ZVEI: Die Elektroindustrie

Merkblatt | 82016:2018-08

Datenschutzaspekte im Beratungsgespräch

Hinweise für Planungs- und Installationsunternehmen der Sicherheitstechnik

Arbeitsgemeinschaft Errichter und Planer

Inhalt

1. Allgemeine Hinweise für Planungs- und Installationsunternehmen

Beim Einsatz moderner Sicherheitstechnik, insbesondere von Systemen zur Videoüberwachung oder der Zutrittskontrolle, können auch persönliche Informationen erfasst werden, die dem Datenschutz unterliegen. Wer solche Daten erhebt, verarbeitet oder nutzt, ist verpflichtet, sich an datenschutzrechtliche Regelungen zu halten. Neu ist an dieser Stelle die seit dem 25. Mai 2018 geltende Europäische Datenschutzgrundverordnung (DSGVO).

Für Mitarbeiter in Planungs- oder Installationsunternehmen für Sicherheitstechnik kommt der Datenschutz im Kunden- bzw. Beratungsgespräch fast zwangsläufig zur Sprache. Kunden wollen wissen, was beim Datenschutz zu beachten ist oder welche Maßnahmen technischer oder organisatorischer Art im Einzelnen umzusetzen sind. Vertriebs- und sonstige Mitarbeiter mit Kundenkontakt können in ein Dilemma geraten: Einerseits erwartet der Kunde hier eine umfassende Beratung, andererseits darf die Grenze zur unzulässigen Rechtsberatung nicht überschritten werden.

In Verkaufs- oder Beratungsgesprächen ist darauf zu achten, dass lediglich allgemeine Hinweise zu relevanten oder beachtenswerten rechtlichen Aspekten gegeben werden sollten. Werden konkrete Rechtsthemen diskutiert, kann schnell die Schwelle zur Rechtsberatung überschritten werden. Dabei ist nach dem Rechtsdienstleistungsgesetz (RDG) „Rechtsdienstleistung ... jede Tätigkeit in konkreten fremden Angelegenheiten, sobald sie eine rechtliche Prüfung des Einzelfalls erfordert" (§ 2, Abs. 1 RDG). Die Erbringung von Rechtsdienstleistungen ist einem definierten Personenkreis nach dem RDG vorbehalten, beispielsweise Rechtsanwälten.

Hinzu kommt: Ein Kunden- oder Vertriebsberater kann durch eine unzulässige Beratung neben dem RDG auch gegen das Gesetz gegen den unlauteren Wettbewerb (UWG) verstoßen mit der Folge einer möglichen wettbewerbsrechtlichen Abmahnung.

Grundsätzlich unproblematisch ist es, wenn im Verkaufs- oder Beratungsgespräch auf allgemeine Aspekte hingewiesen wird. Hierzu einige Beispiele:

- Es kann darauf hingewiesen werden, dass der Kunde datenschutzrechtliche Rahmenbedingungen zu beachten hat, die in für ihn geltenden gesetzlichen Datenschutzvorschriften – insbesondere der DSGVO – enthalten sind.

- Das maßgebliche Gesetz in Bezug auf datenschutzrechtliche Vorgaben ist seit dem 25. Mai 2018 in der gesamten Europäischen Union die DSGVO. Daneben können für den Kunden aber auch weitere bereichsspezifische Datenschutzgesetze relevant werden, die an bestimmten Stellen, an denen die DSGVO Öffnungsklauseln vorsieht, weitere Konkretisierungen vornehmen. In erster Linie ist hier das an die DSGVO angepasste neue Bundesdatenschutzgesetz (BDSG) zu nennen.

- Verantwortliche Stellen (z. B. Unternehmen, Behörden, Vereine) oder deren Auftragsverarbeiter müssen unter Umständen einen Datenschutzbeauftragten benennen, damit dieser sich um die Klärung und Prüfung datenschutzrechtlicher Fragestellungen kümmert. Dabei kann sich eine Benennungspflicht sowohl aus der DSGVO als auch dem BDSG ergeben. Nach der DSGVO muss beispielsweise ein Datenschutzbeauftragter benannt werden, wenn die Kerntätigkeit des Verantwortlichen (oder des Auftragsverarbeiters) in der umfangreichen oder systematischen Überwachung von Personen liegt (Art. 37 DSGVO). Nach dem BDSG besteht zum Beispiel dann eine Benennungspflicht, wenn beim Verantwortlichen (oder Auftragsverarbeiter) in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 BDSG). Führt der Verantwortliche eine Datenschutz-Folgenabschätzung durch, so ist der Rat eines benannten Datenschutzbeauftragten einzuholen.

