NORDEMANN

Nordemann Czychowski & Partner Rechtsanwältinnen und Rechtsanwälte mbB • Kurfürstendamm 178 • 10707 Berlin

VPK Landesverband Brandenburg e.V.
Frau Constanze Klunker
Geschwister-Scholl-Straße 83
14471 Potsdam

Ihr Zeichen / your. ref.

Unser Zeichen / our ref.

VPKP60001

Dr. Thomas W. Boddien

Kurfürstendamm 178
10707 Berlin

T +49 30 863 2398 86
F +49 30 863 2398 21

thomas.boddien@nordemann.de
www.nordemann.de

Datum / date

24. Oktober 2025

Beratung Mediennutzungsverträge mit Jugendlichen

Sehr geehrte Frau Klunker,

wir haben uns die von Ihnen zur Verfügung gestellten Informationen angesehen, die Rechtslage im Zusammenhang mit den aufgeworfenen Fragen geprüft und möchten wie folgt hierzu Stellung nehmen:

I.

Hintergrund und Fragestellungen

1. Der VPK Landesverband Brandenburg e. V. ist der Dachverband privater Träger der Kinder-, Jugend- und Sozialhilfe in Brandenburg. [redacted] (nachfolgend „Einrichtung"), eines der Verbandsmitglieder des VPK, ist an den Verband mit verschiedenen Fragestellungen im Zusammenhang mit der Benutzung von IT-Geräten (insbesondere Smartphones, Tablet PCs) durch die betreuten Kinder und Jugendlichen herangetreten.

   Die Einrichtung hält eine IT-Geräteregelung vor („IT-Geräteregelung bei den [redacted] om 22. Mai 2025), die es Kindern ab 12 Jahren erlaubt, Smartphones und Smartwatches zu benutzen:

   > Ziffer 3:
   > *„Jedes [redacted] Kind ab 12 Jahren und jede/r [redacted] Jugendliche ab 14 Jahren darf das eigene Handy und die eigene Smartwatch mit in die Schule nehmen, sofern die Schulordnung dies erlaubt."*

Die Benutzung ist hierbei von der Unterzeichnung eines „Mediennutzungsvertrages“ abhängig gemacht, was in einer IT-Geräteregelung der Einrichtung festgelegt ist:

> „Allgemeines“, erster Spiegelstrich:
> *Voraussetzung für die Nutzung eines IT-Geräts durch junge Menschen ist das Vorliegen eines individuellen Mediennutzungsvertrages, der die Grundrechte aus dieser Regelung nicht unterschreiten darf.*

Dieser Mediennutzungsvertrag wird über die Internetseite mediennutzungsvertrag.de erstellt, einem kostenlosen Online-Tool von klicksafe und Internet-ABC, mit dem Eltern und Kinder gemeinsam verbindliche Regeln für die Nutzung digitaler Medien festlegen können. Er sensibilisiert die Kinder und Jugendlichen insbesondere vor Gefahren im Umgang mit IT-Geräten und enthält verschiedene die Kinder bzw. Jugendlichen treffende Pflichten und Verbote, wie z. B. das Verbot, im Internet Namen, Anschriften und Telefonnummern bekannt zu geben, keine Fotos von anderen ohne Zustimmung zu verbreiten, die Pflicht, die Betreuer im Falle von Cyber-Mobbing einzubeziehen usw.

Ferner sieht die IT-Geräteregelung eine gemeinsame Kontrolle von Geräten in Verdachtsfällen sowie die Einziehung von Geräten und das Löschen verbotener Inhalte vor:

> Allgemeines, dritter Spiegelstrich:
> *„Bei Verdacht auf verbotene Inhalte (Gewalt / pornografische Inhalte / Mobbing / etc.) wird das IT-Gerät gemeinsam mit dem jungen Menschen kontrolliert. Bestätigt sich der Verdacht, wird das IT-Gerät beim Betreuenden abgegeben bzw. darf von diesem abgenommen werden. Die Rückgabe erfolgt nach pädagogischer Aufarbeitung und der Löschung verbotener Inhalte.“*

Schließlich ist zumindest die Möglichkeit der Installation und Nutzung von Jugendschutz-/Elternkontroll-Apps, sog. Parental Control Apps (PCA), wie z. B. Google Family Link, Microsoft Family Safety, Apple Bildschirmzeit usw. vorgesehen:

> Ziffer 9:
> *„Apps zur Beschränkung von Bildschirmzeiten und (Web-)Inhalten (z. B. Bildschirmzeit, Family Link, Family Safety, Switch Altersbeschränkungen) können ausschließlich als Hilfsmittel zur Umsetzung der im Mediennutzungsvertrag vereinbarten Regelungen eingesetzt werden. Für die Einstellungen der vorgenannten Beschränkungs-Apps (Elternfunktion) werden die WG-Handys genutzt. Die Installation der*

Elternfunktion auf privaten Endgeräten der Betreuenden wird zum Schutz derer Privatsphäre untersagt.“

2. Im Zusammenhang mit diesen Regelungen bittet der VPK um Beantwortung der folgenden Fragen:

   - Können Jugendeinrichtungen mit den Jugendlichen Mediennutzungsverträge schließen und dies zur Bedingung für die Nutzung von IT-Geräten machen?

   - Ist es zulässig, in den internen Regelungen vorzusehen, dass Jugendliche erst ab 12 Jahren nutzen dürfen?

   - Ist es zulässig, die Elternfunktion auf betrieblichen Gruppenhandys zu installieren?

   - Ist es zulässig, im Verdachtsfall IT-Geräte gemeinsam mit den Jugendlichen zu kontrollieren?

II.
Stellungnahme

Diesen soeben dargestellten Fragen soll nachfolgend nachgegangen werden.

1. Generelle Zulässigkeit von IT-Geräte-Regeln

Fraglich ist zunächst, ob IT-Geräte-Regeln, welche konkrete Vorgaben zu dem „Ob“ und dem „Wie“ der Nutzung von IT-Geräten beinhaltet, generell mit Entfaltung einer Wirksamkeit vorgehalten werden dürfen.

Private Träger der Kinder- und Jugendhilfe nehmen im Rahmen des Systems der öffentlichen Jugendhilfe eine eigenständige, aber in die staatliche Gesamtverantwortung eingebundene Rolle wahr; sie erfüllen Aufgaben nach dem Achten Buch Sozialgesetzbuch (SGB VIII) in freigemeinnütziger oder privater Trägerschaft und tragen durch pädagogische, beratende und unterstützende Leistungen zur Förderung, Erziehung und zum Schutz von Kindern und Jugendlichen bei.

