

Smart Lighting verstehen und gestalten

Ein Überblick für Hersteller, Planer, Betreiber und Nutzer

Günter Martin, 26.09.2018, komplett überarbeitet 17.09.2026



Das Licht ist smart geworden. Smart Lighting verbindet energieeffiziente LED-Technik mit intelligenter Steuerung, Sensorik und vernetzten Gebäudefunktionen. Die Anwendungen reichen von komfortablen Lichtszenen im Smart Home über bedarfsgerechte Arbeitsplatzbeleuchtung bis zur Betriebs- und Wartungsoptimierung im Zweckbau.

Dabei geht es um mehr als Energieeinsparung: Lichtqualität, die Wirkung auf den Menschen und das Zusammenspiel mit anderen Systemen prägen den Nutzen. Wer Smart Lighting verstehen und gestalten will, muss deshalb Technologien und Kommunikationsstandards ebenso kennen wie die Anforderungen an Planung, Installation und langfristigen Betrieb. Datenschutz, Cybersecurity und aktuelle gesetzliche Vorgaben gehören dabei von Anfang an dazu. Der Beitrag gibt Herstellern, Planern, Betreibern und privaten Nutzern einen Überblick über Möglichkeiten, Grenzen und Verantwortlichkeiten – auf dem Stand September 2026.

Inhalt

1	Was ist Smart Lighting?	3
2	Wie funktionieren Smart Lighting Systeme?	4
3	Welche Standards sind einzuhalten?	6
4	Welche Einsatzfelder gibt es?	8
5	Warum Datensicherheit?	10
6	Wie wird Datensicherheit erreicht?	11
7	Warum Datenschutz?	15
8	Wie wird Datenschutz erreicht?	16
9	Was bringt die Zukunft?	17
10	Quellenverzeichnis	18

1 Was ist Smart Lighting?

Smart Lighting vereint die Merkmale, die an intelligente Leuchten gestellt werden. In der folgenden Abbildung sind sie dargestellt und anschließend im einzelnen beschrieben.

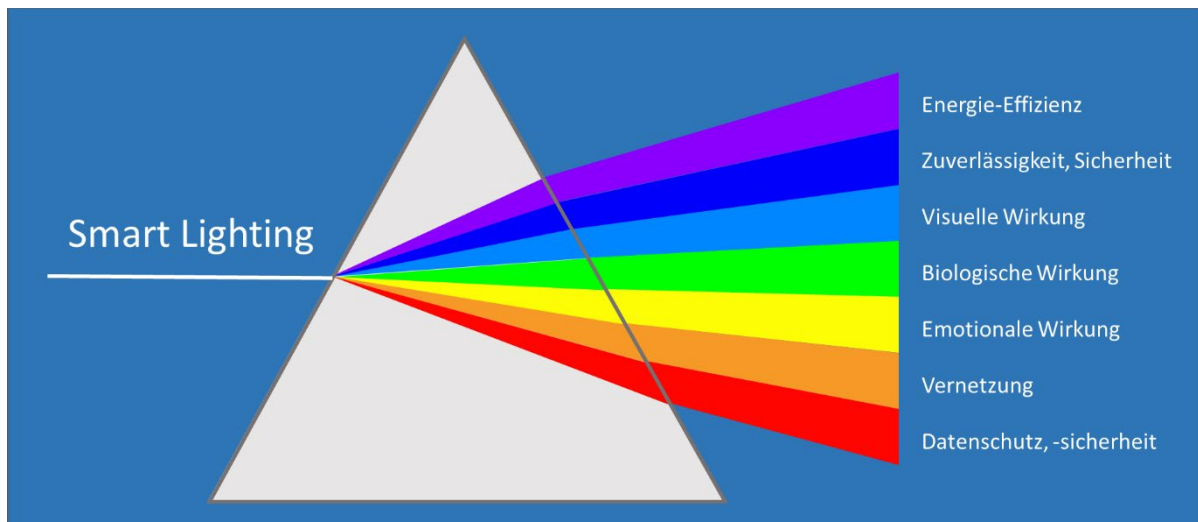


Abbildung 1: Smart Lighting umfasst das gesamte Spektrum von der Energie-Effizienz bis zum Datenschutz