- Besteht eine Mitarbeitervertretung (z. B. Betriebsrat, Personalrat) im Unternehmen oder Betrieb, müssen gegebenenfalls Mitbestimmungsrechte (z. B. § 87 Betriebsverfassungsgesetz – BetrVG) gewahrt werden.

- Es obliegt letztendlich dem Kunden, ob und wie er den für ihn einschlägigen Datenschutzbestimmungen gerecht wird. Vernachlässigt er das, was zwingend notwendig ist, muss er beispielsweise mit einem Bußgeld rechnen (Art. 83 DSGVO, § 41 BDSG). Ein solches kann nach den neuen Regelungen im Extremfall bei bis zu vier Prozent des gesamten Konzernjahresumsatzes oder 20 Millionen Euro liegen (je nachdem, was höher ist).

Ein Kunde ist stets gut beraten, wenn er zur Klärung (datenschutz-)rechtlicher Fragen seinen Datenschutzbeauftragten oder einen Rechtsanwalt seines Vertrauens hinzuzieht. Diese können die Vereinbarkeit des konkreten Vorhabens mit rechtlichen Rahmenbedingungen unter den spezifischen Umständen des Einzelfalls prüfen. Bei rechtzeitiger Einbindung können sie im Vorfeld Hinweise und Empfehlungen für konkrete Projekte aus datenschutzrechtlicher Sicht geben.

Darüber hinaus können sich Unternehmen und Datenschutzbeauftragte auch an die zuständige Aufsichtsbehörde für den Datenschutz wenden. Diese hat nach Art. 51 ff. DSGVO einen gesetzlichen Kontrollauftrag. Sie berät und unterstützt verantwortliche Stellen und deren Datenschutzbeauftragte mit Rücksicht auf deren typische Bedürfnisse.

2. Praxistipps für das Beratungsgespräch

Bei der Beratung von Kunden sollten folgende Hinweise beachtet werden:

- **Nur allgemeine Hinweise geben**
  Bei Fragen seitens des Kunden, was datenschutzrechtlich erlaubt ist (und was ggf. nicht), sollte deutlich klargestellt werden, dass keine juristische Bewertung abgegeben und der Kunde nicht umfassend datenschutzrechtlich beraten werden kann. Zulässig sind allgemeine Hinweise, anhand derer sich der Kunde weiter informieren kann.

- **Perspektive des Planungs- bzw. Installationsunternehmens kann weder verbindlich noch vollständig sein**
  Auch allgemeine Äußerungen können vom Kunden als verbindliche Aussagen verstanden werden. Es sollte daher darauf hingewiesen werden, dass Hinweise des Planungs- bzw. Installationsunternehmens weder verbindlich sind noch alle denkbaren und zu beachtenden Aspekte berücksichtigen können.

- **Nicht zu unhaltbaren Zusagen verleiten lassen**
  Sofern der Kunde ganz konkrete Zusagen verlangt, ist äußerste Vorsicht und Zurückhaltung geboten. Ob etwa eine Videoüberwachung in einer konkreten Ausgestaltung zulässig und damit datenschutzkonform ist, hängt von verschiedenen und nicht immer offensichtlichen Faktoren und Rahmenbedingungen ab. Es sollte im Gespräch deutlich signalisiert werden, dass die Verantwortung in letzter Konsequenz stets beim Kunden liegt, insbesondere für die Einhaltung datenschutzrechtlicher Anforderungen.

- **Zur Beantwortung rechtlicher Fragen an Spezialisten verweisen**
  Zur Beantwortung konkreter rechtlicher Fragestellungen sollte ein zuständiger Spezialist hinzugezogen werden. Dies kann neben dem benannten Datenschutzbeauftragten und den Datenschutzaufsichtsbehörden auch ein niedergelassener Rechtsanwalt mit datenschutzrechtlicher Spezialisierung sein.

