassungsgericht etabliert wurde,[16] besagt, dass personenbezogene Daten nur für eindeutig festgelegte, rechtmäßige Zwecke erhoben und weiterverarbeitet werden dürfen (Art. 5 Abs. 1 b DS-GVO). Bei offener Datenerhebung kennen die Betroffenen in der Regel den Erhebungszweck. So ist z. B. beim Einbau eines GPS-Senders in ein Fahrrad oder einen anderen mobilen Gegenstand bekannt, dass der Sender die Ortung des Gegenstands ermöglicht. Der Zweckbindungsgrundsatz schützt das Vertrauen der Betroffenen, dass bei der Verarbeitung keine anderen, ihnen unbekannte Nutzungszwecke hinzukommen.

#### *3.2.1 Datenübertragung durch das FindMyBike-System an die Polizei*

Das *FindMyBike-System* stellt eine Software-Schnittstelle zur Polizei dar, damit die Positionsdaten gestohlener Fahrräder an die Polizei übertragen werden können. Da durch die Betätigung der Pedale die aufladbaren Batterien von GPS-Sendern immer wieder aufgeladen werden können, bestünde die Möglichkeit, dass für längere Zeit weiterhin Positionsdaten an die Polizei übertragen werden. Daher muss im *FindMyBike-System* sichergestellt werden, dass die Daten nur solange an die Polizei übertragen werden, wie sie für die Strafverfolgung bzw. straftatenbezogene Gefahrenabwehr, d. h. die Wiedererlangung des gestohlenen Fahrrades, benötigt werden. Wenn z. B. das Fahrrad wiedergefunden und an die rechtmäßigen Eigentümer*innen oder andere Berechtigten zurückgegeben wurde, muss die Datenübertragung an die Polizei beendet werden, was im Sinne von Privacy by Design möglichst sowohl im *FindMyBike-System* als auch in der polizeilichen IT technisch angelegt sein sollte.

Technisch voreingestellte zeitliche Grenzen könnten sich an den Verjährungsregeln für die Verfolgbarkeit des Diebstahls orientieren.[17] Eine Datenübertragung der Live-Positionsdaten an die Polizei kann nur solange erfolgen, wie der Diebstahl auch verfolgt werden kann, d. h. nach §§ 78 Abs. 3 Nr. 5 i. V. m. 242 Abs. 1 StGB üblicherweise drei Jahre. Dies erscheint allerdings zu lang. Einerseits ist nicht zu erwarten, dass die Polizei nach einem längeren

16 BVerfGE 65, 1 (Volkszählungsentscheidung).

17 Vgl. Keppeler/Berning, ZD 2017, S. 315 m. w. N.

Zeitraum noch eine Verfolgung beginnt, da in diesem Fall das Fahrrad oft nicht mehr im Zugriffsbereich der Polizei befindet oder bereits in seine Einzelteile zerlegt wurde. Gleichzeitig ist kaum noch mit einer wirksamen Ermittlungsarbeit zu rechnen, u. a. weil sich etwaige Zeug*innen in der Regel nicht mehr erinnern werden oder andere Spurenansätze nicht mehr verfolgt werden können. Allerdings könnte die Polizei auch nach einem längeren Zeitraum das Fahrrad immer noch im Rahmen der Gefahrenabwehr zurückholen, jedenfalls solange das Fahrrad nicht ins Ausland verbracht wurde. Auch könnte es sein, dass das Fahrrad länger steht und deswegen nicht geortet werden kann. Wenn aber dann der Akku wieder durch den Betrieb des Dynamos aufgeladen wird, könnte das Fahrrad wieder geortet werden. Der Betreiber des *FindMyBike-Systems* und die Trackingservice-Anbieter*in stehen damit vor dem Problem, dass sie selbst nicht beurteilen können, wie lange die Daten für die polizeilichen Verfahren von Bedeutung sind.

Ein gangbarer Weg könnte sein, dass das System nach sechs und neun Monaten automatisch anfragt, ob das Verfahren noch läuft, was von Polizei-Seite in der Fallbearbeitungssoftware zu bestätigen ist. Im Sinne eines wirkungsvollen Datenschutzes sind auch kürzere Zeiträume denkbar. Hierzu könnte etwa ein Dialogfenster in die Web-View integriert und möglicherweise in das polizeiliche Vorgangsbearbeitungssystem eingebunden werden. Nach einem Jahr sollte die Datenübertragung eingestellt werden, und es bedarf dann einer erneuten Aufforderung durch die Polizei oder die Tracking-Berechtigten zur Wiederaufnahme der Übertragung. So hat die Polizei einerseits die Möglichkeit, bei konkreten Hinweisen den Sachverhalt weiter aufzuklären, gleichzeitig wirkt das System darauf hin, unnötige Datenverarbeitungsprozesse zu beenden (Privacy by Design). Die Festlegung von Zeiträumen für den Abbruch der Datenübertragung ist im *FindMyBike-System* vorgesehen, sollte aber an den jeweiligen Workflow der Polizeien bei der Diebstahlsbearbeitung individuell angepasst werden.

Zudem ist den Tracking-Berechtigten bekannt, ob die Ermittlungsverfahren noch laufen. Werden sie als Geschädigte von der zuständigen Staatsanwaltschaft über die Einstellung des Verfahrens informiert, so sind sie verpflichtet, den Übertragungsvorgang abzubrechen, soweit dies nicht bereits die Polizei veranlasst hat, da die Daten nunmehr nicht mehr seitens der Polizei benötigt werden. Dementsprechend muss auch eine Abbruchmöglichkeit der Übertragung für den Bestohlenen vorhanden sein, etwa in der jeweiligen App der Trackingservice-Anbieter*in. Sofern das *FindMyBike-System* mit einem polizeilichen Datenverarbeitungssystem verknüpft ist, könnte ein Abbruch erfolgen, wenn die Polizei das Verfahren abschließt und an die Staatsanwaltschaft gibt.

### *3.2.2 Datenerhebung durch die Trackingservice-Anbieter*

Die Datenverarbeitung durch die Trackingservice-Anbieter*in kann mit Blick auf den Diebstahlsfall zwei Zwecke verfolgen, die rechtlich getrennt zu betrachten sind. Die Trackingservice-Anbieter*in erhebt die Daten, damit die Tracking-Berechtigten ihr Fahrrad wiedererhalten. Dies kann einerseits durch die Polizei andererseits aber auch auf dem zivilgerichtlichen Wege geschehen, d. h. die Tracking-Berechtigten können versuchen einen Herausgabetitel zu erlangen, wenn ihnen bekannt ist, wer das gestohlene Fahrrad in Besitz genommen hat. Alternativ können die Bestohlenen Schadensersatz verlangen, falls ihnen eine zu verklagende Person, insbesondere die Dieb*in bekannt ist. Insofern ist vom DS-GVO-konform verfolgten Zweck erfasst, dass die Daten solange erhoben werden, bis die Bestohlenen ihr Fahrrad zurückerhalten, bzw. bis sie das Fahrrad einer Person eindeutig zugeordnet haben.

Zivilrechtlich verjähren Herausgabeansprüche und andere dingliche Rechte erst nach 30 Jahren, siehe § 197 Abs. 1 Nr. 2 BGB. Dementsprechend könnte auch gerechtfertigt sein, die Daten solange durch den Trackingservice-Anbieter erheben zu lassen. Dies ist aber gerade im Hinblick darauf, dass es wahrscheinlich ist, dass das Fahrrad innerhalb von 30 Jahren – sollte es solange benutzbar sein - mehrfach die Besitzer*innen wechselt, höchst problematisch, da so diese meist über einen sehr langen Zeitraum beobachtet werden können. Geht es nur um die Herausgabe des Fahrrades oder um Schadensersatzansprüche, so sollten diese aufgrund des schnellen Wertverlustes von Fahrrädern zeitnah geltend gemacht werden. Wie lange eine Erhebung zur Förderung eines zivilrechtlichen Verfahrens erfolgen sollte, lässt sich aber nicht abstrakt, sondern nur im Einzelfall beurteilen. Sofern sich aus den Gesamtumständen ergibt, dass ein zivilrechtlicher Herausgabeanspruch nicht ernsthaft verfolgt wird, ist die Datenerhebung rechtswidrig. Dafür würde sprechen, dass über einen längeren Zeitraum weder zivilrechtliche Ansprüche geltend gemacht werden, noch die Polizei informiert wird. Dies wird oft spätestens nach sechs bis neun Monaten naheliegend sein. Daher sollten auch in diesem Fall die technischen Voreinstellungen die Übertragung zeitlich begrenzen und die Wiederaufnahme an gesondert zu begründende Software-Befehle geknüpft werden.

## *3.3 Transparenz*

Der Grundsatz der Transparenz gewährleistet, dass Betroffene Datenschutzvorgänge nachvollziehen können. Das Gebot der Transparenz bezweckt ein umfassendes Angebot an Informationen gegenüber den Betroffenen über die

Datenverarbeitung.[18] Dadurch soll ein effektiver Daten- und Rechtsschutz gewährleistet werden, da die betroffenen Personen nur so wirksam von ihrem Recht auf informationelle Selbstbestimmung Gebrauch machen können und so die Möglichkeit erhalten, entweder die Datenerhebung zuzulassen oder sich gegen diese zur Wehr zu setzen.[19]

Für die polizeiliche Arbeit gibt es kein umfassendes Transparenzgebot, was bereits aus zahlreichen Ermächtigungen zur heimlichen Überwachung in der StPO folgt.[20] D. h. aber nicht, dass die Polizei keine Pflichten zum transparenten Handeln hat, diese folgen vielmehr aus zahlreichen Vorschriften sowie verfassungsrechtlichen Vorgaben.[21] Entsprechende Pflichten bestehen aber oftmals nicht während der strafrechtlichen Ermittlung bzw. nur bei offenen Ermittlungsmaßnahmen unter die eine Ortung regelmäßig nicht fällt. Hinsichtlich der Polizei werden sich bei dem Anwendungsfall des *FindMyBike-Systems* regelmäßig nur nachträgliche Informationspflichten ergeben.

Allerdings muss nach der DS-GVO die Datenverarbeitung transparent ablaufen, Art. 5 Abs. 1 a und 13 ff. DS-GVO. Eine Datenverarbeitung nach dem Fairness-Grundsatz setzt voraus, dass Datenverarbeiter*innen den betroffenen Personen ermöglichen, von der Datenverarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden.[22]

Insofern stellt sich die Frage, inwieweit die heimliche Beobachtung von den Bewegungen von Diebesgut überhaupt mit der DS-GVO zu vereinbaren ist. In Teilen der Literatur wird davon ausgegangen, dass durch die Transparenz- und Informationspflichten der DS-GVO ein prinzipielles Verbot heimlicher Überwachung begründet wird.[23] Verdeckte Beobachtungen wären demnach nur möglich, wenn das Transparenzgebot durch einen Rückgriff auf Art. 23 Abs. 1 DS-GVO oder durch Normen beschränkt wird, die aufgrund von der Öffnungsklausel aus Art. 88 DS-GVO erlassen werden.[24] Weder ist aber Art. 88 DS-GVO einschlägig, noch sind Regelungen nach Art. 23 Abs. 1 DS-GVO erlassen worden, sodass heimliche Überwachungen nach der DS-GVO nicht gestattet wären.

---

18 Vgl. Ehmann/Selmayr-Heberlein 2018, Art. 5, Rn. 11 f.

19 Paal/Pauly- Frenzel 2021 , DS-GVO Art. 5 Rn. 21; Gierschmann/Schlender/Stentzel/Veil-Veil 2018, Art. 13 und 14, Rn. 2; Ehmann/Selmayr-Heberlein 2018, Art. 5, Rn. 11.

