FORUM VERLAG HERKERT GMBH ISSN 2365-0990 Mai 2017

# Der Bauleiter

## Recht, Technik und Management in der Bauleitung

## Sichtbeton

**Realisierung anspruchsvoller sichtbarer Betonoberflächen**

### Smartphone, Tablet & Co.

**Datenschutz im Bauleiter-Alltag**

### Abfallmanagement

**Rechtssicherer Umgang mit Bauabfällen**

### Schwellenlos

**Barrierefreie Eingangs- und Terrassentüren**

## April, April, der macht, was er will

Diese bekannte Bauernregel war im April 2017 wirklich Programm. An manchen Tagen wechselten sich strahlender Sonnenschein, Bewölkung, Regen und Schnee beinahe stündlich ab. Der Wintereinbruch Mitte des Monats war gerade für die Autofahrer, welche sich an die Faustregel „Winterreifen von O wie Oktober bis O wie Ostern“ gehalten haben, eine unerfreuliche Überraschung. Der Nachfrost war vor allem für die Landwirte in den Wein- und Obstanbaugebieten ein Problem. Die Medien berichteten ausführlich über die Anstrengungen zum Schutz der jungen Triebe. Das April-Wetter setzte allerdings auch Baufirmen zu. Die Schlechtwetterzeit für das Saison-Kurzarbeitergeld endete wieder am 31. März, doch an dieses Datum hat sich das Wetter nicht gehalten.

Die klimatischen Bedingungen sind auch beim Sichtbeton ein großes Thema. Im Beitrag ab S. 12 können Sie nachlesen, mit welchen Maßnahmen Sie das gewünschte Erscheinungsbild des Sichtbetons erreichen können.

Eine spannende Lektüre wünscht Ihnen

Stefanie Ritter, Redaktion „**Der Bauleiter**“

## Inhalt



## Autoren dieser Ausgabe

**Prof. Dr. rer. nat. Frank Bär, Dipl.-Geologe**

Sachverständiger und Geschäftsführer der BAeR-Agentur für Bodenaushub GmbH; Referent für Boden- und Abfallmanagement

**www.bodenbaer.de**

**Uwe Gutjahr, Dipl.-Ing. FH, Architekt**

Büroleitung der Architekturbüros GUTJAHR**ARCHITEKT**; Sachverständiger für Barrierefreiheit, Energieberater DIN 180599

**www.gutjahr-architekt.de**

**Patrick Knittel**

Direktor der Knittel Akademie für Datenschutz & Compliance; Datenschutzbeauftragter (extern); Lehrbeauftragter HTW Berlin (Recht); Lehrgangsleiter „Compliance Officer (TAW)“ mit Zertifikatsprüfung

**www.knittel-compliance.de**

**Dr. Michael Siegwart**

Beratender Ingenieur, Sachverständiger für Schäden an Gebäuden und Bauwerksinstandsetzung, zuvor Projektleiter bei internationalen Hoch- und Tiefbauprojekten

**www.ibsiegwart.de**

# „Darf ich mein eigenes Smartphone benutzen?“ – Datenschutz im Bauleiter-Alltag *Von P. Knittel*

**Die Verwendung von mobilen Endgeräten wie Smartphone oder Tablet, ist kaum noch aus dem Alltag eines Bauleiters wegzudenken. Doch bei der Nutzung sollte man sich auch Gedanken über Datenschutz und Datensicherheit machen. Ein Überblick und praktische Tipps zur gesetzeskonformen Anwendung.** ■

Es gehört für viele Bauleiter zum Tagesgeschäft, auf der Baustelle schnell zum Smartphone zu greifen, um ein Foto vom Objekt zu machen, noch fehlende Arbeiter anzurufen, korrigierte Anweisungen per E-Mail oder gar per WhatsApp zu verschicken usw. Mobile Endgeräte sind für viele Berufstätige unerlässlich geworden, weil sie eine ständige Erreichbarkeit und schnelle Reaktionen garantieren. Zudem können Fotos, Videos, Daten, Aufzeichnungen aller Art sofort angenommen, verarbeitet und innerhalb weniger Minuten wieder unkompliziert an die nächste Adresse weitergeleitet werden. Dass es hierbei zu erheblichen Verstößen gegen Datenschutz und Datensicherheit kommen kann, ist meistens nicht bekannt bzw. wird nicht als relevant eingestuft.

## Datenschutz bei Videokameras auf dem Bau

Beim Aufstellen von Videokameras sind viele bereits dafür sensibilisiert worden, dass der Datenschutz beachtet werden muss. Die Aufnahmen dienen der Dokumentation des Baufortschritts oder der Abschreckung vor Diebstählen oder Vandalismus. Als Facette des Persönlichkeitsrechts wird bei der Kamera das **Recht am Bild jedes Einzelnen** geschützt, sodass genau entschieden werden muss, ob und wann und in welchem Umfang die Baustelle überwacht werden soll.