Es dürfte wohl der einhelligen Ansicht entsprechen, dass der Medien- und Internetkonsum durch Kinder und Jugendliche Gefahren birgt, denen Sorgeberechtigte geeignet begegnen müssen; dies betrifft die zeitliche Begrenzung des Medienkonsums als auch die inhaltliche Kontrolle (vgl. z. B. OLG Frankfurt a. M., Beschluss vom 15. Juni 2018, Az. 2 UF 41/18). Das Gericht betonte auch, dass die Nutzung digitaler Medien zum Schutz von

Minderjährigen gegebenenfalls pädagogisch begleitet werden müsse, hier sich aber individuelle Spielräume ergeben, die - solange keine konkrete Kindeswohlgefährdung vorliegt - innerhalb der jeweiligen Familien eigenverantwortlich festgelegt werden können. Sorgeberechtigte bestimmen im Rahmen ihres Erziehungsauftrags gem. § 1626 BGB Abs. 1 BGB grundsätzlich über Fragen der Nutzung von Internet, Smartphone und sozialen Medien.

Fraglich ist, in welchem Umfang die Einrichtungen der Kinder- und Jugendhilfe im Rahmen ihrer Aufgaben eigenverantwortlich handeln dürfen. Den Trägern solcher Einrichtungen werden nicht automatisch die Rechte und Pflichten der elterlichen Sorge nach § 1626 BGB übertragen. Vielmehr sind die in der Einrichtung tätigen Personen gemäß § 1688 Abs. 1 und 2 BGB befugt, die Angelegenheiten des täglichen Lebens wahrzunehmen, soweit das Kind im Rahmen einer Hilfe nach §§ 34, 35 oder 35a Abs. 2 Nr. 3 und 4 SGB VIII untergebracht ist. Unter „Angelegenheiten des täglichen Lebens“ sind nach § 1687 Abs. 1 Satz 3 BGB solche zu verstehen, die häufig vorkommen und keine schwer abzuändernden Auswirkungen auf die Entwicklung des Kindes haben.

In diesem Zusammenhang wird in Veit/Fink in: BeckOK BGB, Hau/Poseck, 75. Edition, Stand: 01.08.2025, § 1687 Rn. 17.1 ausgeführt, dass die Überlassung eines internetfähigen Endgerätes wie Smartphone, Computer oder Tablet sowie die Entscheidung über das „Ob“ und das „Wie“ der Mediennutzung, einschließlich der Austausch über soziale Netzwerke tatsächlich nicht als Angelegenheiten des täglichen Lebens angesehen werden, insbesondere mit Blick auf die erheblichen Gefahren, die mit der Mediennutzung einhergehen. Andere Stimmen halten hingegen die Überlassung eines Smartphones wie auch die Nutzung des Internets angesichts der „heutigen Üblichkeit“ nicht (mehr) für eine besondere Angelegenheit, zumindest soweit es um eine normale, altersangemessene Nutzung geht. (s. Hennemann in: Münchener Kommentar zum BGB, 9. Auflage 2024, § 1687 Rn. 12), wohl aber jedenfalls dann, wenn dem Kind die Mediennutzung gänzlich untersagt werden soll (Rake, FamRZ 2017, 1733, 1734).

Allerdings hat die Einrichtung nicht nur einen Erziehungs- und Betreuungsauftrag, sondern auch eine Aufsichts- und Schutzpflicht. Diese umfasst selbstverständlich auch den Umgang mit digitalen Medien. Diese eben auch den Bereich der Mediennutzung umfassenden Aufgaben kann die Einrichtung unserer Ansicht kaum erfüllen, wenn sie die Nutzung der IT-Geräte gänzlich unreguliert gestattet. Ohne jegliche Regulierung würden die Kinder und Jugendlichen letztlich gänzlich einschränkungslos in die Welt der Medien gelassen und den hiermit einhergehenden Gefahren ausgesetzt.

Die IT-Regeln stellen unserer Ansicht nach insoweit keine individuellen Sorgerechtsentscheidungen dar, sondern sind Teil eines pädagogischen Konzepts zum Schutze des Wohles der Kinder und Jugendlichen, zur Abwehr von Gefahren und gleichzeitig auch zur Erziehung im Bereich des sozialen Umgangs. Sie verfolgen das Ziel, die Kinder/Jugendlichen zu schützen, ihre Entwicklung zu fördern und sie bei der eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeitsentwicklung zu unterstützen. Die Vorgabe allgemeiner Regeln zur Mediennutzung sind insoweit ein legitimer und wohl auch notwendiger Teil eines pädagogischen Konzepts und dient der Erfüllung des Auftrages der Einrichtung; es fördert zum einen die Medienkompetenz und dient dem Schutz vor übermäßiger und/oder sonst schädlicher oder gefährdender Nutzung.

Wir halten es daher für zulässig, als private Kinder- und Jugendhilfeeinrichtung Regeln für die Mediennutzung jedenfalls im Rahmen des zivilrechtlichen Hausrechts festzulegen. Das Hausrecht ist von dem Grundstückseigentum (§§ 903, 1004 BGB) und/oder dem Besitz (§§ 858ff. BGB) abgeleitet und gewährt dem Berechtigten nicht nur das Recht, den Zugang zum Eigentum/Besitz zu regeln, sondern es dient auch der Wahrung der äußeren Ordnung in dem Gebäude, auf die sich das Hausrecht erstreckt (vgl. z. B. BGH BeckRS 2006, 2450 Rn. 19).

Die Einrichtung kann in einer Hausordnung auch grundsätzliche Aspekte hinsichtlich des Umgangs mit den IT-Geräten regeln und auch klare Vorbote bezüglich bestimmter Inhalte aussprechen, wie beispielsweise das bewusste Aufrufen von rechtswidrigen, pornografischen oder gewaltverherrlichenden, sowie bezüglich bestimmter Benutzungen (wie beispielsweise Verbot des Mobbings, Stalkings usw.). Solange und soweit die Regeln der Aufrechterhaltung der Ordnung in der Einrichtung und insbesondere auch dem Schutz der Kinder/Jugendlichen dienen und im Übrigen angemessen, nachvollziehbar und verhältnismäßig sind, halten wir diese Vorgehensweise zulässig.