20 Erwägungsgrund 26 zur Justiz Richtlinie.

21 Aden/Fährmann/Bosch 2020, S. 6 ff.; Aden/Fährmann, TATuP 2020, S. 24 ff.

22 Gierschmann/Schlender/Stentzel/Veil-Veil 2018, Art. 13 und 14, Rn. 2.

23 Kühling/Buchner-Herbst 2020, Art. 5 Rn. 18; Byers, NZA 2017, S. 1887 f.; vgl. Ehmann/Selmayr-Heberlein 2018, Art. 5, Rn. 11.

24 Vgl. Kort, RdA 2018, S. 31; Byers NZA 2017, S. 1887 ff.; Lachenmann, ZD 2017, S. 411; Kühling/Buchner-Bäcker 2020, Art. 13 Rn. 14.

Allerdings könnte die DS-GVO auch so auszulegen sein, dass heimliche Überwachungen nicht grundsätzlich ausgeschlossen sind. Dafür könnte Art. 6 Abs. 1 f DS-GVO sprechen, der die zentrale Abwägungsklausel der DS-GVO darstellt.[25] Nach dieser Norm ist eine Interessenabwägung durchzuführen, bei der die jeweiligen Interessen der Beteiligten zu gewichten sind. Ein ausnahmsloses Verbot von heimlichen Kontrollen würde eine Interessenabwägung in Konstellationen unmöglich machen, in denen eine Partei die andere nicht kennt. So zeigt etwa der Diebstahl von Gegenständen, die geortet werden können, dass in diesem Bereich eine Interessenabwägung notwendig ist, da vielfach die Bestohlenen keine andere Möglichkeit haben, die entwendeten Gegenstände anders zurückzuerhalten. Bei einem ausnahmslosen Verbot von heimlicher Überwachung würde das aus Art. 14 Abs. 1 GG erwachsene Interesse am Schutz des Eigentums gänzlich unberücksichtigt bleiben. Es sind aber auch weitere Konstellationen denkbar, in denen das berechtigte Interesse an einer heimlichen Überwachung, die Interessen der Betroffenen überwiegen kann.[26] Verdeckte Überwachungen können etwa das einzige effektive Mittel sein, um einen konkreten Straftatverdacht im Unternehmen nachzugehen[27] oder um zivilrechtliche Ansprüche zu beweisen.[28] Dieb*innen können zudem damit rechnen, dass Fahrräder und anderes Diebesgut ortbar sind, da es entsprechende technische Lösungen und Produkte mittlerweile seit geraumer Zeit gibt. Vor dem Hintergrund, dass Dieb*innen Überwachungsrisiken kennen und diese in Kauf nehmen, werden ihre Interessen vielfach kaum überwiegen. Daher wird eine umfassende Berücksichtigung der Interessen, insbesondere der Eigentümer*innen oder anderer Berechtigter, nur dann ermöglicht, wenn eine Bewertung der Verhältnismäßigkeit im konkreten Einzelfall nicht pauschal ausgeschlossen wird.[29] Andernfalls wäre es nicht möglich, Eigentum und Besitz wirksam durch Ortungsfunktionen zu schützen, die auch eine präventive Wirkung entfalten können, gerade, wenn Dieb*innen die Sender nicht ohne weiteres stören oder entfernen können.

Auch deutet der Wille der Legislative darauf hin, dass heimliche Maßnahmen nicht zwingend ausgeschlossen sind. Aus dem Erwägungsgrund 47 Satz 3 geht hervor, dass bei der Interessenabwägung zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Datenverarbeitung erfolgen wird. Daraus wird

25 Byers, NZA 2017, S. 1089; vgl. Gola/Heckmann-Schulz 2022, DS-GVO Art. 6 Rn. 59.
26 Z. B. BAG NJW 2012, 49/2012, S. 3594 (3596).
27 Byers, NZA 2017, S. 1090.
28 Z. B. BGH NZV 2018, 08/2018, S. 367 (370 ff.) m. w. N.
29 Vgl. Byers, NZA 2017, S. 1090.

deutlich, dass auch heimliche Datenerhebungen vorgesehen sind, da diese Erwägung bei einer zwingenden Transparenz keinen Anwendungsfall hätte.

Zusätzlich lässt sich die Zulässigkeit von heimlichen Kontrollen im Einzelfall auch durch eine analoge Anwendung des Ausnahmetatbestands aus Art. 14 Abs. 5 b DS-GVO begründen. Diese Norm bezieht sich auf die Informationspflichten der datenschutzrechtlich Verantwortlichen (Art. 26 DS-GVO ff.), wenn die Datenerhebung bei Dritten und nicht unmittelbar beim Betroffenen erfolgt. Von den Informationspflichten sieht Art. 14 Abs. 5 b DS-GVO eine Ausnahme vor, wenn die vorherige Information der Betroffenen die Verwirklichung der Ziele der Datenverarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde. In Art. 13 DS-GVO, der die Informationspflichten der Verantwortlichen bei der direkten Datenerhebung regelt, fehlt eine solche Ausnahmeregelung, womit eine Regelungslücke vorliegt. Es ist auch davon auszugehen, dass diese planwidrig ist, da kein nachvollziehbarer Grund ersichtlich ist, weshalb bei der Datenerhebung bei Betroffenen keine Ausnahme von der Informationspflicht aus Art. 13 Abs. 1 DS-GVO gemacht werden kann, wenn die Informationen den Zweck der Datenerhebung vereiteln oder ernsthaft beeinträchtigen würden.[30] Diese Lücke erscheint zudem im vorliegenden Anwendungsfall besonders widersprüchlich, da es bei der Ortung gestohlener Gegenstände gar nicht möglich wäre, die Informationsverpflichtung einzuhalten, da die Ortung gerade dazu dient, die Dieb*innen aufzuspüren. Entsprechende Fallkonstellationen sind offenbar in der DS-GVO nicht mitgedacht worden. Es ist jedoch kaum vorstellbar, dass mit der DS-GVO bezweckt wird, Dieb*innen bzw. unberechtigte Besitzer*innen in ihrer rechtswidrigen Besitzposition umfassend zu schützen und damit die Aufklärung von Diebstählen mittels Positionsdaten unmöglich zu machen. Wäre diese Konstellation mitgedacht worden, hätte die Legislative für die Konstellation eine Ausnahmeregelung gestaltet.

Insgesamt steht die DS-GVO dem nicht-offenen Tracken gestohlener Fahrräder durch Privatpersonen oder –firmen sowie der Datenübertragung an die Polizei grundsätzlich nicht entgegen. Da die Interessen der Dieb*innen hier nicht überwiegen und Transparenz gegenüber den vom Tracking Betroffenen kaum gewährleistet werden kann, sind keine besonderen Transparenzanforderungen im *FindMyBike-System* umzusetzen. Anders ist dies indes zu beurteilen, wenn die Datenerhebung durch die Polizei erfolgt, die an die aus rechtsstaatlichen Gründen engeren Voraussetzungen der Strafprozessordnung gebunden ist.

Es wäre wünschenswert, wenn der Gesetzgeber von seinen Regelungsmöglichkeiten aus Art. 23 Abs. 1 DS-GVO Gebrauch machen würde. So könnten die Grenzen und die Pflichten im Zusammenhang mit einer heimlichen Datenerhebung eindeutiger festgelegt werden. Die bisherigen Ausführungen zeigen,

30 Byers, NZA 2017, S. 1090.

dass eine heimliche Datenerhebung in gewissen Konstellationen notwendig sein und auf die Betroffenenrechte unterschiedlich umfangreiche Auswirkungen haben kann. Da diese aber auch sehr eingriffsintensiv sein kann,[31] sollten dafür klare Regelungen bestehen.[32] Die Legislative könnte sich dabei etwa auf Art. 23 Abs. 1 d, j oder die Generalklausel aus e[33] stützen.

### *3.4 Datenminimierung, Speicherbegrenzung und Löschkonzepte*

Eine besondere Bedeutung für den Datenschutz hat der Grundsatz der Erforderlichkeit. Die Erhebung, Verarbeitung und Übermittlung personenbezogener Daten ist nur dann gestattet, wenn sie zur rechtmäßigen Aufgabenerfüllung der datenverarbeitenden und erhebenden Stelle für den jeweils damit verbundenen Zweck das mildeste, gleich geeignete Mittel ist. Gerade bei der automatisierten Verarbeitung personenbezogener Daten ist ein Verfahren auszuwählen oder zu entwickeln, welches die zur Zweckerreichung nötige Menge personenbezogener Daten so gering wie möglich hält. Diese Gedanken drücken sich im Grundsatz der Datenminimierung oder der Datensparsamkeit aus, Art. 5 Abs. 1 c DS-GVO. Der Grundsatz der Datenminimierung stellt einen zentralen Grundsatz des Datenschutzrechts dar[34] und drückt sich in verschiedenen Vorschriften aus und wird dort konkretisiert.[35]

Art. 5 Abs. 1 c DS-GVO vereint insgesamt drei eng miteinander verbundene Anforderungen unter dem Begriff der Datenminimierung. Personenbezogene Daten müssen für den mit der Erhebung und Verarbeitung verfolgten Zweck angemessen und erheblich sein und dabei zweckorientiert auf das nötige Maß beschränkt werden.[36] Dem Zweck angemessen sind Daten dann, wenn ihre Zuordnung zu dem angestrebten Zweck nicht zu beanstanden ist.[37] Aus der Kombination von Angemessenheit und Erheblichkeit ergibt sich schließlich, dass die Daten nicht nach der Präferenz der datenschutzrechtlich Verantwortlichen erhoben und verarbeitet werden dürfen, sondern vielmehr für die Zweckerreichung förderlich sein müssen.[38] Das Wort „Minimierung" schreibt eine möglichst weite Begrenzung vor,[39] die Anforderungen wurden insofern mit der DS-GVO gegenüber der vorherigen Rechtslage konkretisiert und verschärft.

31 Z. B. BVerfG NJW 2016, 25/2016, 1781 (1785).
32 Vgl. Byers, NZA 2017, S. 1088.
33 Paal/Pauly-Paal 2021, Art. 23 Rn. 31a.
34 Vgl. Simitis-Scholz 2014, § 3 a Rn. 1.
35 Ehmann/Selmayr-Hebelein 2018, Art. 5 Rn. 23.
36 Paal/Pauly-Frenzel 2021, Art. 5 Rn. 34.
37 Schantz/Wolff 2017, Rn. 421.
38 Paal/Pauly-Frenzel 2021, Art. 5 Rn. 36.
39 Paal/Pauly-Frenzel 2021, Art. 5 Rn. 34.

Also sind so wenige Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.[40] Der Grundsatz Datenminimierung lässt sich bereits beim Design eines IT-Systems umsetzen, indem das System so konzipiert wird, dass nur die Eingaben zugelassen werden, die für den Verarbeitungszweck unbedingt erforderlich sind. Insofern hängen Datenminimierung und *Privacy by Design* eng zusammen.

In § 47 Nr. 3 BDSG wird zwar nicht explizit von dem Grundsatz der Datenminimierung gesprochen, jedoch ergibt sich dieser Grundsatz aus dieser Norm und weiteren des BDSG und der JI-Richtlinie. So wird in § 47 Nr. 3 BDSG betont, dass von mehreren gleich geeigneten Maßnahmen stets diejenige zu wählen ist, die den geringsten Eingriff darstellt.[41] Dieser Grundsatz drückt sich auch in § 483 Abs. 1 StPO aus, nach dem nur Daten gespeichert werden dürfen, die für das Strafverfahren erforderlich sind. Auch wird in § 71 Abs. 1 Satz 1 BDSG von dem Grundsatz der Datensparsamkeit gesprochen, der mit der Datenminimierung teilidentisch ist. Zudem sind die in der JI-Richtlinie vorgeschriebenen Datenschutzgrundsätze wie die Datenminimierung im Hinblick auf den Anwendungsvorrang des Rechts der EU wirksam umzusetzen,[42] was für das gesamte BDSG gilt, unabhängig davon, ob der Anwendungsbereich der JI-Richtlinie oder der DS-GVO betroffen ist.