Der wichtigste Grund für eine Überwachung ist die Verhinderung oder Aufklärung von Straftaten, vor allem Diebstählen und Vandalismus, manchmal auch zur Zutrittskontrolle für Unberechtigte von einem Baubüro aus. An diesem Zweck muss sich die Überwachung am öffentlich zugänglichen Bereich orientieren, so dass die Kamera also z. B. nicht den Straßenbereich oder gar gegenüberliegende Wohnungen erfassen darf. Im Hinblick auf die Aufzeichnungsdauer und die aufgezeichneten Bereiche muss sie geeignet sein, den o. g. festgelegten Zweck einzuhalten.

Sogenannte optisch-elektronische Einrichtungen wie die Videoüberwachung sind im Baubereich nach Maßgabe des § 6b Bundesdatenschutzgesetz (BDSG) nur zulässig, soweit sie

- zur **Wahrnehmung des Hausrechts** (Nr. 2) oder
- zur **Wahrnehmung berechtigter Interessen für konkret festgelegter Zwecke** (Nr. 3)

erforderlich sind und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Umstand der Beobachtung und die verantwortliche Stelle sind z. B. durch einen Hinweis oder ein Schild erkennbar zu machen.

## Schutz der Beschäftigten

Im sogenannten nicht öffentlichen Raum, also im Bereich des Firmen- oder Werksgeländes ohne jeglichen Publikumsverkehr, gehen indes diese Persönlichkeitsrechte weiter. Dabei handelt es sich um Personen, die von Aufzeichnungen von der Kamera erfasst werden können. Werden dabei **vor Ort beschäftigte Personen** gefilmt oder gar aufgezeichnet, ist eine gezielte Überwachung nur zulässig, wenn ein konkreter Verdacht von Straftaten oder anderen schweren Verfehlungen besteht und keine weniger einschneidenden Mittel in Betracht kommen. Selbst wenn der Beschäftigte sich bei einer zulässigen Überwachung nur zufällig oder zwangsläufig im Blickfeld der Kamera befindet, sind seine **Persönlichkeitsrechte** zu **beachten**. Höchst private Bereiche wie Sanitär- oder Umkleideräume können von vornherein nicht überwacht werden.

Eine in der Praxis gängige Lösung besteht oft darin, die **Kameras nur außerhalb der Arbeitszeiten** einzuschalten und die nachts gemachten Aufnahmen innerhalb einer kurzen Zeit in einem sogenannten Ringspeicherverfahren zu löschen, sofern es nicht zu Diebstählen, Vandalismus oder anderen Vorfällen gekommen ist. Letzteres entspricht auch dem **Grundsatz der Speicherbegrenzung und der Datenminimierung**, wonach der Zweck angemessen und erheblich sowie auf das notwendige Maß beschränkt sein muss.

## Datenschutz beim Fotografieren

Diese Vorgaben gelten ebenfalls beim Einsatz von mobilen Endgeräten. Gerade im Baubereich werden durch die Kamerafunktion spontan – leider oftmals ohne Beachtung der Persönlichkeitsrechte – Fotos nicht nur zur Dokumentation des Baufortschritts, sondern auch bei der Mängelbeseitigung im bereits bewohnten Haus oder auch des Nachbarhauses gemacht. Bereits die zufällige Aufnahme der Bewohner oder deren Gäste ist jedoch gemäß § 22 des Kunstur-

hebergesetzes **nur mit deren ausdrücklicher Einwilligung** zulässig.

In der Praxis werden bereits bei der Aufnahme in der Wohnung höchstpersönliche Dinge zufällig fotografiert oder unbewusst in der Baudokumentation später in einem Aushang der Öffentlichkeit gezeigt, die einen Rückschluss auf die Lebensart oder andere höchstpersönliche sensible Dinge geben. Dabei wird außer Acht gelassen, dass jedes Merkmal, das in sachlicher oder persönlicher Hinsicht Rückschlüsse auf eine bestimmte oder bestimmbare natürliche Person zulässt, als personenbezogen anzusehen ist, vgl. § 3 BDSG. Dies hat zur Folge, dass nicht nur die Erhebung, sondern auch die Verarbeitung und Nutzung der Daten damit ohne Berechtigung in Form eines Vertrags oder einer Einwilligung erfolgt und damit nicht datenschutzkonform ist. Bei dieser Fallkonstellation ist somit relevant,

- wer auf dem Foto aufgenommen wird,
- wo diese auf dem mobilen Endgerät gespeichert und
- an wen diese mit oder ohne Zweck weitergeleitet werden.