Allerdings handelt es sich bei der IT-Regelung nach unserem Verständnis um ein rein internes Dokument (Spezifizierung einer Dienstanweisung). Wir empfehlen daher, gespiegelte Regelungen in Form einer verbindlichen IT-Richtlinie als Teil einer Hausordnung auszuarbeiten, die den Beteiligten (den Sorgeberechtigten und den Kindern/Jugendlichen) zur Kenntnis geben werden. Hierbei sollte in Erwägung gezogen werden, die Regeln zu optimieren und zu konkretisieren.

Die Regeln sollten den Sorgeberechtigten vor bzw. bei dem Abschluss des Betreuungsvertrages zur Kenntnis gegeben und auch in den Betreuungsvertrag referenzierend eingebunden werden. Die Einverständniserklärung (FB 1.3b) enthält zwar in der dortigen Ziffer 8.3 eine Bestätigung der Kenntnis, dass bestimmte Gegenstände (einschließlich IT-Geräte) nur

nach Einverständnis der [redacted] in die Wohngruppe gebracht werden dürfen. Es bietet sich jedoch an, das Formular um einen expliziten Hinweis auf die IT-Regelung und ein Einverständnis mit ihnen zu ergänzen (und diese idealerweise auch auszuhändigen).

2. Zulässigkeit der einzelnen angesprochenen Regelungen

Nachdem wir das Aufstellen von IT-Nutzungsregeln in Form von oder Teil einer Hausordnung für zulässig erachten, möchten wir uns den spezielleren Fragenstellungen widmen:

a) Mindestalter 12 Jahre

Wir konnten keine Rechtsprechung recherchieren, aus der sich ein „Mindestalter" für die Nutzung von IT-Geräten, insbesondere Smartphones, entnehmen lässt oder ausgeführt wurde, ab welchem Alter Kindern ein „Recht auf IT-Nutzung" zuzusprechen wäre. Die Wahl des Mindestalters von 12 Jahren entspricht aber jedenfalls in etwa den Empfehlungen der Bundesinstituts für Öffentliche Gesundheit (BIÖG) :

> *„Erst wenn Sie sicher sind, dass Ihr Kind verantwortungsvoll mit dem Internet umgeht und am heimischen Computer ausreichend Erfahrung sammeln konnte, können Sie über die Anschaffung eines internetfähigen Smartphones nachdenken. Im Alter von ca. elf bis zwölf Jahren ist dies häufig der Fall."*

Die Altersgrenze von 12 Jahren für die Nutzung von IT-Geräten innerhalb der Einrichtung erscheint sinnvoll und erforderlich. Kinder unterhalb dieser Altersgrenze verfügen wohl in der Regel noch nicht über die kognitiven und sozialen Fähigkeiten, um digitale Inhalte verantwortungsbewusst zu nutzen und Risiken oder unangemessene Inhalte angemessen einzuschätzen. Zudem dient die Regelung dem Schutz vor Überforderung und fördert eine altersgerechte Entwicklung, in der direkte soziale Interaktionen und analoge Lernformen Vorrang haben. Ab einem Alter von 12 Jahren können Kinder im Rahmen pädagogischer Begleitung schrittweise an den verantwortungsvollen Umgang mit digitalen Medien herangeführt werden, was den Bildungs- und Schutzauftrag der Einrichtung in Einklang bringt.

Das Festlegen eines Mindestalters der Kinder/Jugendlichen für die Benutzung von IT-Geräten ist aus unserer Sicht im Lichte des oben Gesagten zulässig, sofern die Sorgeberechtigten von den IT-Regeln vor Unterzeichnung des Betreuungsvertrages Kenntnis genommen haben und sich mit ihnen einverstanden erklärt haben. Je nach Alter und Einsichtsfähigkeit sollten auch die Kinder/Jugendlichen Zugang zu den Regeln erhalten; jedenfalls volljährige Jugendliche sollten die Kenntnisnahme und auch ihr Einverständnis bestätigen.

b) Mediennutzungsvertrag als Voraussetzung für die Gerätenutzung

Der Mediennutzungsvertrag ist sicherlich ein gutes pädagogisches Instrument, um die Medienkompetenz, das Verantwortungsbewusstsein und Regelbewusstsein zu fördern. Durch die gemeinsame Erarbeitung und Unterzeichnung werden die Kinder aktiv in die Festlegung von Nutzungsregeln einbezogen und verstehen dadurch besser die Hintergründe und Konsequenzen ihres Handelns im digitalen Raum. Darüber hinaus unterstützt er die Einrichtung dabei, ihren Schutzauftrag umzusetzen, indem er eine Grundlage für die Aufklärung über Datenschutz, Urheberrechte und respektvolles Verhalten im Internet bietet.

Rechtlich betrachtet kommt selbst bei Unterzeichnung des Dokuments aber im Zweifel kein „echter“ zivilrechtlicher Vertrag mit den Kindern/Jugendlichen zustande, zumindest nicht mit den Minderjährigen. Kinder unter sieben Jahre sind geschäftsunfähig (§ 104 BGB) und können Verträge generell nicht wirksam abschließen; abgegebene Willenserklärungen sind nichtig. Minderjährige zwischen dem siebten und dem achtzehnten Lebensjahr (und hierunter fallen dann die Jugendlichen ab 12) sind beschränkt geschäftsfähig (§ 106 BGB), d. h. Willenserklärungen zum Abschluss von Verträgen bedürfen der (vorherigen) Einwilligung der gesetzlichen Vertreter oder einer (nachträglichen) Genehmigung, sofern das Kind hierdurch nicht lediglich einen rechtlichen Vorteil erlangt, was vorliegend hingegen nicht der Fall wäre.

Theoretisch wäre es denkbar, sich hinsichtlich des „Vertragsschlusses“ vorab eine Einwilligung der Sorgeberechtigten einzuholen, und (ebenfalls theoretisch) wäre es denkbar, das Dokument bzw. einzelne Regelungen juristisch auf ihre Zulässigkeit und Durchsetzbarkeit zu prüfen. Allerdings ist es von vornherein nicht Sinn und Zweck des Mediennutzungsvertrages, mit den Kindern/Jugendlichen einen echten zivilrechtlichen Vertrag zu schließen, der zivilrechtlich durchsetzbare Rechte und Pflichten begründet, sondern es ist ein pädagogisches Instrument zur Aufklärung, Sensibilisierung und Erziehung der Kinder und Jugendlichen hinsichtlich des Umgangs mit Medien, und zwar mit der vordergründigen Triebfeder ihres eigenen Schutzes und des Schutzes Dritter. Wir gehen davon aus, dass auch Sie hierin keinen (zu prüfenden) zivilrechtlichen Vertrag sehen; andernfalls lassen Sie uns das bitte wissen.