Der Grundsatz der Datenminimierung wird in zeitlicher Hinsicht durch den Grundsatz der Speicherbegrenzung aus Art. 5 Abs. 1 e DS-GVO ergänzt.[43] Die eigenständige Betonung dieses Grundsatzes neben dem Grundsatz der Datenminimierung verleiht ihm ein besonderes Gewicht.[44] Aus ihm resultieren Pflichten zur Definition der für die jeweiligen Daten im Hinblick auf den konkreten Verarbeitungszweck erforderlichen Speicherdauer sowie Löschpflichten, die in Art. 17 DS-GVO zugleich als Löschanspruch der Betroffenen ausgestaltet sind. Zugleich folgt aus dem Zweckbindungsgrundsatz, dass keine Löschpflicht besteht, solange ein mit der Verarbeitung verfolgter rechtmäßiger Zweck vorliegt. Die sich aus der Verpflichtung zur Löschung ergebenden und anzuwendenden Löschfristen sind zu dokumentieren und nachzuweisen.[45]

Gerade bei den Grundsätzen der Datenminimierung und Speicherbegrenzung haben datenschutzfreundliche Voreinstellungen von Systemen eine beson-

40 Vgl. Landessozialgericht Berlin-Brandenburg, Urteil vom 01. Dezember 2011 – L 3 U 7/10 –, Rn. 48.

41 Wolff/Brink-Hertfelder Stand 2021, BDSG, § 47 Rn. 18; vgl. Johannes/Weinhold 2018, S. 66; Schantz/Wolff 2017, Rn. 440.

42 BT-Drs 18/11325, S. 98; Kühling/Buchner-Schwichtenberg 2020. § 47 BDSG Rn. 2.

43 Albrecht/Jotzo 2017, S. 52 f.; Wolff/Brink Stand-Schantz 2018, DS-GVO Art. 5 Rn. 32.

44 Wolff/Brink Stand-Schantz 2021, DS-GVO Art. 5 Rn. 32; vgl. Erwägungsgrundsatz 39 Satz 8.

45 Keppeler/Berning, ZD 2017, S. 315.

dere Bedeutung, die sich auch im *FindMyBike-System* niederschlagen müssen, Art. 25 Abs. 1 und Abs. 2 DSGVO[46] bzw. §§ 47 Nr. 3 und 71 BDSG. Daraus folgt, dass das *FindMyBike-System* und damit zusammenhängenden Systeme zur Verarbeitung von Positionsdaten bereits so zu gestalten sind, dass so wenig wie möglich personenbezogene Daten erhoben werden und gleichzeitig ein angemessenes Konzept für eine soweit wie möglich automatisierte Löschung besteht.[47]

### *3.4.1 Live-Postions- und Bewegungsdaten im FindMyBike-System*

Die Datenverarbeitung im *FindMyBike-System* dient dem Zweck, die Positionsdaten gestohlen gemeldeter Fahrräder an die Polizei zu übertragen, um die Strafverfolgung und eine Wiedererlangung des Fahrrades zu ermöglichen. Mithin sind nach dem Grundsatz der Datenminimierung nur die Daten zu übertragen, die für die Ermittlungsarbeit bzw. die Gefahrenabwehr notwendig sind. Dabei ist zwischen Live-Positionsdaten und gespeicherten Bewegungsdaten zu unterscheiden.

Um eine Live-Ortung zu ermöglichen, werden Live-Positionsdaten an die Polizei übertagen. Diese beinhalten den jeweils letzten, durch das Tracking der Positionsdaten bekannten Standort des gestohlenen Fahrrades (geographische Länge und Breite), den zugehörige Zeitstempel sowie einen Wert, der die Genauigkeit der jeweiligen Standortbestimmung beschreibt (*accuracy*). Diese Daten können als Kreis um einen Punkt (mit den oben erwähnten geographischen Koordinaten) visualisiert werden. Der Radius des Kreises entspricht dem Wert der *accuracy* in Metern. Weiterhin wird der genaue Zeitpunkt der letzten Standortbestimmung übermittelt. Diese Daten sind für die Ermittlungsarbeit erforderlich, weil die Polizei im Regelfall keine anderen Ansätze für das Ermittlungsverfahren bei gestohlenen Fahrrädern hat, soweit nicht ausnahmsweise andere Tatspuren oder Zeug*innen verfügbar sind. Die Kenntnis über den Standort des Fahrrades ermöglicht der Polizei nicht nur einen ersten Ermittlungsansatz, sondern kann im besten Falle zum Aufspüren der Dieb*innen führen, wenn diese das Fahrrad im Besitz haben.

Der Grundsatz der Datenminimierung wird im *FindMyBike-System* umgesetzt, indem die Ortungsdaten nur im Arbeitsspeicher verbleiben und nach der Speicherung eines (über den entsprechenden Datensatz berechneten) Hashwertes nicht dauerhaft gespeichert werden. Damit findet kein aktives Speichern von Ortungsdaten im *FindMyBike-System* statt. Aus dem Hashwert allein ergibt sich kein Personenbezug. Der Hashwert ermöglicht die Authentizität der

46 Baumgartner/Gausling, ZD 2017, S. 312.
47 Keppeler/Berning, ZD 2017, S. 318.

Daten nachzuweisen, was insbesondere für die Beweisqualität der Daten in einem späteren Strafverfahren relevant ist.[48] Zwar kann es aus Gründen des Integritätsschutzes (Datensicherung) sinnvoll sein, die Datensätze an mehreren Stellen zu speichern. Dies erfordert aber nicht zwingend, eine Speicherung bei unterschiedlichen Akteuren. Durch eine solche Speicherung wird zudem dem Grundsatz der Datenminimierung widersprochen und das Risiko eines illegalen Zugriffs erhöht. Eine sichere Speicherung mit den üblichen Backups beim Trackingservice-Anbieter reicht vorliegend aus. So ist gewährleistet, dass das *FindMyBike-System* selbst datenarm ausgestaltet ist, und es auch keines gesonderten Löschkonzepts bedarf, da die Daten nicht im *FindMyBike-System* verbleiben.

Durch den Umstand, dass im *FindMyBike-System* selbst keine Daten gespeichert werden, wird dem Grundsatz der Datenminimierung noch nicht vollständig entsprochen, da das System die Übertragung von beim Trackingservice-Anbieter gespeicherten Bewegungsdaten an die Polizei ermöglicht. Daher muss das System aus Gründen der Datenminimierung eine solche Datenübertragung nur dann umsetzen, wenn und solange die Polizei die Bewegungsdaten zwingend benötigt. So wird sichergestellt, dass die Daten auf das notwendige Mindestmaß beschränkt werden und gleichzeitig die Systeme der Polizei nicht mit unnötigen Daten belastet werden. Andernfalls bestünde auch ein Risiko, dass die Polizei aufgrund der Datenmenge relevante Hinweise übersieht[49] oder dass die Daten irrtümlich in den polizeilichen Systemen für andere Zwecke verarbeitet werden. Gleichzeitig wird so einer Speicherung auf Vorrat entgegengewirkt, da die Polizei selbst aktiv werden muss, um die Daten zu erlangen. Ein Abbruch des Vorganges wird durch den Vorgang ermöglicht, der unter 3.2.1 beschrieben wird.

Da nur die Polizei erkennen kann, wann die Bewegungsdaten für das Ermittlungsverfahren erforderlich sind, muss die Polizei diese über das *FindMyBike-System* anfordern. Eine automatische Übersendung wäre mit dem Grundsatz der Datenminimierung unvereinbar. Dies wurde im *FindMyBike-System* umgesetzt.

### *3.4.2 Speicherung der Bewegungsdaten bei der Polizei und beim Trackingservice-Anbieter*

Die stärkste Beeinträchtigung der Betroffenenrechte erfolgt durch die Speicherung der Bewegungsdaten bei Trackingservice-Anbieter*innen und bei der Polizei. Daher muss dort gewährleistet werden, dass die Daten gelöscht werden,

48 Näher hierzu Fährmann/Vollmar/Görlitz in diesem Band, S. 211ff.

49 Vgl. dazu Fährmann, MMR 2020, S. 231ff.

wenn sie nicht mehr für zivil- bzw. das strafrechtliche Verfahren benötigt werden.

Bei der Polizei können die Daten nur gespeichert werden, wenn sie konkret an ein Ermittlungsverfahren anknüpfen, vgl. § 483 Abs. 1 StPO. Die Löschfristen ergeben sich aus § 489 StPO, was sich in erster Linie danach beurteilt, ob die Daten für die Polizeiarbeit (noch) erforderlich sind. Auch die Polizei muss eine Infrastruktur vorhalten, die die Löschung von nicht mehr benötigten und rechtswidrigen Daten umsetzt,[50] vorrangig in einem automatisierten, im System-Design voreingestellten Verfahren. Das *FindMyBike-System* kann durch die beschriebene datensparsame Übertragungsform den Grundsatz der Datenminimierung und der Speicherbegrenzung auch für die polizeilichen Systeme lediglich fördern. Die genaue Umsetzung obliegt aber der Polizei.

Wie lange müssen die Bewegungsdaten aber von Trackingservice-Anbieter*innen für Polizei und Tracking-Berechtigte vorgehalten werden? Es kann sein, dass Fahrradbewegungen länger beobachtet werden müssen, um das Fahrrad oder den Diebstahl einer Person oder Personengruppe zuordnen zu können, insbesondere wenn es darum geht, Rückschlüsse auf bandenmäßige oder gewerbsmäßige Kriminalität zu ziehen. Ferner kann es sein, dass die Polizei das Fahrrad erst nach einiger Zeit auffinden kann, insbesondere, wenn die Polizeiressourcen stark ausgelastet sind. Daher müssen die Daten solange gespeichert werden, wie das Ermittlungsverfahren andauert. Hier ist auch zu beachten, dass eine Veranlassung der Löschung durch die Tracking-Berechtigten bzw. die Trackingservice-Anbieter*in unter Umständen eine Strafvereitlung nach § 258 Abs. 1 StGB bzw. eine versuchte Strafvereitlung[51] darstellen könnte. Die endgültige Löschung von Daten kann eine Vernichtung von Beweisen darstellen.[52] Vor diesem Hintergrund kann, solange das Verfahren läuft, von beiden nicht erwartet werden, dass sie Daten löschen, sodass die Speicherung durch ein Überwiegen der Interessen nach Art. 6 Abs. 1 f DS-GVO gerechtfertigt ist. Sollten allerdings bereits Daten an die Polizei übertragen worden sein, so sollten diese auch von den Trackingservice-Anbieter*innen gelöscht werden, wenn diese nicht für ein zivilrechtliches Verfahren oder für andere rechtlich zulässige Zwecke benötigt werden. Auch hierfür ist eine automatisierte Kennzeichnung der betreffenden Datensätze und die ebenfalls automatisierte Löschung zu empfehlen.