Energieeffizienz und Zuverlässigkeit sind die ersten in der Abbildung genannten Punkte. LED-Technik hat den Strombedarf der Beleuchtung deutlich gesenkt. Smart Lighting erschließt zusätzliche Einsparungen durch Tageslichtregelung, Präsenzsteuerung und passende Betriebszeiten. Entscheidend ist der Verbrauch des gesamten Systems einschließlich Treibern, Sensoren, Gateways und Bereitschaftsbetrieb.

Für einen sachgerechten Vergleich zählen Lichtstrom in Lumen, elektrische Leistung in Watt und Lichtausbeute in Lumen pro Watt. Hinzu kommen Farbwiedergabe, Lichtverteilung und Betriebsbedingungen. Aktuelle Produktdaten lassen sich über das EU-Energielabel und die Datenbank EPREL vergleichen. Seit September 2021 gilt für Lichtquellen die Skala A bis G statt A+ und A++. Eine vernetzte Lichtquelle erreicht nicht automatisch eine bestimmte Klasse. [1]

Auch die Lebensdauer ist differenziert zu betrachten. Angaben von beispielsweise 25.000 oder 50.000 Betriebsstunden sind keine Garantie für ebenso viele störungsfreie Stunden des Gesamtsystems. Lichtstromrückgang, Ausfall von Treibern, Temperatur und Schaltzyklen spielen eine Rolle. Bei drei Stunden täglicher Nutzung entsprechen 25.000 Stunden rechnerisch etwa 23 Jahren; daraus folgt keine Zusage für Elektronik, Cloud-Dienste oder Sicherheitsupdates. Bei der Beschaffung sind deshalb Austauschbarkeit, Ersatzteile, Garantiebedingungen und Software-Unterstützung gesondert zu vereinbaren.

Die **visuelle, biologische und emotionale Wirkung** von Licht wird häufig unter „Human Centric Lighting“ (HCL) zusammengefasst. Die Internationale Beleuchtungskommission CIE verwendet den Begriff „integrative lighting“. Gute Planung verbindet Sehaufgabe, Wohlbefinden, Tageslicht, Energiebedarf und Umweltwirkungen. Dabei ist nicht jede beworbene Gesundheits- oder Produktivitätswirkung wissenschaftlich gesichert. [2]

Licht beeinflusst unter anderem die innere Uhr. Für nichtvisuelle Wirkungen zählen Spektrum, Intensität am Auge, Zeitpunkt, Dauer und vorausgegangene Lichtexposition. Die Farbtemperatur allein reicht als Maß nicht aus. CIE S 026:2018 definiert geeignete α -optische Größen, darunter die melanopische

äquivalente Tageslichtbeleuchtungsstärke (melanopic EDI). Die CIE empfiehlt in ihrer Stellungnahme von 2024 viel Licht am Tag, weniger Licht vor dem Schlafen und möglichst Dunkelheit im Schlaf; Blendung und Energieverbrauch bleiben zu berücksichtigen. [2]

Vernetzung ergänzt die elektrische Versorgung um Steuer- und gegebenenfalls Sensordaten. Dafür stehen kabelgebundene und drahtlose Lösungen zur Verfügung. Leuchten können geschaltet, gedimmt und je nach Ausstattung in ihrer Farbtemperatur oder Farbe verändert werden. Rückmeldungen betreffen beispielsweise Energieverbrauch, Betriebsstunden und Fehlerzustände. Präsenz-, Helligkeits- oder weitere Sensoren können integriert oder separat angeordnet sein. Weder Farblicht noch Personenerfassung ist Voraussetzung für Smart Lighting.