3. Videoüberwachung

In Verkaufs- oder Beratungsgesprächen für Anlagen und Systeme zur Videoüberwachung ist darauf zu achten, dass allenfalls allgemeine Hinweise zu relevanten oder beachtenswerten rechtlichen Aspekten, ohne Vollständigkeit in der Sache oder Berücksichtigung sämtlicher gegebenenfalls zu berücksichtigender Details, gegeben werden können.

Beispiele:

- Bei Bilddaten handelt es sich in der Regel um Daten, die einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können; sie können damit datenschutzrechtlichen Bestimmungen unterliegen. Nach der DSGVO ist die Verarbeitung personenbezogener Daten durch einen Verantwortlichen oder Auftragsverarbeiter nur dann gestattet, wenn ihm das Gesetz ausdrücklich eine Erlaubnis dazu einräumt. Nach Art. 6 DSGVO kann eine solche Erlaubnis unter anderem in der Einwilligung der betroffenen Person oder in einem berechtigten Interesse des Verantwortlichen bzw. eines Dritten liegen.

- Wichtige rechtliche Aspekte zur Videoüberwachung im öffentlich zugänglichen Raum (z. B. Tankstellen, Supermärkte, Parkhäuser) enthält § 4 BDSG. Bei nicht öffentlich zugänglichen Räumen (z. B. Firmengelände, Lagerhallen) kommen § 87 Betriebsverfassungsgesetz – BetrVG, insbesondere Art. 88 DSGVO sowie §§ 24 und 26 BDSG in Betracht.

- Datenschutzaufsichtsbehörden halten zum Teil beim Einsatz von Videoüberwachung eine Datenschutz-Folgenabschätzung grundsätzlich für erforderlich.

- Wichtig ist auch die Einhaltung datenschutzrechtlicher Grundprinzipien. Im Kontext Datensicherheit ist die Umsetzung angemessener technischer und organisatorischer Maßnahmen (vgl. Art. 32 DSGVO) sowie die Implementierung von „Privacy by Design" und „Privacy by Default" (Art. 25 DSGVO) zu beachten. Zudem steht an oberster Stelle die Wahrung der Rechte der Betroffenen (Art. 12 ff. DSGVO) bzw. die Einhaltung des Grundsatzes der Datenvermeidung und Datensparsamkeit (vgl. Art. 5 DSGVO).

- Soweit Videoüberwachung in Unternehmen eingesetzt wird und eine Mitarbeitervertretung (z. B. Betriebsrat) in Unternehmen oder Betrieben besteht, müssen gegebenenfalls Mitbestimmungsrechte (z. B. § 87 Betriebsverfassungsgesetz – BetrVG) gewahrt werden.

- Wird Videoüberwachung von Privatpersonen für private Zwecke etwa auf dem eigenen Grundstück eingesetzt, sind die Bestimmungen der Datenschutzgesetze meist nicht verbindlich. Allerdings ist damit nicht jegliche Überwachung erlaubt. Auch hier sind grundsätzliche Aspekte zu beachten, etwa die Beschränkung der Videoüberwachung auf das eigene Grundstück. Bei Verstößen dagegen können Betroffene wie Nachbarn gegebenenfalls zivilrechtliche Unterlassungs- oder Beseitigungsansprüche geltend machen.

- Beim Einsatz von Videoüberwachung sind die Informationspflichten (Hinweisschilder) nach Art. 13 DSGVO zu erfüllen. Der Umfang der Informationspflichten bemisst sich dabei nach den Umständen der Videoüberwachung.

  Wichtige Fallgruppen sind:
  - die Videoüberwachung öffentlich zugänglicher Räume nach § 4 BDSG,
  - die Videoüberwachung nicht öffentlich zugänglicher Räume ohne Beschäftigte nach Art. 6 f DSGVO und
  - die Videoüberwachung nicht öffentlich zugänglicher Räume mit betroffenen Beschäftigten nach Art. 6 f DS-GVO und gegebenenfalls § 26 BDSG.