Entscheidend aber ist die Frage, ob die Benutzung von IT-Geräten von der Unterzeichnung des Medienvertrages abhängig gemacht werden kann, wie es die aktuellen IT-Regelungen vorsehen. Als Teil einer bekanntgemachten und akzeptierten „Hausordnung“ umgesetzt (siehe oben) halten wir die Implementierung der Pflicht zum Abschluss

des Mediennutzungsvertrages für zulässig. Er ist aus unserer Sicht ein geeigneter ein Baustein der auf dem Hausrecht basierenden „Spielregeln“ der Einrichtung, um den Pflichten der Einrichtung gegenüber den Kindern/Jugendlichen nachzukommen.

Hierbei ist eben auch zu berücksichtigen, dass der Vertrag keine echten „harten“, durchsetzbaren rechtlichen Pflichten beinhaltet und sie auch gar nicht beinhalten soll. Vielmehr dient er dazu, über einen Gesprächsfaden wichtige Themen der Mediennutzung gemeinsam mit den Kindern/Jugendlichen zu besprechen und ihnen hierbei – durch die Bezeichnung „Vertrag“ und die Unterzeichnung durch das Kind/Jugendlichen – der Wichtigkeit Nachdruck zu verleihen. Die Geeignetheit des Mediennutzungsvertrages hat übrigens schon einmal ein Gericht bestätigt. Insoweit verweisen wir auch auf den Beschluss des Amtsgerichts Bad Hersfeld vom 15. Mai 2017 (Az. F 120/17 EASO). Dort hatte das Amtsgericht einer Kindesmutter gem. § 1666 BGB sogar gerichtlich aufgegeben, einen schriftlichen Mediennutzungsvertrag mit ihrem Sohn abzuschließen. Es erachtete einen derartigen Vertrag für geeignet, jedenfalls bei „erheblichen Fehlverhalten“ und „aufkommender Medien-Suchtgefahr“.

c) Einsatz von Parental Control Apps

Fraglich ist, ob die in den IT-Regelungen enthaltene (interne) Erlaubnis, Parental Control Apps einzusetzen, zulässig ist.

(1) Parental Control Apps („PCA“) sind Softwareanwendungen, die es Eltern ermöglichen, die Gerätenutzung und die Online-Aktivitäten ihrer Kinder zu überwachen und zu steuern. Diese Apps umfassen in der Regel Funktionen zur Filterung und Blockierung unangemessener Inhalte (z. B. pornografische oder gewaltverherrlichende Webseiten), zur Festlegung von Bildschirmzeitlimits für bestimmte Anwendungen oder das gesamte Gerät sowie zur Überwachung der Kommunikationsaktivitäten (z. B. Textnachrichten oder Social-Media-Nutzung). Ferner beinhalten sie oft Standortverfolgungsfunktionen in Echtzeit mittels GPS oder anderen Ortungsdiensten, Benachrichtigungen über verdächtige oder potenziell gefährliche Online-Verhaltensweisen (wie Cyber-Mobbing oder unerlaubte Kontaktaufnahme) und die Möglichkeit, Installationen neuer Apps zu genehmigen oder zu blockieren.

Selbst bereits bei direkter Nutzung von PCAs *durch Sorgeberechtigten* ist ihre Zulässigkeit umstritten. Zwar bestimmen Sorgeberechtigte im Rahmen ihres Erziehungsauftrags gem. § 1626 BGB Abs. 1 grundsätzlich über Fragen der Nutzung von Internet, Smartphone und sozialen Medien, und zugleich obliegt ihnen eine Aufsichtspflicht (§ 1631 BGB), die ebenfalls den Umgang mit IT-

Geräten umfasst. Diese elterlichen Pflichten stehen jedoch in einem Spannungsverhältnis zu den Grundrechten der Kinder/Jugendlichen auf Privatsphäre und die informationelle Selbstbestimmung, die sich aus Art. 2 Abs. 1 des Grundgesetzes (GG) i.V.m. Art. 1 Abs. 1 GG einerseits sowie dem Datenschutzrecht andererseits ergeben.

Das in der Verfassung verankerte Recht auf Privatsphäre und der informationellen Selbstbestimmung gewährleistet das Recht des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, sowie das Recht zu wissen, wer was wann und bei welcher Gelegenheit über ihn weiß. Diese Rechte stehen auch Kindern und Jugendlichen zu, und in diese dürfen auch Sorgeberechtigte nicht in unangemessener Weise eingreifen (vgl. Förster in: BeckOK BGB, Hau/Poseck, 75. Edition, Stand: 01.08.2025, § 832 Rn. 33e). Eingriffe müssen stets sachgerecht, angemessen und verhältnismäßig sowie auf das notwendige Maß beschränkt sein. Insoweit sind die sich gegenüberstehenden Rechte und Pflichten – der Sorgeberechtigten einerseits und der Kinder/Jugendlichen andererseits – gegeneinander abzuwägen. Bei der Prüfung ist im Kontext der Pflichten der elterlichen Sorge auch § 1626 Abs. 2 BGB zu berücksichtigen, nach dem die Eltern bei der Ausübung der Sorge die wachsende Fähigkeit und das wachsende Bedürfnis des Kindes zu selbständigem verantwortungsbewusstem Handeln berücksichtigen müssen.

Insbesondere das anlasslose

- Mitlesen oder Einsehen der von Kommunikationen (z. B. Chatverlauf)
- Tracken von Telefonanrufen
- Einsehen des Surf-Verlaufes / Surfverhaltens
- Aktivitätsprotokolle
- Standort-Tracking

sind Maßnahmen, die sehr stark in die Privatsphäre eingreifen und auch sehr stark das allgemeine Persönlichkeitsrecht der Kinder und Jugendlichen tangieren, und selbst unter Berücksichtigung der mit der Mediennutzung einhergehenden Gefahren dürfte ein dauerhaftes und anlassloses „Überwachen“ in dieser Hinsicht nur schwer begründbar sein. Ein Eingriff in die Grundrechte darf nur erfolgen, wenn er erforderlich und geeignet ist, ein legitimes Schutzinteresse zu wahren – dies ist bei einer pauschalen, anlasslosen Überwachung regelmäßig wohl nicht der Fall. Aus diesem

Grunde werden derartige Maßnahmen sehr kritisch betrachtet und von der vermutlich überwiegenden Ansicht im Zweifel für unzulässig gehalten (vgl. hierzu Grisse NZFam 2022, 189, 196 mit weiteren Nachweisen sowie z. B. MüKoBGB/Huber, 9. Aufl. 2024, BGB § 1626 Rn. 69, dort sogar: Es könne geboten sein, statt inhaltlichen Kontrollen durchzuführen dem Kind gar kein Smartphone zu überlassen oder bestimmte Applikationen von dem Smartphone zu entfernen.).