Beim Datenschutz sind der Zweck der Datenerhebung, deren Verarbeitung oder Nutzung maßgebend. Erfolgt diese über den festgelegten Zweck hinaus, ist eine Aufnahme der Mängel oder gar einer Person nicht zulässig. Vielmehr kann es bei der unzulässigen Aufnahme zu **Schadensersatzansprüchen** kommen.

## Risiko: Datensicherung in der Cloud

Risiken bestehen des Weiteren hinsichtlich der Sicherheit und Vertraulichkeit der Daten beim Hochladen von sensiblen Daten in eine Cloud oder externen Plattformen wie Dropbox, die von einem Anbieter betrieben werden, der die Daten außerhalb der EU in einem Drittstaat (wie Indien oder USA) vorhält oder speichert, ohne dabei in seinem Land ein ausreichendes Datenschutzniveau zu garantieren. Hierzu bedarf es des Abschlusses eines Vertrags zur Auftragsdatenverarbeitung gemäß § 11 BDSG mit dem Auftragnehmer. Dies ist hier der Cloudanbieter, weil er die Daten im Auftrag weiter verarbeitet.

Weiter sollte eigentlich geprüft werden, ob der Anbieter nach Maßgabe die datenschutzrechtlichen Vorgaben des BDSG oder EU-Datenschutz-Richtlinien einhält und ob der Anbieter ausschließen kann, dass es zu Zugriffen aus den USA oder einem Drittstaat, z. B. zu Wartungszwecken, kommt. Dies ist jedenfalls gegeben, wenn der Anbieter zur Herausgabe der Inhalt der Cloud oder anderer Plattform durch (amerikanische) Behörden verpflichtet werden.

© goodluz – Fotolia.com

**1** | *Tablets und Smartphones sind auf der Baustelle praktisch, jedoch sollte der Datenschutz dabei nicht außer Acht gelassen werden.*

## Schutzbedürftigkeit von Daten

Die Rechtmäßigkeit der Datenerhebung richtet sich zudem auch nach der Schutzbedürftigkeit der Daten. Ein **besonderer Schutz** richtet sich dabei nach dem Stand der Technik und umfasst nicht nur Daten mit Personenbezug von Kunden oder anderen Dienstleistern, sondern v. a. auch an Daten, die dem Geschäftsgeheimnis unterliegen und deshalb vertraulich bleiben sollen, vgl. § 17 Gesetz gegen den unlauteren Wettbewerb (UWG). Dies kann ein Bauplan oder die Zeichnung eines besonders zu sichernden Gebäudes, einer Botschaft oder eines Hauses mit besonders zu sichernder Infrastruktur wie dem BND sein.

## Dienstliche und private Nutzung

Ein häufig vernachlässigtes Risiko im Baubereich besteht hinsichtlich der Frage nach der Art der Nutzung mobiler Endgeräte, denn oftmals fehlt eine derartige Festlegung. Stellt der Arbeitgeber seinen Beschäftigten z. B. ein Smartphone zur Verfügung, sollte er vor Inbetriebnahme klar festlegen, ob das Gerät allein zum dienstlichen oder auch gar privaten Gebrauch genutzt werden darf. Als Eigentümer der Sache ist er die verantwortliche Stelle im Datenschutz, damit auch haftbar, und sollte v. a. die Nutzung und Rückgabe verbindlich und schriftlich regeln. Sofern auch die private Nutzung erlaubt ist, kommt es regelmäßig zum Konflikt, dass der Zugriff des Arbeitgebers auf die privat genutzten Daten des Beschäftigten grundsätzlich aufgrund des Persönlichkeitsrechts bzw. dem **Telekommunikationsgeheimnis** nach dem Telekommunikationsgesetz (TKG) verboten ist. Es ist daher aus Sicht des Eigentümers ratsam, die private Nutzung von vornherein zu verbieten, um derartige Konflikte auszuschließen.

Höchst kritisch aus Sicht der Datensicherheit ist indes der umgekehrte Fall, bei dem der Beschäftigte sein eigenes privates Endgerät wie Tablet-PC oder Smartphone zur geschäftlichen Nutzung einsetzt. Auch wenn es auf den ersten Blick praktische und ökonomische Vorteile wie Einsparungen bei Beschaffung und Schulungsbedarf und ggf. eine höhere Produktivität hat, wiegen die Risiken schwer. In diesen Fällen, das als **„Bring your own Device“** (BYOD) bezeichnet wird, besteht ein erhöhtes Risikopotenzial für Eigentümer und Anwender.

Es kommt dabei nicht nur zur Vermischung von dienstlich und privat genutzten Daten, sondern auch zu einem Konflikt zwischen dem Inhaber des Endgeräts und dem Arbeitgeber, weil er beim Einsatz im Unternehmen die verantwortliche Stelle im Sinne des Datenschutzgesetzes bleibt. Vielmehr wird der Arbeitgeber bei der Erlaubnis der Nutzung privater Endgeräte zum Dienstanbieter gemäß dem TKG und ist damit auch für die rechtskonforme Einhaltung der gesetzlichen Vorgaben verantwortlich.