Wenn ein Ermittlungsverfahren mehr als ein Jahr in Anspruch nimmt, sollten sich Trackingsystem-Anbieter*innen und/oder Tracking-Berechtigte an

50 BT-Drs. 18/11325, S. 114 f.

51 Kapp/Schlump, BB 2008, S. 2482.

52 Vgl. Kapp/Schlump, BB 2008, S. 2482; Altenhain/Brunhöber/Cierniak-Cramer 2017, § 258 Rn. 24.

die Polizei wenden, um sicherzugehen, dass die Daten noch benötigt werden. Dazu sollten entsprechende niedrigschwellige Kommunikationsmöglichkeiten geschaffen werden und automatische Meldungen aus dem System erfolgen.

### *3.4.3 Pseudonomysierung personenbezogener Daten im FindMyBike-System*

Ein effektiver Datenschutz kann zudem über eine Pseudonymisierung unterstützt werden. Diese ist Ausdruck der Datenminimierung und kann ein wesentlicher Teil der datenschutzfreundlichen Gestaltung technischer Systeme sein.[53] Art. 4 Nr. 5 DSGVO definiert die Pseudonymisierung als Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen (Schlüssel) nicht mehr einer spezifischen Person zugeordnet werden können. Diese zusätzlichen Informationen müssen gesondert, d. h. räumlich getrennt aufbewahrt werden. Die Informationen und Daten dürfen sich also nicht am selben Ort oder im selben System befinden oder zusammen weitergegeben werden.[54] Beim Einsatz von Pseudonymisierungsverfahren ist stets im Vorfeld zu klären, wer über Zuordnungstabellen bzw. das Verschlüsselungsverfahren verfügen soll, wer das Pseudonym generiert, ob ein Re-Identifizierungsrisiko ausgeschlossen werden kann und unter welchen Voraussetzungen eine Zusammenführung von Schlüssel und den personenbezogenen Daten gestattet ist.[55] Auch setzt die Pseudonymisierung voraus, dass technische und organisatorische Maßnahmen erfolgen, die die Nichtzuordnung sicherstellen.[56]

Ob eine Pseudonymisierung notwendig und sinnvoll ist, hängt davon ab, ob überhaupt Daten im System enthalten sind, die Rückschlüsse auf Personen zulassen. Die Positionsdaten werden im *FindMyBike-System* nicht gespeichert und können von den Betreibern keiner Person zugeordnet werden, da diese nur als Fall-ID übertragen werden, die keine Zuordnung erlaubt. Diese Fall ID- stellt damit eine Pseudonymisierung dar und setzt sich im *FindMyBike-System* aus einem beliebigen String aus Hexadezimal-Zeichen mit einer Länge von 64 Zeichen zusammen. Insofern ist die ID gegen Rückschlüsse abgesichert.

Insofern sind die Fahrradortungsdaten im *FindMyBike-System* gut geschützt.

Zusätzlich stellt sich die Frage, ob es sinnvoll ist, dass weitere Daten im System enthalten sind, die Rückschlüsse erlauben und ggf. eine Pseudonymisierung notwendig machen. Dies könnten die Daten der Bestohlenen sein. Da das

53 Paal/Pauly-Ernst 2021, DS-GVO Art. 4, Rn. 41; Marnau, DuD 2016, S. 431 f.
54 Auernhammer-Eßer 2020, Art. 4 Rn. 69; Paal/Pauly-Ernst 2021, DS-GVO Art. 4, Rn. 43.
55 Paal/Pauly-Ernst 2021, DS-GVO Art. 4, Rn. 44.
56 Paal/Pauly-Ernst 2021, DS-GVO Art. 4, Rn. 46.

*FindMyBike-System* eine Softwareschnittstelle darstellt, um Daten an die Polizei weiterzuleiten, sind die Daten der Bestohlenen im System eigentlich nicht erforderlich, da die Polizei selbst über diese Daten aufgrund der Onlineanzeige verfügt. Bei einer Schnittstelle soll nämlich gerade gewährleistet werden, dass diese von verschiedenen Anbietern genutzt werden kann, ohne dass sich das System auf jeden Anbieter gesondert einstellen muss. Daher ist es ausreichend, das System zu konfigurieren, dass die eindeutige Zuordnung der jeweiligen Trackingdaten zu der dazugehörenden Diebstahlsanzeige möglich ist.

Jedoch könnten die Bestohlenen wirksam einwilligen, dass ihre Daten im System hinterlegt werden. Die polizeiliche Fahndung könnte etwa dadurch unterstützt werden, dass – soweit verfügbar – ein Foto oder eine Beschreibung des Fahrrades mit übertragen werden, was die Wahrscheinlichkeit eines Auffindens erhöhen dürfte. Diese Daten müssen aber ebenfalls nicht im *FindMyBike-System,* sondern bei der Polizei gespeichert werden. Die Bestohlenen könnten im Rahmen der Online-Anzeige, ein Bild des Fahrrades und eine Beschreibung an die Polizei senden. Noch effektiver erscheint es, dass die Daten des Fahrrades, inklusive Beschreibung und Foto, bereits im Vorfeld gespeichert werden. Andernfalls besteht die Gefahr, dass die notwendigen Daten bei der Anzeigeerstellung nicht griffbereit sind. Dazu könnte etwa die Fahrradpass-App der Polizei genutzt werden, in der sich sämtliche relevante Daten speichern lassen, die dann im Falle eines Diebstahls leicht an die die Polizei weitergeleitet werden können.[57] Im besten Fall könnte man in dieser App auch noch eine Verbindung zur Onlineanzeige herstellen, sodass die Daten automatisiert mit der Online-Anzeige versandt und automatisch mit dem polizeilichen Vorgang verknüpft werden. Auf die App könnte beim Kauf von GPS-Sendern oder entsprechend ausgestatten Fahrrädern direkt hingewiesen werden.

Hinsichtlich der Trackingservice-Anbieter*innen wäre eine Pseudonymisierung der Daten der Bestohlenen aus datenschutzrechtlichen Gründen sinnvoll, sofern diese nicht für die Abwicklung der vertraglichen Beziehungen vonnöten sind. Dies hängt aber von der Ausgestaltung des konkreten Service ab.

Allerdings ist es gegenwärtig bei der Online-Anzeige an die Berliner Polizei noch nicht möglich, Bilder des gestohlenen Gegenstandes (z. B. Fahrrad) im Rahmen der Onlineanzeige hochzuladen. Allerdings sollte diesem Umstand dringend abgeholfen werden, da dies die Ermittlungstätigkeit, nicht nur bei Fahrrädern, vereinfachen würde. So hätte die Polizei sofort Zugang zu Fotos gestohlener Gegenstände und diese auch digital zur Verfügung, sodass sie bei Bedarf unmittelbar für Fahndungs- und Ermittlungszwecke genutzt werden

57 https://www.polizei-beratung.de/themen-und-tipps/diebstahl-und-einbruch/diebstahl-von-zweiraedern/fahrradpass-app/ (letzter Aufruf: 26.02.2023).

können. Auch lassen sich Polizeibeamt*innen in Ermittlungsverfahren schon oft Bilder und Videos per Mail oder über spezielle Portale zusenden, was den Bedarf verdeutlicht. Für eine effektive Beweissicherung ist es sinnvoll, eine sichere Möglichkeit zur Übertragung von Bildern an die Polizei zu schaffen. Andernfalls müssten die Bürger*innen im Falle von vorhandenen Fotos immer noch extra zur Wache kommen, wodurch es sein kann, dass einige Bilder nicht zur Polizei gelangen. Eine Erleichterung der Arbeit durch die Online-Anzeige würde so nur partiell erreicht. Auch würde dem Grundsatz der Datenminimierung entsprochen, wenn Daten nur dort gespeichert würden, wo sie tatsächlich benötigt werden. Ziel sollte es also sein, der Polizei die für den Diebstahl notwendigen Daten einfach verfügbar zu machen.

### *3.5 Integrität der Daten*

Aus Art. 5 Abs. 1 f DS-GVO und § 47 Nr. 6 BDSG folgt, dass die Integrität und Vertraulichkeit der Daten vor unbefugter oder unrechtmäßiger Verarbeitung und durch geeignete technische und organisatorische Maßnahmen vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung zu schützen ist. Die Schutzmechanismen sind nicht verbindlich festgelegt und orientieren sich am konkreten Einzelfall.[58] Die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Diensten gehören zu den Schlüsselelementen moderner IT-Sicherheitsmechanismen. In der DS-GVO wird der Grundsatz der Integrität in Art. 32 und Art. 24 Abs. 1 DS-GVO konkretisiert.[59] Nach Art. 32 Abs. 1 DS-GVO sind nach dem Risikoprinzip[60] geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Schutzniveau zu gewährleisten. Dabei sind der Stand der Technik, der Umfang sowie der Zweck der Verarbeitung, die Implementierungskosten und die Eintrittswahrscheinlichkeit sowie die Schwere möglicher Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigten. Auch hier orientiert sich das Schutzniveau daran, was nach dem Grundsatz der Verhältnismäßigkeit im konkreten Fall von den Datenverarbeiter*innen gefordert werden kann und welche Risiken für die Betroffenen bestehen.[61]

Integrität lässt sich als „Unversehrtheit" definieren. „Unversehrtheit" bedeutet, dass keine Veränderung der Daten durch unbefugte Zugriffe erfolgt ist, d. h. keine Verfälschung, Ergänzung oder Beschränkung. Die Datensätze

58 Vgl. BT-Drs. 18/11325, 111; Kühling/Buchner-Schwichtenberg 2020, BDSG § 47 Rn. 2.
59 Baumgartner/Gausling, ZD 2017, S. 310.
60 Gola/Heckmann-Piltz 2022, Art. 32 Rn. 22.
61 Gola/Heckmann-Piltz 2022, Art. 32 Rn. 13.

müssen aber auch gegen Schadensereignisse geschützt werden.[62] Vom Integritätsschutz ist damit der Schutz vor Zugriffen Dritter, etwa durch Hacker*innen, aber auch die technisch reibungslose Gewährleistung des Regelbetriebs umfasst. So ist etwa eine Überlastung informationstechnischer Systeme oder eine fehlerhafte Datenverarbeitung zu vermeiden.[63]

Ein Datum ist nur vertraulich, wenn personenbezogene Daten nur einem befugten Empfängerkreis bekannt werden.[64] Auch aus Gründen der Vertraulichkeit ist also ein unbefugter Zugriff auf die Daten auszuschließen.[65] Maßnahmen zur Umsetzung der Vertraulichkeit sind beispielsweise eine Zutritts-, Zugriffs-, Zugangskontrolle oder die Verschlüsselung von Daten, Art. 32 Abs. 1a DS-GVO.[66]

Ein manipulativer Zugriff auf die Positionsdaten gestohlener Fahrräder erscheint zunächst eher unwahrscheinlich. Allerdings handelt es sich um Daten, die für ein strafrechtliches Verfahren relevant sein können. Eine Manipulation könnte damit beträchtliche Folgen haben. Etwa könnte es zu einem unberechtigten Strafverfahren kommen, was wiederum Zwangsmittel bis hin zu einer unberechtigten Festnehme fälschlich eines Diebstahls bezichtigter Personen führen könnte. Wenn ein umfassender Schutz vor Zugriffen von außen nicht gewährleistet ist, muss die Polizei die Integrität der Daten deswegen allein aufgrund ihrer rechtsstaatlichen Verpflichtung aus 20 Abs. 3 GG genau prüfen.

Bei der Trackingservice-Anbieter*in gespeicherte Bewegungsdaten sind hinsichtlich der personenbezogenen Informationen deutlich sensibler als die im *FindMyBike-System* verarbeitete Live-Position, so dass hier gesteigerte Pflichten zur Gewährleistung eines adäquaten Zugriffsschutzes bestehen.