Vorstehendes gilt insbesondere – wohl „erst recht“ – dann, wenn hinsichtlich des Alters der Kinder/Jugendlichen keine Differenzierung erfolgt, denn gem. § 1626 Abs. 2 BGB haben Eltern bei der Wahrnehmung ihrer erzieherischen Aufgaben die wachsende Fähigkeit und das wachsende Bedürfnis des Kindes zu selbständigem verantwortungsbewusstem Handeln zu berücksichtigen. So wäre es möglicherweise im Einzelfall eher vertretbar, das Surfverhalten eines zwölfjährigen Kindes zu überwachen als bei einem fünfzehnjährigen oder siebzehnjährigen Jugendlichen.

Unklar ist, inwieweit sich dies ändern kann, wenn die Kinder/Jugendlichen der „Überwachung“ zustimmen. Auf den Schutz der Privatsphäre und der informationellen Selbstbestimmung kann grundsätzlich auch verzichtet werden, d. h. die betroffene Person kann den Maßnahmen grundsätzlich zustimmen. Dies setzt aber eine hinreichende Einsichtsfähigkeit voraus, und diese muss im Einzelfall beurteilt werden. Dies bedeutet aber auch, dass allgemeine Regelungen, die unterschiedslos für alle Altersstufen gleichermaßen gelten, generell kaum umsetzbar sind, weil natürlich die Altersstufen und auch die Entwicklungsstufen sehr individuell ausfallen und etwaige Überwachungen individuell angepasst werden müssten

(2) Letztlich kann es aber dahingestellt bleiben, ob und in welchem Umfang die oben genannten Funktionen bei einer Installation von PCAs *durch die Sorgeberechtigten selbst* unter dem Gesichtspunkt des Eingriffes in das Recht auf Privatsphäre und das Recht der informationellen Selbstbestimmung eingreifen, denn neben diesen Rechten ist auch das Datenschutzrecht zu berücksichtigen. Im unmittelbaren familiären Umfeld kommt die Datenschutzgrundverordnung (DSGVO) nicht zum Tragen, denn gemäß Art. 2 Abs. 2 lit. c) DSGVO findet die DSGVO keine Anwendung bei einer Datenverarbeitung durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (sog. Haushaltsprivileg). Daher stellen sich datenschutzrechtliche Fragen bei dem Einsatz von PCAs durch das Sorgeberechtigen selbst nicht.

Die DSGVO gilt generell auch für freie Träger der Kinder- und Jugendhilfe (Kipker/Voskamp, Sozialdatenschutz in der Praxis, 1. Auflage 2021, Kap. 9 Rn 15). Für Träger der öffentlichen Jugendhilfe gelten darüber hinaus die speziellen datenschutzrechtlichen Regeln in den SGB I und SGB X (sog. bereichsspezifischer Datenschutz).

Bei privaten Trägern handelt es sich jedoch nicht um öffentliche Leistungsträger, so dass der bereichsspezifische Datenschutz grundsätzlich nicht, jedenfalls nicht unmittelbar, zur Anwendung gelangt (Kipker/Voskamp, Sozialdatenschutz in der Praxis, 1. Auflage 2021, Kap. 9 Rn 19). Allerdings bestimmt § 61 Abs 3 SGB VIII, dass bei Inanspruchnahme von Einrichtungen und Dienste von Trägern der bei freien Jugendhilfe sicherzustellen sei, dass der Schutz der personenbezogenen Daten bei ihrer Verarbeitung entsprechend der §§ 67-85a SGB X geschützt sind. Durch diese Vorschrift werden die Träger der freien Jugendhilfe zu „abgeleiteten Normadressaten“ des Sozialgesetzbuchs (Wiesner/Wapler, SGB VIII, Stand 1. Dez. 2021, vor § 61 Rn. 18, 19). Somit sind Sozialdaten von privaten Leistungsträgern jedenfalls in gleichermaßen zu schützen.

In jedem Falle aber gilt, wie gesagt, die DSGVO in jedem Falle ergänzend. Die Einrichtung jedoch wird sich – anders als die Sorgeberechtigten – auf die oben beschriebene Haushaltsprivileg nicht stützen können, denn sie gilt nur zugunsten natürlicher Personen (vgl. BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 53. Edition, Stand: 01.08.2023, Art. 2 Rn. 13), während die Einrichtung aber eine juristische Person ist. Selbst wenn man hier nicht an die Einrichtung, sondern an die einzelnen Betreuerinnen und Betreuer anknüpfen würde, käme man zu keinem anderen Ergebnis, denn jedenfalls wäre ihre Verarbeitung der beruflichen Tätigkeit zuzuordnen, was die Anwendung von Art. 2 Abs. 2 lit. c) DSGVO ausschließt (vgl. Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Art. 2 Rn. 19).

(3) Standortdaten, Chatverläufe, Surf-Verläufe usw. stellen unzweifelhaft personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO dar, die auch verarbeitet (Art. 4 Nr. 2 DSGVO) werden, und da sich die Einrichtung nicht auf Art. 2 Abs. 2 lit. c) DSGVO berufen kann, ist der Anwendungsbereich der DSGVO eröffnet.

Die Zulässigkeit der Verarbeitung personenbezogener Daten setzt eine rechtliche Grundlage voraus. Zu denken wäre hier zunächst an § 67a Abs. 1 SGB X. Gemäß § 67a Abs. 1 SGB X ist die Erhe-

bung von Sozialdaten zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist. Allerdings dürfte § 67a Abs. 1 SGB X aus den oben genannten Gründen nicht anwendbar sein. Zwar haben private Träger der Kinder- und Jugendhilfe ein hohes Maß an Datenschutz sicherzustellen; allerdings ist nicht davon auszugehen, dass sich ein privater Träger auf die gesetzliche Erlaubnisnorm, die öffentliche Stellen zu einer Datenverarbeitung ermächtigt, berufen kann.