Aus diesen Gründen ist es notwendig, eine **schriftliche Festlegungen** zur Regelung der rechtlichen und technischen Details zu treffen. Diese kann in Form von Betriebsvereinbarungen oder in bestimmten Fällen in Einzelvereinbarungen erfolgen. Hierbei ist u. a. festzulegen, wie man die geschäftlichen und privaten Daten sauber voneinander trennt. Letztere unterliegen dem Telekommunikationsgeheimnis. Daher darf der Arbeitgeber keinen Zugriff darauf haben. Gleichwohl sind die Beschäftigten verpflichtet, die Verschwiegenheit über geschäftliche Daten einzuhalten.

Verliert ein Mitarbeiter sein privates Endgerät, und werden die Kunden- oder Personaldaten anderer (nicht berechtigten) Personen bekannt, kann im Einzelfall eine **Datenpanne** im Sinne des § 42a BDSG vorliegen, die eine Meldepflicht gegenüber dem Betroffenen und der Aufsichtsbehörde sowie Bußgeld und möglicherweise Reputationsschäden zur Folge haben kann.

Aus den rechtlichen und technischen Gründen ist der Einsatz eines sogenannten **Mobil-Device-Management** (MDM) zu empfehlen. Dies gilt zum einen, um einheitlichen Schutz im gesamten Unternehmen oder bei allen Beschäftigten zu erreichen. Zum anderen zielt es darauf ab, einen umfassenden höchst möglichen Schutz der Ziele der Informationssicherheit zu gewährleisten, um deren Vorgaben zu erfüllen. Damit werden Ziele wie Integrität, Vertraulichkeit und Verfügbarkeit von der Installation und Wartung bis hin zur datenschutzkonformen Einräumung von Rechten je nach Funktion, Rolle und Stellung im Unternehmen sichergestellt. Dabei muss hinsichtlich der Behandlung der Daten vielschichtig sichergestellt werden, dass ein Zugriff auf Daten der Beschäftigten von vornherein ausgeschlossen und bei Verlust der Daten das Löschen privater Daten notfalls über eine Einwilligung abgesichert wird.

Arbeitgebern ist aufgrund der genannten Risiken zu empfehlen, die einzusetzenden Geräte selber anzuschaffen. So können Risikobereiche durch eine einzugrenzende Zahl möglicher Hardware- und Softwarekombinationen vermindert und damit der Aufwand für Administration erheblich erleichtert werden. Ein einheitliches System stellt dabei nicht nur mehr Sicherheit in technischer und rechtlicher Hinsicht her, sondern kann Mengenrabatte im Einkauf und beim Abschluss von Wartungsverträgen bieten.

Im Gegensatz zum BYOD steht es dem Arbeitgeber als Eigentümer beim **„Choose your own Device“** (CYOD) frei, über die Nutzungsvorgaben zu entscheiden. Dies wird erfahrungsgemäß eine höhere Akzeptanz bei der Einhaltung der Nutzungsvereinbarungen und den damit verbundenen Einschränkungen infolge der datenschutzrechtlichen Vorgaben als beim Einsatz der eigenen Endgeräte bewirken. ■

- Verwenden Sie auch für Ihr Endgerät einen Virenschutz und eine Firewall. Vergewissern Sie sich, dass alle vorhandenen Sicherheitseinstellungen eingeschaltet sind, und aktualisieren Sie Apps und das Betriebssystem.
- Prüfen Sie unbekannte Nummern vor dem Rückruf.
- Nutzen Sie Sperrcodes und Passwörter. PIN und Bildschirmsperre sollten stets aktiviert sein.
- Besonders sensible Daten sind zu vermeiden oder durch ein Passwort zu schützen.
- Deaktivieren Sie Drahtlosschnittstellen wie Bluetooth, WLAN oder Infrarot, wenn Sie diese nicht benötigen. Sie erschweren die Erstellung von Bewegungsprofilen, wenn Sie die GPS- und WLAN-Funktion ausschalten, Öffentliche Hotspots (WLAN) sind mit erhöhter Vorsicht zu nutzen!
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen und prüfen Sie die Zugriffsberechtigungen.
- Sichern Sie Ihre gespeicherten Daten durch regelmäßige Backups. Speichern Sie die Backup-Dateien auf einem externen Medium (z. B. einer Speicherkarte) oder auf Ihrem PC.
- Löschen Sie alle Speicher, bevor Sie das Endgerät verkaufen oder entsorgen und vergessen Sie nicht, die SIM-Karte zu entfernen.

**2** | *Checkliste für sicheren Umgang mit mobilen Endgeräten, angelehnt an den „Basisschutz für Computer & Smartphone“ des Bundesamtes für Sicherheit in der Informationstechnik*