Damit wird die Leuchte Teil eines IT- beziehungsweise Automatisierungssystems. Solche Ökosysteme verbinden Lichtsteuerung, Sensorik und weitere Gebäudefunktionen. Die Architektur entscheidet, welche Daten das Gerät verlassen, ob eine Zentrale benötigt wird und wie gut die Beleuchtung bei einem Netz- oder Dienstaussfall weiterarbeitet. Für intelligente Leuchten standardisiert D4i beispielsweise Leuchten-, Energie- und Diagnosedaten. [3]

Datenschutz und Datensicherheit müssen daher von Anfang an Kernelemente von Smart Lighting sein. Akzeptanz entsteht durch nachvollziehbare Funktionen, eine datensparsame Gestaltung und klare Regeln darüber, welche Daten zu welchem Zweck verarbeitet werden. Sicherheits- und Datenschutzpflichten betreffen unterschiedliche Beteiligte und sind über den gesamten Betrieb zu organisieren. [4–6]

2 Wie funktionieren Smart Lighting Systeme?

Abbildung 2 zeigt eine mögliche Architektur mit Funknetz, Gateway und optionalen Cloud-Diensten. Daneben gibt es vollständig lokale und kabelgebundene Systeme. Bei Thread verbindet ein Border Router das IPv6-Funknetz mit anderen IP-Netzen; er ist nicht mit einer anwendungsspezifischen Protokollbrücke gleichzusetzen. [7]

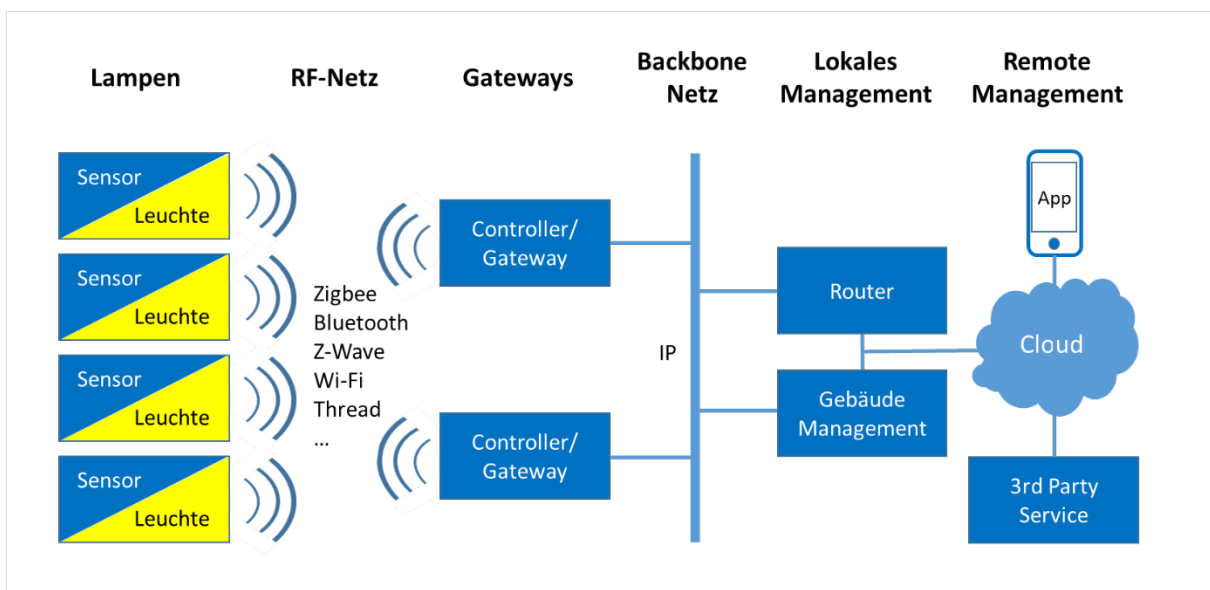


Abbildung 2: Architektur Smart Lighting, beispielhaft

Lampen sind der sichtbare Teil eines Smart Lighting-Systems. Alles andere läuft im Hintergrund. Unterschieden wird zwischen „Lampe“ und „Leuchte“. Die **Leuchte** ist das vollständige Beleuchtungsgerät einschließlich der zum Betrieb und zur Lichtverteilung nötigen Komponenten. Die **Lampe** ist die Lichtquelle beziehungsweise das Leuchtmittel. LED-Lichtquellen können austauschbar oder fest eingebaut sein.