Möglicherweise kann sich der private Träger auf § 62 Abs. 1 SGB VIII berufen. Dort heißt es, dass Sozialdaten „nur erhoben werden" dürfen, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe „erforderlich" ist. Fraglich ist hier, ob dies als echte Erlaubnisnorm, also als Rechtsgrundlage für die Verarbeitung von Daten, zu verstehen ist. Zweifel kommen wegen des Wortes „nur" in der Norm auf; jedenfalls der Wortlaut „darf… nur… erhoben werden") lässt darauf schließen, dass die Vorschrift den Umfang der Datenverarbeitung eher einengt, als eine Rechtsgrundlage darzustellen. Insoweit ist zu beachten, dass die Ermächtigungsnorm des § 67a Abs. 1 SGB X das Wort „nur" nicht beinhaltet („Die Erhebung von Sozialdaten durch die in § 35 des Ersten Buches genannten Stellen ist zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist."). Dennoch wird § 62 Abs. 1 SGB VIII wohl als Erlaubnisnorm aufgefasst, und zwar als *lex specialis* gegenüber § 67a Abs. 1 SGB X (Kipker/Voskamp, Sozialdatenschutz in der Praxis, 1. Auflage 2021, Kap. 9 Rn 29).

Letztlich kann dies unseres Erachtens aber dahingestellt bleiben. Denn „erforderlich" sind die Daten nur dann, wenn sie notwendig sind, um eine gesetzliche Aufgabe rechtmäßig, vollständig und in angemessener Zeit erfüllen zu können (Kipker/Voskamp, Sozialdatenschutz in der Praxis, 1. Auflage 2021, Kap. 9 Rn 32). Die Formulierung „erforderlich" darf – wie auch bei Art. 6 Abs. 1 S. 1 lit. b) und c) DSGVO – nicht mit „sinnvoll", hilfreich" o. ä. gleichgesetzt werden; „erforderlich" ist eng auszulegen und im Sinne von „notwendig" zu verstehen (Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019, Kap. 4 Rn. 66).

Die dauerhafte Überwachung der Kinder/Jugendlichen mithilfe von PCAs wird man jedoch nicht als „erforderlich" in diesem Sinne ansehen können. Sie ist zwar effektiv und ohne Weiteres geeignet, den erfolgten legitimen Zweck zu verfolgen; sie ist hingegen nicht notwendig, weil eine Medienerziehung und ein Schutz der Kinder/Jugendlichen auch anderweitig erfolgen kann. Jedenfalls kann

nicht ohne Weiteres davon ausgegangen werden, dass der Einsatz dieser Apps z. B. von einer Aufsichtsbehörde als „erforderlich“ für die Erfüllung der Aufgaben der Einrichtung angesehen würde, wodurch ein entsprechendes Risiko damit einherginge, sich auf die Vorschrift zu verlassen. Daher scheidet unseres Erachtens die Rechtsgrundlage des § 67a Abs. 1 SGB X eher aus bzw. dient sie jedenfalls nicht als sichere Rechtsgrundlage.

(4) In Betracht käme ferner die Rechtsgrundlage einer Einwilligung (Art. 6 Abs. 1 S. 1 lit. a) DSGVO), und zwar zunächst seitens der Kinder/Jugendlichen selbst. Bei Minderjährigen ist hinsichtlich der Wirksamkeit der Einwilligung auf die individuelle Einsichts-, Entschließungs- und Steuerungsfähigkeit. In der Tendenz (nur als Orientierung) gilt aber die oben schon beschriebene Systematik des BGB: Minderjährige zwischen dem siebten und dem achtzehnten Lebensjahr sind beschränkt geschäftsfähig (§ 106 BGB), und Einwilligungen bedürfen der vorherigen Einwilligung der gesetzlichen Vertreter oder einer (nachträglichen) Genehmigung (Artikel 8 DSGVO kommt hier nicht zur Anwendung, weil kein Dienst der Informationsgesellschaft betroffen ist). Ein guter Teil der betroffenen Kinder/Jugendliche über 12 Jahren dürften grundsätzlich über erforderliche Einsichtsfähigkeit verfügen (wenn auch sicherlich nicht alle).

Allerdings gelten im Datenschutzrecht Besonderheiten für die Einwilligung: Eine datenschutzrechtliche Einwilligung muss immer frei widerruflich und vor allem freiwillig sein. An Letzterem würde es hier jedenfalls dann fehlen, wenn die Installation von PCAs zur Voraussetzung für die Nutzung der IT-Geräte gemacht würde. Eine Einwilligung kann nur dann als Ausdruck individueller Selbstbestimmung begriffen werden, wenn sie auf einem freien Willensentschluss der betroffenen Person beruht; die betroffene Person muss eine echte Wahl haben, und die diesbezügliche Rechtsprechung ist streng. Druck und Nachteile bei einer Nichterteilung einer Einwilligung können ohne Weiteres genügen, um die Freiwilligkeit verneinen zu müssen, und auch ein „Machtungleichgewicht“ ist zu berücksichtigen. Vor diesem Hintergrund hätten wir durchgreifende Bedenken hinsichtlich der Freiwilligkeit der Einwilligung, falls dies zur Bedingung zur Nutzung der Geräte gemacht würde, denn: Stimmt das Kind/der Jugendliche nicht zu, dürfte er IT-Geräte gar nicht nutzen. Der Druck könnte auch von den Eltern ausgeübt werden.

Nun könnte man an eine Einwilligung durch die Sorgeberechtigten denken. Hier aber gäbe es zwei Aspekte, die zu berücksichtigen wären: Zum einen muss den Kindern/Jugendlichen mit steigendem

Alter ein eigenes Mitbestimmungsrecht eingeräumt werden, wenn es um die Verarbeitung ihrer personenbezogenen Daten fehlt; die Grundrechtsmündigkeit des Kindes verbietet zudem Einwilligungen der Eltern gegen seinen erklärten oder mutmaßlichen Willen (Gola/Heckmann, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz, 3. Auflage 2022, Art. 8 Rn. 18). Verweigert ein z. B vierzehnjähriger Jugendlicher die Zustimmung, die Sorgeberichtigen aber stimmen zu, wäre dies sehr problematisch.

Hinzukommt, dass auch bei den Eltern ggf. die Freiwilligkeit der Einwilligung fraglich sein kann. Eltern könnten sich unter Druck gesetzt fühlen, um den Betreuungsplatz nicht zu gefährden, wobei zusätzlich das Kopplungsverbot gem. Art. 7 Abs. 4 DSGVO zu berücksichtigen ist: Die DSGVO verbietet es grundsätzlich, die Erfüllung eines Vertrags von einer Einwilligung zur Datenverarbeitung abhängig zu machen, die für die Vertragserfüllung nicht zwingend erforderlich ist. Der Hauptzweck eines Betreuungsvertrags ist die pädagogische Betreuung und die Unterbringung der Kinder/Jugendlichen, während die Installation von PCA nicht zwingend notwendig und ist und nicht unter den Kernzweck des Vertrages fällt.