Das *FindMyBike-System* ist gegen unbefugten Zugriff von außen durch die folgenden technisch-organisatorischen Vorkehrungen geschützt: Der Zugriff auf die Ortungsdaten erfolgt über einen URL. Es ist daher sicherzustellen, dass von außen nicht auf die URL zugegriffen werden kann. Dies wird durch die Beschränkung des IP-Bereichs erreicht, d. h. nur Rechner aus dem Netzwerk der Polizei Berlin können mittels der URL auf das *FindMyBike-System* zugreifen, für alle andern IP-Adressen ist der Zugriff nicht möglich. Weiterhin verhindert

62 Paal/Pauly-Frenzel 2021, DS-GVO Art. 5 Rn. 47; Schwartmann/Jaspers/Thüsing/Kugelmann-Ritter 2020, Art. 32 Rn. 43.

63 Paal/Pauly-Martini 2021, DS-GVO Art. 32 Rn. 35.

64 Auernhammer-Kramer/Meints 2020, Art. 32 Rn. 33; Schwartmann/Jaspers/Thüsing/Kugelmann-Ritter 2020, Art. 32 Rn. 45.

65 Schwartmann/Jaspers/Thüsing/Kugelmann-Ritter 2020, Art. 32 Rn. 36; vgl. BVerfGE 120, 274 (315).

66 Paal/Pauly-Martini, 2021 DS-GVO Art. 32 Rn. 35; Schwartmann/Jaspers/Thüsing/Kugelmann-Ritter 2020, Art. 32 Rn. 30 ff.

die Firewall einen Zugriff auf andere Ports als Port 443 (HTTPS, Hypertext Transfer Protocol Secure).

Auch sind die Daten auf dem risikobehafteten Übertragungsweg gegen unautorisierte Zugriffe und Veränderungen zu schützen. Dazu muss eine Verschlüsselung der Daten erfolgen,[67] wozu das kryptografische Verfahren in Betracht kommt.[68] Aus Art. 32 Abs. 1 DS-GVO könnte folgen, dass die BSI-Standards der Verschlüsselung zu Grunde gelegt werden können. In Art. 32 Abs. 1 a 2. Alt. DS-GVO wird unter anderem als Maßnahme die Verschlüsselung der Daten genannt. Anhaltspunkte für den Stand der Technik bieten die Technischen Richtlinien des Bundesamts für die Sicherheit in der Informationstechnik (BSI). Den vom BSI ausgearbeiteten IT-Schutzmaßnahmen kommt zwar keine unmittelbare rechtlich verbindliche Wirkung zu.[69] Die Richtlinien geben aber eine Orientierung zu den aktuellen Möglichkeiten der IT-Sicherheit und damit für den Stand der Technik.[70] Art. 32 Abs. 1 DSGVO enthält keine konkreten Angaben, wie die Verschlüsselung auszugestalten ist, sondern orientiert sich, wie bereits festgestellt, am Risikoprinzip. Daher ist es naheliegend, hier die BSI-Richtlinien als Stand der Technik zu Grunde zu legen, wie dies auch nach Rechtslage vor Inkrafttreten der DS-GVO der Fall war (§ 9 BDSG alt[71] und Anlagen).[72] Zudem ist es sinnvoll, die aktuellen Vorgaben an dynamische Regelungen anzupassen, die sich u. a. in den jeweils aktuellen technischen Anforderungen in den BSI-Richtlinien widerspiegeln.[73]

Die Umstände, unter denen die Daten übertragen werden, sowie die Art der Daten und die Wahrscheinlichkeit einer Rechtsgutsverletzung erfordern eine sichere Verschlüsselung. Auch wenn ein unbefugter Zugriff auf den Datenübertragungsprozess eher unwahrscheinlich ist, ist wiederum entscheidend, dass die Daten ein polizeiliches und ggf. gerichtliches Handeln nach sich ziehen. Daher sind hohe Verschlüsselungsstandards anzulegen, gleichgültig ob es sich um Bewegungsdaten oder einzelne Live-Positionsdaten handelt. Die Verschlüsselung der Datenübertragung richtet sich daher nach BSI TR-02102. Zur Verschlüsselung wird das Verschlüsselungsprotokoll „Transport Layer Security“ (TLS)

67 Paal/Pauly-Martini 2021, DS-GVO Art. 32 Rn. 36; Roßnagel 2003, 3.4 Rn. 77.
68 Heinson 2015, S. 149; Marnau, DuD 2016, S. 431.
69 Vgl. Kilian-Illies/Lochter/Stein 2018, Kryptografie Rn. 58.
70 Mitterer/Wiedemann/Zwissler, BB 2018, S. 7; Günther, VV 2018, S. 52; Paal/Pauly-Nolden 2021, BDSG § 64 Rn. 3; Kühling/Buchner-Schwichtenberg 2020, BDSG § 64 Rn. 3.
71 Wolff/Brink Stand-Paulus 2021, DS-GVO Art. 32 Rn. 3.
72 Baumgartner/Gausling, ZD 2017, S. 311.
73 Vgl. Baumgartner/Gausling, ZD 2017, S. 311; Grosskopf/Momsen, CCZ 2018, S. 105; Roßnagel/Nebel, NJW 2014, S. 887; Bartsch/Rieke, EnWZ 2017, S. 437; Roßnagel, MMR 2018, S. 34.

verwendet. Hierbei werden vom BSI grundsätzlich die Versionen TLS 1.2 und TLS 1.3 empfohlen.[74]

Für den Aufbau einer gesicherten Datenverbindung im TLS-Protokoll wird eine Cipher-Suite, eine standardisierte Sammlung der zu verwendenden kryptographischen Algorithmen für Schlüsseleinigung (und ggf. für die Authentisierung), für die Verschlüsselung der Daten sowie eine Hashfunktion für die Integritätssicherung der Datenpakete verwendet. Für das *FindMyBike-System* wurde eine Cipher-Suite mit Perfect Forward Secrecy (gewählt, mit der „eine Verbindung auch bei Kenntnis der Langzeit-Schlüssel der Kommunikationspartner nicht nachträglich entschlüsselt werden kann".[75] Alle in den Technischen Richtlinien TR-02102-2 aufgeführten Cipher-Suites[76] sind für den Aufbau von gesicherten Datenverbindungen geeignet.

Ferner können sogenannte Eingabekontrollen zum Schutz der Integrität beitragen. Durch diese werden Protokolldaten in IT-Systemen ausgewertet. Dadurch wird ermöglicht, nachträglich zu überprüfen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.[77]

Vergleichbare Standards sind auch bei der Datenübertragung durch die Trackingservice-Anbieter*in einzuhalten. Für die Übertragung an die Polizei ergibt sich die Anwendbarkeit der BSI-TR zudem aus § 64 Abs. 1 S. 2 BDSG. Aus dieser Norm folgt, dass der Gesetzgeber die BSI-TR als Standard zur Umsetzung von den datenschutzrechtlichen Vorgaben sieht, der zumindest zu berücksichtigen ist.

Überdies stellt sich die Frage, inwieweit Doppelt- oder Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung im *FindMyBike-System* zu gewährleisten sind. Grundsätzlich ist es eine wirksame Maßnahme zum Schutz der Integrität der Daten, regelmäßig Kopien der Datensätze zu erstellen und diese sicher zu speichern.[78] Dabei ist allerdings zu beachten, dass das Erstellen von Kopien im Konflikt zum Grundsatz der Datenminimierung steht.[79] Weitere Kopien an verschiedenen Orten erhöhen außerdem das Risiko, dass auf die Daten unbefugt zugegriffen wird. Daher sind die Kopien ebenfalls gesondert zu sichern, und die Anzahl der Kopien muss in einem angemessenen Verhältnis zu

74 Bundesamt für Sicherheit in der Informationstechnik 2021.
75 Bundesamt für Sicherheit in der Informationstechnik 2021, S. 8.
76 Bundesamt für Sicherheit in der Informationstechnik 2021, S. 8 ff.
77 Paal/Pauly-Martini 2021, DS-GVO Art. 32 Rn. 37.
78 Sydow/Marsch-Mantz 2022. Art. 32, Rn. 18 m. w. N.; Paal/Pauly-Martini 2021, Art. 32 Rn. 38a; vgl. Härting 2016, S. 38.
79 Paal/Pauli-Martini 2021, DS-GVO Art. 32 Rn. 38a.

der Bedeutung der Daten und den erfolgten Arbeitsschritten stehen. Es dürfen daher nicht mehr Kopien erstellt werden als unbedingt notwendig sind.

Wie dargelegt, ist das *FindMyBike-System* bewusst darauf angelegt, dass auf die Speicherung von Daten innerhalb des Systems verzichtet wird, um in erster Linie eine Softwareschnittstelle bereitzustellen, die von unterschiedlichen Anbieter*innen genutzt werden kann. Dies schließt nicht aus, dass bei der Trackingservice-Anbieter*in und bei der Polizei entsprechende Kopien angelegt werden und ist sogar insbesondere mit Blick auf die Beweisqualität der Daten empfehlenswert.

Neben diesen „datenbezogenen Maßnahmen" sind die Normadressaten dauerhaft und kontinuierlich verpflichtet,[80] den ungestörten Betrieb der Datenverarbeitungsanlage sicherzustellen. Dazu muss das System im Sinne des Art. 32 Abs. 1 b 5. Var. DS-GVO belastbar sein. Dazu ist z. B. eine unterbrechungsfreie Stromversorgung sicherzustellen, um einem Datenverlust vorbeugend entgegenzuwirken.[81] Die Datenverarbeitungssysteme müssen so belastbelastbar sein, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gewährleistet ist. Dazu muss das System auch vor Angriffen von außen, etwa durch die gezielte Überlastung von Servern mittels sog. DoS- oder DDoS-Attacken geschützt sein.[82] Dies müsste bei einer Umsetzung des *FindMyBike-Systems* in der Praxis beachtet werden. Hinsichtlich der Polizei und der Trackingservice-Anbieter*in bleibt festzuhalten, dass die betroffenen Systeme insgesamt wenigstens ein dem *FindMyBike-System* vergleichbares Schutzniveau aufweisen sollten, wobei gerade bei der Polizei ein deutlich höheres Schutzniveau zu erwarten wäre.

## 4. Rechtliche Einordnung der Datenverarbeitung beteiligten Akteure

An dem *FindMyBike-System* partizipieren unterschiedliche Akteure (Übersicht unter 2.), die zueinander in unterschiedlichen rechtlichen Verhältnissen stehen. Um die gegenseitigen Rechte und Pflichten sowie die rechtlichen Risiken zu klären, die für die einzelnen Akteure bestehen, wird der rechtliche Rahmen untersucht. Dabei ist zu beachten, dass die Rechtsverhältnisse wesentlich durch vertragliche Absprachen bestimmt werden. Empfehlungen für die vertragliche Ausgestaltung sollen an dieser Stelle nicht ausgesprochen werden (diese ori-

80 Paal/Pauly-Martini 2021, DS-GVO Art. 32 DS-GVO Rn. 40.

81 Auernhammer-Kramer/Meints 2020, DS-GVO Art. 32 Rn. 41 f.; Paal/Pauly Martini 2021, DS-GVO Art. 32 Rn. 38b.

82 Sydow/Marsch-Mantz 2022, Art. 32, Rn. 17; vgl. Gerlach 2015, S. 585.

entieren sich an den Leistungen im Einzelfall), sondern nur der rechtliche Rahmen, der aus der DS-GVO folgt.