Smart Lighting kann bereits durch Schalten und Dimmen entstehen. Für einstellbares Weiß („Tunable White“) werden häufig LEDs unterschiedlicher Farbtemperatur kombiniert; für Farblicht kommen etwa RGB- oder RGBW-Systeme zum Einsatz. Weißes Licht aus RGB-Kanälen hat nicht automatisch gute Farbwiedergabeeigenschaften. Kommunikation und Sensorik sind zusätzliche Funktionen. Ob Personen lediglich als anwesend erkannt, gezählt oder räumlich verfolgt werden, hängt von Sensorprinzip, Auflösung und Auswertung ab.

Über das **RF-Netz** (Radio Frequency) kommunizieren die Lampen drahtlos mit ihrer Umgebung. Einige RF-Netze sind meshed (vermascht): Jede Leuchte empfängt die Signale der benachbarten Leuchten und sendet sie weiter. Auf die Weise wird die Reichweite erhöht. Es gibt verschiedene Funkprotokolle. Welche zum Einsatz kommt, muss bei der Planung entschieden werden. Eine Orientierung gibt die nachfolgende Tabelle. Sie unterscheidet Netztechnologien und die darüber liegenden Anwendungsstandards. [7, 9–12]

	Zigbee ist ein verbreitetes Funk- und Anwendungssystem für Beleuchtung und Gebäudeautomation. Die CSA veröffentlichte Zigbee 4.0 im November 2025 mit zusätzlichen Sicherheits- und Integrationsfunktionen; Suzi bezeichnet die Sub-GHz-Erweiterung. Neue Funktionen sind nicht automatisch in Bestandsgeräten verfügbar. Reichweite und Skalierung hängen von Aufbau, Frequenz, Implementierung und Funkumgebung ab. [10]
	Bluetooth Mesh ist eine eigene Spezifikation auf Basis von Bluetooth Low Energy; Mit Bluetooth 5 wurde die Vermaschung eingeführt, über die sich auch große Netze realisieren lassen. Mesh 1.1 erweitert unter anderem Weiterleitung, Inbetriebnahme und Geräteaktualisierung. Der Funktionsumfang der konkreten Produkte und das Schlüsselmanagement sind entscheidend. Eine unbegrenzte Netzgröße oder grundsätzliche Überlegenheit gegenüber Zigbee lässt sich daraus nicht ableiten. [11]
	Z-Wave arbeitet mit regional unterschiedlichen Sub-GHz-Frequenzen. Die Vermaschung, die Bluetooth erst Mitte 2017 einführt, wurde bei Z-Wave bereits lange vorher realisiert. Klassisches Z-Wave-Mesh und Z-Wave Long Range sind zu unterscheiden: Long Range verwendet eine Sterntopologie und unterstützt bis zu 4.000 Knoten. Die europäische Zertifizierung für Long Range wurde 2025 erweitert. Frequenzregion, Controller, Geräteunterstützung und Sicherheitsfunktionen müssen zusammenpassen. [12]
	WLAN bindet Geräte direkt in IP-Netze ein und ist der Standard, wenn es nicht um batteriebetriebene IoT-Geräte geht. Denn der Stromverbrauch ist sehr viel höher als bei den anderen Funklösungen. Für netzversorgte Leuchten ist WiFi eine mögliche und am Markt erhältliche Lösung. Leistungsaufnahme, Funkabdeckung und Kapazität sind produktabhängig. Aus WLAN folgt weder automatisch hohe Sicherheit noch der Ausschluss einer bestimmten Energieeffizienzklasse. Für batterieversorgte Sensoren ist der tatsächliche Energiebedarf gesondert zu prüfen. [1, 9]
	Thread ist ein stromsparendes IPv6-Mesh auf IEEE 802.15.4. Es transportiert Daten und benötigt für die Einbindung in andere IP-Netze einen Border Router. Die Anwendungsfunktion liefert etwa Matter; Thread allein garantiert keine gemeinsame Lichtsteuerung. Thread 1.4 verbessert unter anderem die Zusammenarbeit von Netzen