(5) Eine weitere alternative datenschutzrechtliche Rechtsgrundlage läge in Art. 6 Abs. 1 S. 1 lit. f) DSGVO („berechtigtes Interesse“). Danach ist eine Datenverarbeitung zulässig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Nach der Rechtsprechung des EuGH sind die Voraussetzungen für die Annahme eines berechtigten Interesses in diesem Sinne eng auszulegen. Da wie oben ausgeführt die Maßnahmen durchaus recht erheblich potentiell in die Interessen, Grundrechte und Grundfreiheiten der Kinder/Jugendlichen eingreifen, können wir Ihnen nicht empfehlen, sich auf diese Rechtsgrundlage zu verlassen. Es bestünde das Risiko, dass eine Datenschutzbehörde die Maßnahmen als zu stark in die Rechte der Kinder/Jugendlichen eingreifend ansieht, was zur Folge hätte, dass die Datenverarbeitung rechtswidrig wäre.

Allgemein gilt auch: Wenn derartige Überwachungsmaßnahmen schon bei Installation von PCAs durch Eltern umstritten und potentiell unzulässig sind, dürfte das erst recht im Falle der Installation durch eine Einrichtung gelten, weshalb wir nicht guten Gewissens zu der Umsetzung raten können, weil sie zu rechtsunsicher wäre.

Zu denken wäre daran, nur bestimmte, weniger eingreifende Funktionen der PCAs zu aktivieren. Das Aktivieren z. B. von Inhaltsfiltern oder Bildschirmzeiten würde sehr deutlich weniger in die Rechte der Betroffenen eingreifen, weil kein Zugriff auf Inhalte, Verläufe usw. genommen würde. Hier sähen wir allerdings das Problem, dass bereits die Installation der PCAs als solche potentiell die Gefahr mit sich bringt, dass die einschneidenderen Funktionen (wie das Tracking) unproblematisch jederzeit aktiviert werden könnten – und dies im Zweifel, ohne dass die Kinder/Jugendlichen dies bemerken. Eine Datenverarbeitung im datenschutzrechtlichen Sinne liegt bereits dann vor, wenn eine Zugriffsmöglichkeit zu den Daten geschaffen wird.

Wir hielten diesen Mittelweg (nur Konfiguration der Inhaltsfilter und Regelung der Handyzeiten) nicht für von vornherein eindeutig unzulässig; jedoch gingen hiermit rechtliche Unsicherheiten einher. Möglicherweise könnten Sie aber einmal recherchieren, ob am Markt Apps existieren, die ausschließlich Inhaltsfilter und die Konfiguration von Bildschirmzeiten ermöglichen.

Eine denkbare Alternative läge im Übrigen vielleicht auch darin, im Hause über die WLAN-Router Inhaltsfilter zu installieren / zu konfigurieren. Nachteil hierbei wäre allerdings, dass diese durch die Einwahl über das Handy-Netz umgangen werden könnten.

d) Gemeinsames Überprüfen von Geräten in Verdachtsfällen

Schließlich stellt sich die Frage, ob die gemeinsame Einsichtnahme in das Gerät bei Verdachtsfällen zulässig ist.

Mit der Einsichtnahme in das Gerät greifen die Betreuer/innen der Einrichtung sehr intensiv in die Privatsphäre der Kinder/Jugendlichen ein. Zusätzlich findet mit der Einsichtnahme eine (datenschutzrechtliche) Datenverarbeitung statt. Hier gilt das oben in Bezug auf die PCAs Gesagte entsprechend.

Anders als im Rahmen der PCAs erfolgt die Einsichtnahme hier allerdings nicht anlasslos, sondern gerade aufgrund eines Verdachts „verbotener Inhalte“, wie es in der IT-Regelung heißt. Hier sind wir der Ansicht, dass jedenfalls dann, wenn das Kind/der Jugendliche hinreichend einsichtsfähig ist und in die Einsichtnahme einwilligt, ein Eingriff im Einzelfall gerechtfertigt werden *kann*, und zwar auf der Grundlage § 8a Abs. 4 SGB VIII in Verbindung mit § 62 Abs. 1 SGB VIII, ergänzend gem. § 6 Abs. 1 S. 1 lit. c) DSGVO (Verarbeitung zur Erfüllung gesetzlicher Pflichten) in Verbindung mit den sich aus dem SGB VIII ergebenen Schutzpflichten.

Die Einrichtung hat einen Schutzauftrag. Gemäß § 8a Abs. 4 SGB VIII schließen die Träger der öffentlichen Jugendhilfe mit den Trägern von Einrichtungen und Diensten, die in ihrem örtlichen Zuständigkeitsbereich Leistungen nach dem SGB VIII erbringen, Vereinbarungen zur Wahrnehmung des Schutzauftrages. § 8a Abs. 4 Nr. 1 SGB VIII ist zu entnehmen, dass Fachkräfte einer Einrichtung bei Bekanntwerden gewichtiger Anhaltspunkte für die Gefährdung eines von ihnen betreuten Kindes oder Jugendlichen eine Gefährdungseinschätzung vornehmen haben; bei einer Gefährdungseinschätzung ist eine insoweit erfahrene Fachkraft beratend einzubeziehen (Nr. 2), ebenso wie die Erziehungsberechtigten und das Kind (Nr. 3).

Insoweit *kann* aus unserer Sicht im Einzelfall die gemeinsame Einsichtnahme in die IT-Geräte erforderlich sein, um die Gefährdung des Kindes/Jugendlichen einzuschätzen und auch Gefahren abzuwehren. Allerdings darf die Einsicht nicht generell ohne vorherige Abwägung der Interessen erfolgen; die Maßnahme (= Eingriff in die Rechte des Kindes/Jugendlichen) muss angemessen sein und muss auf Fälle reduziert werden, in denen konkrete und schwerwiegende Anhaltspunkte für eine erhebliche Kindeswohlgefährdung bestehen. Eine private Einrichtung der Kinder- und Jugendpflege ist keine Ermittlungsbehörde; die Aufgaben sind auf das Wohl und den Schutz des Kindes/Jugendlichen gerichtet, und jegliche Eingriffe in die Rechte eines Kindes/Jugendlichen dürfen ausschließlich erfolgen, um Gefahren *dieses Kindes/Jugendlichen* abzuwehren. Ausgeschlossen wäre z. B. die Einsicht in das Gerät des Kindes A aufgrund von Anhaltspunkten, dass A das Wohl des Kindes B gefährdet.