4. Zutrittskontrolle

Auch beim Einsatz von Zutrittskontrolleinrichtungen kann es notwendig sein, persönliche Informationen zu verarbeiten. Beispiele sind unter anderem die auf einem Mitarbeiterausweis gespeicherten Informationen wie Name und Bild.

Soweit notwendig, kann im Beratungsgespräch auf die folgenden allgemeinen datenschutzrechtlichen Aspekte hingewiesen werden:

- Jede Verarbeitung personenbezogener Daten durch einen Verantwortlichen oder Auftragsverarbeiter bedarf einer gesetzlich geregelten Erlaubnis (Art. 6 DSGVO). Beinhaltet eine Zutrittskontrolleinrichtung entsprechende Informationen, muss diese Anforderung berücksichtigt werden.

- Spezielle datenschutzrechtliche Vorgaben, wie es sie etwa zur Videoüberwachung gibt, bestehen für das Thema Zutrittskontrolle nicht. In Betracht kommen insbesondere die allgemeinen Zulässigkeitsvorschriften der Art 6, 7 und 88 DSGVO oder der §§ 24 und 26 BDSG.

- Werden zur Steuerung des Zutritts biometrische Merkmale verwendet, können Risiken für die Rechte und Freiheiten natürlicher Personen bestehen, sodass eine Datenschutz-Folgenabschätzung, sprich eine datenschutzrechtliche Vereinbarkeitsprüfung, notwendig ist (Art. 35 DSGVO). Bei einer solchen ist der Rat eines benannten Datenschutzbeauftragten einzuholen. Auch in anderen Fällen ist die Beratung durch einen Fachmann, sprich den Datenschutzbeauftragten oder Rechtsanwalt, sinnvoll.

- Wichtig ist auch die Einhaltung datenschutzrechtlicher Grundprinzipien. Im Kontext Datensicherheit ist die Umsetzung angemessener technischer und organisatorischer Maßnahmen (vgl. Art. 32 DSGVO) sowie die Implementierung von „Privacy by Design" und „Privacy by Default" (Art. 25 DSGVO) zu beachten. Zudem muss an oberster Stelle die Wahrung der Rechte der Betroffenen (Art. 12 ff. DSGVO) oder die Einhaltung des Grundsatzes der Datenvermeidung und Datensparsamkeit (vgl. Art. 5 DSGVO) stehen.

- Mit einer Zutrittskontrolleinrichtung kann auch eine Verhaltenskontrolle einhergehen. Weil schon die bloße Möglichkeit ausreicht, sind die Mitbestimmungsrechte (z. B. § 87 Abs. 1 Nr. 6 BetrVG) einer Mitarbeitervertretung zu wahren, sofern diese im Unternehmen oder Betrieb besteht.

- Sollen moderne Zutrittskontrolleinrichtungen im privaten Umfeld, beispielsweise zur Absicherung von Haus und Wohnung, eingesetzt werden, müssen für den Kunden die gesetzlichen Datenschutzbestimmungen zwar nicht verbindlich sein, aber auf ein Mindestmaß an Datenschutz und Datensicherheit sollte dieser dennoch bedacht sein. Code- und Zutrittsberechtigungskarten sollte er sicher verwahren. Passwörter sollten so gewählt werden, dass sie einen Mindestschutz bieten und nicht einfach zu erraten sind.

ZVEI:
Die Elektroindustrie

Datenschutzaspekte im Beratungsgespräch

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Fachverband Sicherheit
Arbeitsgemeinschaft Errichter und Planer
Lyoner Straße 9
60528 Frankfurt am Main

Verantwortlich: Peter Krapp
Geschäftsführer Fachverband Sicherheit und Arge Errichter und Planer
Telefon: +49 69 6302-245
Fax: +49 69 6302-1245
E-Mail: krapp@zvei.org

Autoren:
Dominik Grossmann, Bosch Sicherheitssysteme
Tarek El Hawi, ZVEI

www.zvei.org

August 2018, 2., überarbeitete Auflage

Das Merkblatt entstand durch die Arge Errichter und Planer sowie den Fachkreis Videosysteme im Fachverband Sicherheit.