Zu klären ist insbesondere die Frage, wer in einem solchen mehrstufigen Datenverarbeitungsprozess bei mehreren Beteiligten die Verantwortung für die Einhaltung von datenschutzrechtlichen Vorgaben trägt und für Fehlverhalten potenziell haftet. Verantwortliche sind natürliche oder juristische Personen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Sie sind neben den Auftragsverarbeiter*innen die zentralen Normadressaten der DS-GVO und für die Einhaltung der Datenschutzbestimmungen rechtlich verantwortlich, haften für Schäden und machen sich ggf. bußgeldpflichtig.[83] Mit der Verantwortlichkeit gehen zahlreiche Prüf-, Rechenschafts- und Dokumentationspflichten einher.[84] So sind die Verantwortlichen nach Art. 5 Abs. 2 DS-GVO für die Einhaltung der Datenschutzgrundsätze aus Art. 5 Abs. 1 DS-GVO verantwortlich. Auch müssen sie nach Art. 24 Abs. 1 DS-GVO nachweisen, dass die Datenverarbeitung DS-GVO-konform erfolgt. Zudem haben sie nach Art. 24 Abs. 2 DS-GVO für angemessene Datenschutzvorkehrungen zu sorgen.

Die DS-GVO sieht ausdrücklich vor, dass es mehrere Verantwortliche geben kann (Art. 4 Nr. 7). In diesem Rahmen können mehrere Personen gemeinsame Entscheidungen fällen. Aber es können auch Personen mit verschiedenen Verantwortungsbereichen arbeitsteilig zusammenwirken.[85] So werden vielfach Infrastrukturen von Anbieter*innen zur Verfügung gestellt, die dann wiederum von anderen Dienstleister*innen genutzt werden.[86] Auch wird der Prozess der Datenverarbeitung zunehmend nicht mehr von den Personen durchgeführt, die diesen veranlasst haben, sondern dieser wird an entsprechend spezialisierte Anbieter*innen ausgelagert. Erschwerend kommt teilweise hinzu, dass die Anbieter*innen von Infrastrukturen selbst Zugang auf die dabei verarbeiteten Daten haben, z. B. im Rahmen der Systemadministration. Auch Privatpersonen greifen auf Datenverarbeitungsangebote von externen Anbietern zurück. Insofern sind oft verschiedene Akteure an einem Datenverarbeitungsprozess beteiligt, die in unterschiedlichem Maße Einfluss auf die einzelnen Verarbeitungsschritte haben.

83 Auernhammer–Eßer 2020, Art. 4 Rn. 77; Schwartmann/Jaspers/Thüsing/Kugelmann- Schwartmann/Mühlenbeck 2020, DS-GVO Art. 4, Rn. 128 f.

84 Radtke 2021, S. 36.

85 Schwartmann/Jaspers/Thüsing/Kugelmann-Schwartmann/Mühlenbeck 2020, DS-GVO Art. 4, Rn. 139 f.

86 Berlit 2016, Anm. 3.

Maßgeblich für die Einstufung als Verantwortliche ist, dass die betreffenden Akteure über den Zweck und die Mittel der Verarbeitung mitentscheiden.[87] Für eine Verantwortlichkeit ist erforderlich, dass eine tatsächliche Einflussnahme auf das „Ob", „Warum" und das „Wie" der Datenverarbeitung erfolgt.[88] Dabei ist zu berücksichtigen, dass der Einfluss auf den Zweck und die Mittel unterschiedlich ausgeprägt sein kann;[89] gerade bei mehreren Beteiligten. Daher muss ein Grad an Einfluss auf Zweck und Mittel erreicht werden, der es rechtfertigt, die jeweiligen Beteiligten im konkreten Einzelfall als Verantwortliche einzustufen. Abhängig vom Kontext der Verarbeitung können die Zwecke oder die Mittel stärker im Vordergrund stehen.[90]

Auftragsverarbeiter*innen sind nach Art. 4 Nr. 8 DS-GVO natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten im Auftrag der Verantwortlichen verarbeiten. Die Auslagerung von Datenverarbeitungsprozessen an externe Anbieter kommt mittlerweile sehr oft vor. Den Rahmen hierfür definiert Art. 28 DS-GVO, der aufgrund der mit der Auslagerung verbundenen datenschutzrechtlichen Risiken die Zulässigkeit der Auftragsverarbeitung an strenge Voraussetzungen knüpft.[91] Maßgeblich sind vertragliche Vereinbarungen für das Verhältnis, Art. 28 Abs. 3 S. 1 DS-GVO, wobei in S. 3 zahlreiche Inhalte der Verträge geregelt sind, z. B. mit Blick auf die Datensicherheit c oder der Pflicht aus f, die Verantwortlichen bei gewissen Verpflichtungen zu unterstützen. Auch die Haftung auf Schadensersatz ist bei der Auftragsverarbeitung möglich, Art. 82 Abs. 1 DSGVO. Allerdings ist die Haftung in Art. 82 Abs. 2 S. 2 DS-GVO eingeschränkt und geht nicht so weit wie bei den Verantwortlichen.

Die Verantwortlichen haben indes mehr Verpflichtungen als die Auftragsverarbeiter*innen. Ihre Pflichten werden in Art. 24 DS-GVO konkretisiert. Sie haben im Rahmen eines risikobasierten Ansatzes dafür einzustehen, dass die Datenverarbeitung in zulässiger Art und Weise abläuft, wobei sie für die notwendigen technischen und organisatorischen Maßnahmen zu sorgen haben.[92] Sie tragen auch dann die Verantwortung für die Einhaltung der Vorgaben der

87 WP 169, S. 15; BVerwG Beschl. V. 25.2.2016 – 1 C 28.14 Rn. 28; Däubler/Wedde/Weichert/Sommer–Weichert 2020, DSGVO Art. 4 Rn. 87; Schwartmann/Jaspers/Thüsing/Kugelmann-Schwartmann/Mühlenbeck 2020, DS-GVO Art. 4, Rn. 153; Auernhammer-Eßer 2020, Art. 4 Rn. 79.

88 WP 169, S. 11; Gierschmann/Schlender/Stentzel/Veil- Kramer 20218, Art. 4, Rn. 2; Martini/Fritsche, NVwZ-Extra 2015, S. 5 m. w. N.

89 Vgl. BVerwG Beschl. V. 25.2.2016 – 1 C 28.14 Rn. 28.

90 WP 169, S. 16.

91 Wolff/Brink-Spoerr 2021, DS-GVO Art. 28 Rn. 1 ff.; Däubler/Wedde/Weichert/Sommer-Weichert 2020, Art. 4 Rn. 96.

92 Gola/Heckmann-Gola 2022, Art. 4 Rn. 63.

DS-GVO, wenn sie personenbezogene Daten durch Auftragsverarbeiter verarbeiten lassen.[93]

### *4.1 Tracking-Berechtigte*

Die Tracking-Berechtigten bestimmen über das „Ob" der Datenverarbeitung, da sie durch die Installation der Trackinghard und Software und den Abschluss eines Vertrages mit einem Trackingservice-Anbieter die wesentliche Ursache für die Verarbeitung setzen. Auch erfolgt das Tracken, damit sie mit Hilfe der Polizei ihr Fahrrad zurückerlangen können oder um in einem etwaigen zivilrechtlichen Prozess Herausgabe- oder Schadensersatzansprüche beweisen können („Warum").

Allerdings stellt sich die Frage, ob die Tracking-Berechtigten Einfluss auf das „Wie" der Datenverarbeitung haben. Die Kontrolle über die technischen Abläufe obliegt den Trackingservice-Anbieter*innen bzw. dem System-Betreiber*innen. Diese Abläufe werden die Tracking-Berechtigten im Regelfall nicht nachvollziehen können. Damit stellt sich die Frage, inwieweit sie – als die den Datenverarbeitungsprozess veranlassende Person – Kontrolle über die Vorgänge der konkreten Datenverarbeitungsprozesse haben müssen.

Gegen die Verantwortung der Tracking-Berechtigten könnte der begrenzte Einfluss auf die Datenverarbeitung sprechen, da diese den Prozess lediglich starten und beenden können,[94] ohne ausreichenden Einfluss auf die Verarbeitung zu haben, um eine Verantwortlichkeit zu begründen.[95] Eine bloße Mitursächlichkeit für das Aufkommen der personenbezogenen Daten würde dementsprechend nicht für eine Verantwortung ausreichen.[96] Eine solche Rechtsauslegung wäre jedoch mit Blick auf die Gewährung eines effektiven Datenschutzes problematisch. Der Begriff der Verantwortlichen ist zentral für die Anwendung der datenschutzrechtlichen Vorgaben, sodass im Regelfall kein Raum für eine einschränkende Auslegung besteht.[97] Andernfalls könnten sich Betroffene nicht ausreichend gegen Eingriffe zur Wehr setzen. Für einen effektiven Schutz der Rechte und Freiheiten der betroffenen Personen bedarf es – auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen von Aufsichtsbehörden – einer Zuteilung der Verantwortlichkeiten, einschließlich der Fälle, in denen Verantwortliche die Verarbeitungszwecke und -mittel gemeinsam mit anderen

93 Gierschmann/Schlender/Stentzel/Veil-Kramer 2018, Art. 4 Nr. 7 Rn. 2 m. w. N.
94 Vgl. Voigt/Alich, NJW 2011, S. 3543; Hoffmann/Schulz/Brackmann, ZD 2013, S. 123 f.
95 Vgl. BVerwG Beschl. V. 25.2.2016 – 1 C 28.14 - Rn. 28.
96 Martini/Fritsche, NVwZ-Extra 2015, S. 5; Voigt/Alich, NJW 2011, S. 3543; OVG Schleswig, ZD 2014, S. 644.
97 Karg, ZD 2014, S. 55 m. w. N.

Verantwortlichen festlegen oder ein Verarbeitungsvorgang im Auftrag von Verantwortlichen durchgeführt wird. Dies spricht dafür, die Verantwortlichkeit zunächst möglichst weit zu interpretieren, da andernfalls das Datenschutzniveau von vornherein reduziert würde.

Die Anforderungen an die Verantwortlichen sind hoch. Insbesondere müssen sie nach Art. 5 Abs. 2 DS-GVO die Einhaltung der DS-GVO Vorschriften nachweisen können. Dies können Privatpersonen - also Verbraucher/innen - kaum leisten, insbesondere wenn sie keinen Zugriff auf das IT-System haben. Wenn es aber möglich wäre, dass eine Verantwortung bereits dadurch ausgeschlossen wäre, dass die beauftragende Personen die Datenverarbeitungsprozesse nicht beeinflussen kann, dann könnte dies dazu führen, dass sich auch Unternehmen, Organisationen und sogar staatliche Stellen durch die Auswahl entsprechender Anbieter*innen einer datenschutzrechtlichen Verantwortung entziehen könnten.[98] Bewusste Unwissenheit könnte also dazu führen, dass keine Verantwortung besteht, während Personen, die sich trotz externer Anbieter um die Steuerung des Datenverarbeitungsprozesses bemühen, verantwortlich wären.[99] Dies erscheint widersprüchlich. Der Umstand, dass ein eingerichteter Service genutzt wird, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann die Nutzer*innen also nicht von ihren Verpflichtungen zum Schutz personenbezogener Daten befreien.[100]

Eine Verantwortlichkeit kann dementsprechend nur dann mit Sicherheit abgelehnt werden, wenn keinerlei rechtlicher oder tatsächlicher Einfluss auf die Verarbeitung besteht.[101] Die Tracking-Berechtigten können das Tracking starten und bestimmen, wann es beendet wird. Sie können entscheiden, dass die Daten an die Polizei übertragen werden und die Daten auch mehrfach speichern bzw. speichern lassen. Ohne sie würde der Trackingvorgang nicht stattfinden, und das Tracking erfolgt ausschließlich in ihrem Interesse. Somit rechtfertigen ihr Handlungsspielraum und die Steuerungsmöglichkeiten, sie als Verantwortliche zu behandeln. Die Möglichkeiten, auf das Tracking Einfluss zu nehmen, sind so groß, dass sie als Verantwortliche einzustufen sind.