Die Einsichtnahme zielgerichtet, einzelfallbezogen und transparent erfolgt und darf sich ausschließlich auf solche Daten erstrecken, die unmittelbar zur Beurteilung der Gefährdungslage erforderlich sind, etwa Kommunikationsverläufe mit mutmaßlichen Tätern, Hinweise auf sexuelle Ausbeutung oder Cybermobbing. Eine umfassende Durchsicht oder Auswertung des gesamten Geräts, insbesondere privater Chats, Fotos oder Social-Media-Inhalte ohne Bezug zur Gefährdung, wäre unverhältnismäßig und damit unzulässig. Jedenfalls unzulässig wären beispielsweise Einsichtnahmen für

- das Entdecken oder Aufklären von eigenen rechtswidrigen Handlungen des Kindes, etwa das illegale Herunterladen von Filmen oder Musik,
- die Prüfung von Chatverläufen über den Konsum von Cannabis oder Alkohol, sofern keine konkrete Selbstgefährdung vorliegt,

- die Auswertung von politischen oder weltanschaulichen Äußerungen, selbst wenn diese bedenklich erscheinen,

um nur einige Beispiele zur Verdeutlichung zu nennen.

Die Einsichtnahme sollte nur mit (schriftlicher) Zustimmung und im Beisein des Kindes/des Jugendlichen und zusätzlich (insbesondere bei Kindern unter 16 Jahren) zur weiteren Absicherung mit Zustimmung – und idealerweise im Beisein – der Sorgeberechtigten erfolgen. Die Sorgeberechtigten sollten dem allgemein in dem Zustimmungsformular (im Sinne einer Transparenz) sowie zusätzlich in jedem Einzelfall zustimmen. Hierbei ist darauf hinzuweisen, dass gem. § 67b Abs. 2 S. 1 SGB X Einwilligungen schriftlich oder elektronisch erfolgen sollen, um deren Erteilung nachweisen zu können.

Diese Vorgehensweise halten wir für deshalb für sehr empfehlenswert, weil eine Einsichtnahme in die Geräte gegen den Willen der Jugendlichen unter Umständen sogar strafrechtlich relevant sein könnte, und zwar gleich unter mehreren Gesichtspunkten, insbes. § 201a StGB (Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen), § 203 StGB (Verletzung von Privatgeheimnissen), § 202a StGB (Ausspähen von Daten). Auch darf gegenüber dem Kind/Jugendlichen kein Zwang ausgeübt werden. Nur wenn eine akute Gefahr für Leib, Leben oder Freiheiten des Kindes/Dritter besteht und sie durch die Einsichtnahme potenziell abgewehrt werden kann, kann die Einsichtnahme im Einzelfall auch von einem rechtfertigenden Notstand gerechtfertigt sein.

Angesichts der Intensität des Eingriffes empfehlen wir, vor derartigen Einsichtnahmen standardmäßig zunächst Rücksprache mit der Einrichtungsleitung und einer insoweit erfahrenen Fachkraft zu halten und die Abwägungen unbedingt schriftlich zu dokumentieren. Im Zweifel sollte notfalls das Jugendamt involviert werden.

Die Ausführungen in den IT-Regelungen – bzw. in der „Hausordnung – sollten zu der Einsichtnahme sollten konkretisiert werden. Diese halten wir in der jetzigen Fassung für zu allgemein, zumal der Verdacht auf „verbotene Inhalte“ zu weitgehend ist. Beispielsweise ist der Verdacht, dass das Kind/der Jugendliche urheberrechtsverletzendes Material (wie z. B. illegale Filme) heruntergeladen hat, unserer Ansicht nach nicht ausreichend, um einen derartigen Eingriff in seine Rechte nicht rechtfertigen, weil diese Handlung zwar verboten sein mag, nicht aber das Kindeswohl gefährdet und daher Gegenstand der Beurteilung der Gefährdungslage sein kann.

Die Eingriffe müssen, wie erwähnt, auf solche Situationen beschränkt werden, in denen konkrete Anhaltspunkte dafür vorliegen, dass das Kindeswohl schwerwiegend gefährdet ist. Es sollte aus den Regelungen klar hervorgehen, in welche Fällen unter welchen Voraussetzungen eine Einsichtnahme erfolgen kann.

Bei älteren Jugendlichen (in der Regel ab 16 Jahren) ist die Problematik abgeschwächt, soweit die zu erwartende Einsichtsfähigkeit auch tatsächlich vorhanden ist, denn in diesem Alter ist (bei entsprechender Einsichtsfähigkeit und Reife) davon auszugehen, dass der Jugendliche wirksam in die gemeinsame Einsicht einwilligen kann – sowohl unter persönlichkeitsrechtlichen Aspekten als auch unter datenschutzrechtlichen. Dies aber ist immer im Einzelfall zu prüfen. Wichtig aber ist auch hier, dass die Einwilligung wirklich freiwillig und ohne Ausübung von Druck und auch schriftlich (oder elektronisch) erfolgt.

Die vorübergehende Einziehung des Gerätes zu erzieherischen/pädagogischen Zwecken halten wir im Übrigen für zulässig, soweit die Grundsätze der Angemessenheit gewahrt werden.

Wir empfehlen, die Umsetzung etwaiger Maßnahmen in diesem Kontext mit dem Datenschutzbeauftragten der Einrichtung abzusprechen. Ferner muss vor Umsetzung dahingehender Regelungen eine sog. Datenschutzfolgenabschätzung durchgeführt und dokumentiert werden (§ 35 DSGVO).

Noch ein ergänzender Hinweis: Äußerste Zurückhaltung ist geboten bei der eigenmächtigen Anfertigung von „Beweismitteln“; dies sollte unterlassen werden, insbesondere in den Bereichen Kinderpornografie, Gewaltdarstellungen, volksverhetzenden/extremistischen Inhalten und Anleitungen zu Straftaten, weil sich die Mitarbeiter/innen hierdurch selbst strafbar machen könnten.

Wir hoffen, dass wir Ihre Fragen hierdurch beantwortet haben und stehen für Rücksprachen gerne zur Verfügung. Der guten Ordnung halber weisen wir noch darauf hin, dass wir nicht die gesamten IT-Regelungen geprüft, sondern uns auf die Fragestellungen konzentriert haben.

Mit freundlichen Grüßen

NORDEMANN

Dr. Thomas Boddien
Rechtsanwalt