Allerdings können die Pflichten der Tracking-Berechtigten bei einer gemeinsamen Verantwortlichkeit (etwa mit der Trackingservice-Anbieter*in) auch einschränkend interpretiert werden. Dies folgt aus dem risikobasierten

98 Karg, ZD 2014, S. 56.

99 Karg, ZD 2014, S. 56; Caspar, ZD 2015, S. 14; Martini/Fritsche, NVzW-Extra 2015, S. 4 f., die darin allerdings keinen Widerspruch sehen und allein an objektiven Kriterien anknüpfen wollen.

100 EuGH Urt. v. 5.6.2018 – C-210/16, BeckRS 2018, 10155.

101 WP 169, S. 15.

Ansatz.[102] Dieser Ansatz zieht sich durch die Vorschriften der DS-GVO[103] und drückt sich damit als zentrale Ausprägung des Verhältnismäßigkeitsprinzips in zahlreichen Vorschriften aus.[104] So spiegelt sich dieses Prinzip etwa in den Art. Art. 24 Abs. 1 S. 1, Abs. 2, Art. 25 Abs. 1, Art. 30 Abs. 5, Art. 32 Abs. 1, 2, 35 und 39 Abs. 2 i. V. m. 38 Abs. 2 DS-GVO wider, die die Pflichten der Verantwortlichen konkretisieren. Daraus folgt auch, dass die Pflichten bei privater Datenverarbeitung im Vergleich zu Datenverarbeitung im Rahmen geschäftlicher Tätigkeiten weniger weit reichen. So ist es denkbar, dass von Großkonzernen höhere Datenschutzstandards zu erwarten sind als von kleineren Unternehmen oder gar von Privatpersonen. Insbesondere muss dabei berücksichtigt werden, dass die einzuleitenden Schritte wirtschaftlich vertretbar sind, solange die Rechte der Betroffenen angemessen gewürdigt werden.[105] Insofern können abhängig vom konkreten Einzelfall einzelne Verantwortliche auch anders behandelt werden als andere, je nachdem, was sie leisten können. Dies folgt auch aus Art. 26 DS-GVO, der bei mehreren Verantwortlichen auch bewusst von verschiedenen Pflichten ausgeht. Das Bestehen einer gemeinsamen Verantwortlichkeit hat damit nicht zwangsläufig gleichwertige Pflichten zur Folge.[106]

Die Tracking-Berechtigten dürften in der Regel als Kunden nur sehr beschränkt prüfen können, ob datenschutzrechtliche Vorgaben bei dem Trackingservice-Anbieter*innen eingehalten werden. So kann etwa die Datensicherheit kaum überprüft werden, wenn die Hard- und Software ausschließlich beim Anbieter betreiben wird. Auch werden die Daten meist im Zugriffsbereich der Trackingservice-Anbieter*innen verbleiben, sodass die Bestohlenen nicht kontrollieren können, was mit den Daten passiert. Dieses Argument gilt umso mehr, wenn es sich bei den Tracking-Berechtigten um Verbraucher*innen handelt. Daher kann im Wesentlichen von den Tracking-Berechtigten nur zwingend erwartet werden,

- dass Sie Auftragsverarbeiter*innen auswählen, bei denen sie davon ausgehen können, dass diese die datenschutzrechtlichen Vorgaben einhalten; dies kann durch die Gestaltung von Musterverträgen und die Bestellung speziell versierter Datenschutzbeauftragter für die Trackingdienste-Anbieter*in erfol-

102 Ausführlich dazu Veil, ZD 2015, S. 347 ff.; Veil, ZD 2018, S. 13 ff.; Gola/Heckmann-Piltz 2022, Art. 24 Rn. 23.

103 Gola/Heckmann-Piltz 2022, Art. 24 Rn. 23; Schantz/Wolff 2017-Wolf, S. 149; Kühling/Buchner-Bergt 2020, Art. 39, Rn. 23; vgl. Veil, ZD 2015, S. 348.

104 Gola/Heckmann 2022-Piltz Art. 24 Rn. 23; Veil, ZD 2015, S. 350 ff.; vgl. Veil, ZD 2018, S. 15.

105 Sydow/Marsch-Raschauer 2022, Art. 24, Rn. 32.

106 EuGH EuZW 2018, 13/2018, 534 (537).

gen. Außerdem ist es nach Art. 28 Abs. 5 DS-GVO durch die Wahl einer nach Art. 42 DS-GVO zertifizierten Auftragsverarbeiter*innen (der Schutz der Betroffenen wird durch die Zertifizierung sichergestellt) möglich, die Erfüllung der Pflichten aus Art. 28 Abs. 1 – 4 DS-GVO als Verantwortliche nachweisen. In Art. 28 Abs. 5 DS-GVO drückt sich der Gedanke aus, dass die Vorteile der Auftragsverarbeitung nicht durch zu hohe Anforderungen an die Verantwortlichen faktisch unmöglich gemacht werden sollen. Damit soll ermöglicht werden, dass die Verantwortlichen einen Datenverarbeitungsprozess ausgliedern können, ohne dass sie im Einzelnen die Verarbeitung der Daten nachvollziehen oder kontrollieren können. Für private und nicht-kommerzielle Auftraggeber gilt dies in besonderem Maße. Zudem kann sich die Wahl einer zertifizierten Anbieter*in auch auf ein etwaiges Bußgeldverfahren auswirken, § 83 Abs. 2 j DS-GVO. Es ist daher damit zu rechnen,

- dass entsprechende Zertifikate in der Praxis eine hohe Bedeutung haben werden, wodurch allerdings ggf. Kosten entstehen, die in der Regel von den Auftraggeber*innen, hier also von den Tracking-Berechtigten zu tragen sein werden.
- dass sie im Falle einer erkennbar rechtswidrigen Datenverarbeitung die Verarbeitung stoppen und etwaiger rechtswidrig erhobenen Daten löschen und/oder die Löschung veranlassen, Art. 17 Abs. 1 d DS-GVO;
- dass sie gem. der Art. 13 DS-GVO ff. den Informations- und Auskunftsrechten nachkommen, sofern die Betroffenen von der Datenerhebung erfahren haben und die Betroffenen ihnen bekannt sind.[107] Daher sind sämtliche Vorgänge sowohl im *FindMyBike-System* als auch bei den Trackingservice-Anbieter*innen zu dokumentieren, Art. 30 DS-GVO.

### *4.2 Trackingservice-Anbieter*in*

Ob die Trackingservice-Anbieter*innen Verantwortliche im Sinne DS-GVO sind, hängt im Wesentlichen von der vertraglichen Ausgestaltung ab. Sofern die vertragliche Ausgestaltung nicht eindeutig ist, gibt es aber gewisse Indikatoren, die auf eine Verantwortlichkeit der Trackingservice-Anbieter*innen hinweisen. Diese Indikatoren müssen im Rahmen einer wertenden Gesamtbetrachtung aller Umstände beurteilt werden.

107 Da dies im Regelfall erst nach Abschluss der polizeilichen Ermittlungen der Fall sein wird oder wenn der Betroffene von Ermittlungen der Polizei erfährt, steht dies nicht im Konflikt zu den polizeilichen Ermittlungen. In diesen Fällen ist vielmehr damit zu rechnen, dass die Polizei das Fahrrad entweder beschlagnahmt hat oder den Betroffenen bereits als Beschuldigten eingestuft hat. Ggf. haben die Betroffenen im Rahmen eines Strafverfahrens ohnehin Akteneinsicht.

Als wesentliches Abgrenzungskriterium zwischen Auftragsverarbeiter*innen und Verantwortlichen dient die Weisungsbindung gem. Art. 28 Abs. 3 a und Art. 29 DS-GVO. Die Auftragsverarbeiter*innen werden demnach abhängig vom Verantwortlichen tätig. Die Auftragsverarbeitung setzt damit voraus, dass die Auftragsverarbeiter*innen auf Grundlage eines definierten Auftrags gem. Art. 28 DS-GVO in Bezug auf die Daten für die Verantwortlichen fremdbestimmt tätig werden.[108] Ob eine solche Abhängigkeit besteht, bemisst sich danach, wie groß der Entscheidungsspielraum der Auftragsverarbeiter*innen ist. Wenn ihre Rolle auch Entscheidungen enthält, die den Verantwortlichen vorbehalten sind, wie beispielsweise „Welche Daten werden verarbeitet?“, „Wie lange werden sie verarbeitet?“, „Wer hat Zugang zu ihnen?“,[109] kann eine Trackingservice-Anbieter*in auch selbst Verantwortlicher im Sinne von Art. 24 DS-GVO sein. Für eine entsprechende Einstufung kann beispielsweise sprechen, wenn sie die Daten auch für eigene Zwecke verarbeitet, beispielsweise um Rückschlüsse auf die Nutzung bestimmter Fahrradrouten oder die Auslastung von Leihrädern zu ziehen.[110] Für eine alleinige Verantwortung der Tracking-Berechtigten kann sprechen, wenn die Trackingservice-anbieter*innen nur einen engen Entscheidungsrahmen haben und die wesentlichen Entscheidungen vom Tracking-Berechtigten gefällt werden.

### *4.3 Betreiber*in des FindMyBike-Systems*

Auch für die Betreiber*in des *FindMyBike-Systems* stellt sich die Frage, ob sie als Auftragsverarbeiter*in oder als Verantwortliche einzustufen ist. In erster Linie werden durch das *FindMyBike-System* Daten von den Trackingservice-Anbieter*innen zur Polizei weitergeleitet, was dafür spräche, dass es sich um eine Auftragsverarbeitung handelt, da keine wesentlichen Entscheidungen getroffen werden. Das System agiert in erster Linie durch den Datentransport eher passiv, sodass eine Verantwortlichkeit fernliegend ist, wobei sich dies auch durch entsprechende vertragliche Absprachen ändern kann.

108 Paal/Pauly-Ernst 2021, DS-GVO Art. 4 Rn. 56.

109 WP 169, S. 17.

110 Vgl. EuGH Urteil v. 13.5.2014 – C-131/12 -, Rn. 28 ff.; WP 169, S. 18; wobei auch nur eine Verantwortlichkeit im Hinblick auf die für eigene Zwecke erhobenen Daten bestehen könnte, vgl. Martini/Fritsche NVwZ-Extra 2015, S. 8 f. Eine entsprechende Differenzierung erscheint aber wenig praxistauglich, da sich die Datensätze nicht immer klar trennen lassen.

### *4.4 Polizei*

Für die Einhaltung der Datenschutzvorgaben bei der polizeiinternen Verarbeitung der übermittelten Positionsdaten ist die Polizei zuständig. Dies folgt unmittelbar aus den Art. 4 Abs. 4 i. V. m. 3 Nr. 8 der JI-Richtlinie und dem Gebot der Gesetzmäßigkeit der Verwaltung aus Art. 20 Abs. 3 GG.[111]

## 5. Wesentliche Schlussfolgerungen

Es ist deutlich geworden, dass eine Softwareschnittstelle mit hohen Datenschutzstandards umgesetzt werden kann, nicht zuletzt durch interdisziplinäre Forschungsarbeit. Damit können gesteigerte datenschutzrechtliche Risiken durch die Übertragung von Positionsdaten gestohlener Gegenstände an die Polizei wirksam begrenzt werden. Die zunehmende Bedeutung der Grundsätze Privacy by Design und Default kann an diesem Beispiel verdeutlicht werden und es wird erkennbar, wie wenige Daten für eine Übertragung tatsächlich erforderlich sind.

Auch die Rechte, Pflichten und Risiken für die beteiligten Akteure erscheinen überschaubar. Die DS-GVO eröffnet auch in dieser spezifischen Konstellation einen Rahmen, der für Verantwortliche eine sachgerechte Aufteilung der Pflichten und Risiken mit Auftragsverarbeiter*innen oder anderen Verantwortlichen ermöglicht. Das Risiko, von Betroffenen in Anspruch genommen zu werden, erscheint gering und auf grob datenschutzrechtliche Mängel beschränkt. Auch wenn die Pflichten der Tracking-Anbieter*innen an und der Systembetreiber*in höher sind, können diese – wie dargelegt – durch eine entsprechende System- und Organisationsgestaltung wirksam und dauerhaft minimiert werden.

Eine Umsetzung in der Praxis steht aus einer datenschutzrechtlichen Perspektive nichts entgegen, wobei auch der Datenschutz bei der Polizei durch eine Verknüpfung mit dem *FindMyBike-Stystem* verbessert werden könnte.

## Literaturverzeichnis

Aden, H./Fährmann, J. (2020) Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung. Eine Untersuchung am Beispiel der polizeilichen Datenverarbeitungstechnologie, in: TATuP, 29 Jg., Nr 3, S. 24–28.

111 Johannes/Weinhold 2018, S. 68.

Aden, H./Fährmann, J./Bosch, A. (2020) Intransparente Polizeikontrollen – rechtliche Pflichten und technische Möglichkeiten für mehr Transparenz. In: Hunold, D./Ruch, A. (Hg.): Polizeiarbeit zwischen Praxishandeln und Rechtsordnung. Empirische Polizeiforschungen zur polizeipraktischen Ausgestaltung des Rechts. Wiesbaden: Springer VS, S. 3–22.

Albrecht, J. P./Jotzo, F. (2017) Das neue Datenschutzrecht der EU. Grundlagen, Gesetzgebungsverfahren, Synopse. Baden Baden: Nomos.

Barlag, C. (2017) Anwendungsbereich der Datenschutz-Grundverordnung. In: Roßnagel, A. (Hg.): Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts. Baden-Baden, S. 108–117.

Bartsch, A./Rieke, I. (2017) Das neue Datenschutzrecht mit Auswirkungen auch auf Energieversorger, in: EnWZ 06 Jg. Nr. 12, S. 435–441.

Baumgartner, U./Gausling, T. (2017) Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Was Unternehmen jetzt nach der DS-GVO beachten müssen, in: ZD 07 Jg., Nr. 07, S. 308–313.

Berlit, U.-D. (2016): Anmerkung zu BVerwG 1. Senat, Beschluss vom 25.02.2016 - 1 C 28/14, jurisPR-BVerwG (13), Anmerkung 3.

Borell, A./Schindler, S. (2019) Polizei und Datenschutz, Datenschutz und Datensicherheit,– in: DuD 43. Jg. Nr. 12, S. 767–773.

Bosch, A./Fährmann, J./Aden, H. (2021) Kontrollquittungen und -statistiken – Ein Instrument zur Durchsetzung des Diskriminierungsverbots bei Polizeikontrollen, in: ZKKW 7 Jg. Nr. 1, S. 186–218.

Bundesamt für Sicherheit in der Informationstechnik (2021) Technische Richtlinie TR-02102-2. Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2021-01. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=2 (letzter Aufruf: 21.02.2023).

Byers, P. (2017) Die Zulässigkeit heimlicher Mitarbeiterkontrollen nach dem neuen Datenschutzrecht, in: NZA 34. Jg., Nr. 17, S. 1086–1091.

Caspar, J. (2015) Nutzung des Web 2.0- zwischen Bürgernähe und Geschwätzigkeit? Einsatz von Web 2.0-Plattformen durch öffentliche Stellenam Beispiel der Polizei, in: ZD 5 Jg., Nr. 1, S. 12–17.

Däubler, W./Wedde, P./Weichert, T./Sommer, I. (2020) EU-Datenschutz-Grundverordnung und BDSG-neu. 2. Auflage. Frankfurt am Main.

Ehmann, E./Selmayr, M. (2018) Datenschutz-Grundverordnung. 2. Aufl. München: C.H.Beck.

Eßer, M./Kramer, P./von Lewinski, K. (2020) DSGVO BDSG. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze. 7. Aufl. Köln.

Fährmann, J. (2020) Digitale Beweismittel und Datenmengen im Strafprozess, in: MMR 23 Jg., Nr. 04, S. 228–233.

Fährmann, J. (2021) Mehr Transparenz durch technische Innovationen? Wie Technik polizeiliche Personenkontrollen effektiver und transparenter machen könnte, in: MMR 24 Jg., Nr. 10, S. 775–779.

Gerlach, C. (2015) Sicherheitsanforderungen für Telemediendienste - der neue § 13 Abs. 7 TMG, CR 31. Jg., Nr. 9, S. 581–589.

Gierschmann, S./Schlender, K./Stentzel, R./Veil, W. (2018) Kommentar Datenschtuz-Grundverodnung. Köln: Bundesanzeiger Verlag.

Gola, P./Heckmann, D. (2022): DS-GVO. Datenschutz-Grundverordnung VO (EU) 2016/679. 3. Aufl. München.

Gola, P./Schomerus, R. (2015) Bundesdatenschutzgesetz. 12. Aufl. München.

Grosskopf, L./Momsen, C. (2018) Outsourcing bei Berufsgeheimnisträgern – strafrechtliche Verpflichtung zur Compliance?, in: CCZ 11 Jg., Nr. 3), S. 98–108.

Günther, D.-C. (2018) Auf dem Stand der Technik, in: VV, S. 50–52.

Härting, N. (2016) Datenschutz-Grundverordnung. Köln: Otto Schmidt.

Heinson, D. (2015) IT-Forensik. Zur Erhebung und Verwertung von Beweisen aus informationstechnischen Systemen. Tübingen: Mohr Siebeck.

Hoffmann, C./Schulz, S./Brackmann, F. (2013) Die öffentliche Verwaltung in den sozialen Medien? Zulässigkeit behördlicher Facebook-Fanseiten, in: ZD 3 Jg., Nr. 3, S. 122–126.

Johannes, P. C. (2017) Unterschiede in der Datenschutz-Folgenabschätzung für Polizei und Strafverfolgungsbehörden nach europäischem und deutschem Recht, in: ZD-Aktuell 7 Jg., Nr. 19, S. 5852.

Johannes, P. C. (2019) Sicherheit der Datenverarbeitung nach § 64 BDSG im Vergleich zur JI-Richtlinie und DS-GVO, in: ZD-Aktuell, 09 Jg., Nr. 19, S. 6875.

Johannes, P. C./Weinhold, R. (2018) Das neue Datenschutzrecht bei Polizei und Justiz. Europäisches Datenschutzrecht und deutsche Datenschutzgesetze. Baden-Baden: Nomos.

Kapp, T./Schlump, A. (2008) Ist die Vernichtung von (kartellrechtlich relevanten) Unternehmensunterlagen zulässig?, in: BB Nr. 46, S. 2478–2486.

Karg, M. (2014) Anmerkung, in: ZD 4 Jg., Nr. 1, S. 54–56.

Keppeler, L. M./Berning, W. (2017) Technische und rechtliche Probleme bei der Umsetzung der DS-GVO-Löschpflichten. Anforderungen an Löschkonzepte und Datenbankstrukturen, in: ZD 7 Jg., Nr. 7, S. 314–319.

Kilian, W. (2018) Computerrechts-Handbuch. Computertechnologie in der Rechts- und Wirtschaftspraxis. 34. Aufl. München: Beck.

Koós, C./Englisch, B. (2014) Eine „neue" Auftragsverbeitung? Gegenüberstellung der aktuellen Rechtslage und der DS-GVO in der Fassung des LIBE-Entwurfs, in: ZD 4 Jg., Nr. 06, S. 276–285.

Kort, M. (2018) Neuer Beschäftigtendatenschutz und Industrie 4.0, in: RdA 71. Jg., Nr. 1, S. 24–33.

Kühling, J./Buchner, B. (2020) Datenschutz-Grundverordnung. BDSG Kommentar. 3. Aufl. München.

Kühling, J./Klar, M./Sackmann, F. (2021) Datenschutzrecht. 5. Aufl. Heidelberg.

Lachenmann, M. (2017) Neue Anforderungen an die Videoüberwachung. Kritische Betrachtungen der Neuregelungen zur Videoüberwachung in DS-GVO und BDSG-neu, in: ZD 4 Jg., Nr. 9, S. 407–411.

Marnau, N. (2016) Anonymisierung, Pseudonymisierung und Transparenz für Big Data. Technische Herausforderungen und Regelungen in der Datenschutz-Grundverordnung, in: DuD Nr. 7, S. 428–433.

Martini, M./Fritsche, S. (2015) Mitverantwortung in sozialen Netzwerken. Facebook-Fanpage-Betreiber in der datenschutzrechtlichen Grauzone, in: NVwZ-Extra, 34. Jg., Nr. 21, S. 1–16.

Mitterer, K./Wiedemann, M./Zwissler, T. (2018: BB-Gesetzgebungs- und Rechtsprechungsreport zu Industrie 4.0 und Digitalisierung 2017, in: BB 08.01.2018, Nr. 01-02, S. 3–15.

Paal, B./Pauly, D. (2021) Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. 3. Aufl. München: Beck.

Radtke, T. (2021): Gemeinsame Verantwortlichkeit unter der DSGVO. Unter besonderer Berücksichtigung von Internetsachverhalten. Baden-Baden: Nomos.

Roßnagel, A. (2003) Handbuch Datenschutzrecht. München: C. H. Beck.

Roßnagel, A. (2018) Das Vertrauensdienstegesetz. Neue Regelungen zur Anpassung des deutschen Rechts an die EU-eIDAS-VO, in: MMR 21. Jg., Nr. 1, S. 31–35.

Roßnagel, A./Nebel, M. (2014) Beweisführung mittels ersetzend gescannter Dokumente, in: NJW, S. 886–891.

Sander, G. M./Joecks, W./Miebach, K. (2017) Münchener Kommentar zum Strafgesetzbuch. Band 4, §§ 185-262. 3. Aufl. München: C.H.Beck.

Schantz, P./Wolff, H. A. (2017) Das neue Datenschutzrecht. Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis.

Schenk, S. von/Mueller-Stöfen, T. (2017) Die Datenschutz – Grundverordnung: Auswirkungen in der Praxis, in: GWR 9 Jg., Nr. 9, S. 171–179.

Schwartmann, R./Jaspers, A./Thüsing, G./Kugelmann, D. (2020) DS-GVO/BDSG. Datenschutz-Grundverordnung/Bundesdatenschutzgesetz. 2. Auflage. Heidelberg.

Sydow, G./Marsch, N. (2022) Europäische Datenschutzgrundverordnung. 3. Auflage. München.

Veil, W. (2015) DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip. Eine erste Bestandsaufnahme, in: ZD 05 Jg., Nr. 08 , S. 347–353.

Veil, W. (2018) Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, in: ZD 9 Jg., Nr. 1, S. 9–16.

Voigt, P./Alich, (2011) Facebook-Like-Button und Co. - Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber, in: NJW 64 Jg., Nr. 49, S. 3541–3544.

Wolff, H. A./Brink, (2022) BeckOK Datenschutzrecht. 41. Edition. München.