	und Border Routern. Bestandsgeräte müssen die benötigten Funktionen tatsächlich unterstützen. [7]
 matter	Matter ist ein IP-basierter Anwendungsstandard, kein eigener Funkstandard. Es nutzt insbesondere Thread, WLAN und Ethernet; Bluetooth LE unterstützt typischerweise die Inbetriebnahme. Matter 1.6 wurde am 17. Juni 2026 veröffentlicht. Zertifizierte Gerätetypen, unterstützte Funktionen und Controller-Versionen sind gemeinsam zu prüfen. Matter ermöglicht lokale Kommunikation, garantiert aber weder vollständige Funktionsgleichheit noch den Verzicht eines Anbieters auf Cloud-Dienste. [9]
	DALI-2 ist ein zertifiziertes System für die digitale Lichtsteuerung auf Grundlage der IEC-62386-Reihe. D4i erweitert es um standardisierte Daten und Versorgungsfunktionen in intelligenten Leuchten. DALI+ ermöglicht DALI-Kommunikation über drahtlose und IP-basierte Netze. Diese Lösungen ergänzen die Funkverfahren in dieser Tabelle; sie sind keine austauschbaren Bezeichnungen für dieselbe Technik. [3]

Tabelle 1: Kommunikationslösungen für Smart Lighting. Funktionen, Zertifizierung und gemeinsame Geräteunterstützung sind projektspezifisch zu prüfen.

Gateways verbinden unterschiedliche Protokollwelten, beispielsweise Zigbee-Leuchten mit einem IP-basierten Gebäude- oder Smart-Home-System. Thread Border Router leiten dagegen IPv6-Pakete weiter. Ein WLAN-Gerät benötigt nicht zwingend eine eigene Lichtbrücke. Gateway, Controller, Border Router und Firewall sind verschiedene Funktionen, auch wenn ein Produkt mehrere davon bündelt. Keine dieser Bezeichnungen garantiert allein einen wirksamen Schutz des Netzes. [7, 9]

Das **lokale Gebäudemanagement** richtet Geräte ein, steuert Szenen und verarbeitet erforderliche Betriebsdaten. Taster, Bedienpanels, Apps und Automatisierungsregeln können nebeneinander bestehen. Im Zweckbau sind kabelgebundene Lösungen wie DALI-2 und die Anbindung an übergeordnete Gebäudeautomation weiterhin wichtig. Lokale Bedienbarkeit, definierte Ausfallzustände und ein getesteter Wiederanlauf sind in die Planung aufzunehmen. Sicherheitsbeleuchtung benötigt eine eigenständige, normgerechte Auslegung. [3, 13]. Selbstverständlich ist das Gebäudemanagement nicht auf die Steuerung der Beleuchtung beschränkt, sondern soll alle smarten Komponenten im Haus integrieren.

Für das **remote Management** gehen die Daten in die Cloud. Externe Dienste können zusätzliche Analysen ermöglichen, erzeugen aber Abhängigkeiten von Konto, Netzverfügbarkeit, Anbieter und Vertragsbedingungen. Eine Sprachsteuerung kann je nach System auch lokal arbeiten; sie benötigt nicht generell eine Cloud. Vor der Auswahl der Cloud sind Datenflüsse, Speicherorte, Drittanbieter, Löschmöglichkeiten und die Folgen eines Dienst-Endes zu prüfen. [4–6].

3 Welche Standards sind einzuhalten?

Für Lampen, Leuchten und ihre digitalen Dienste gelten unterschiedliche gesetzliche und normative Anforderungen. Tabelle 2 bietet eine Orientierung für Deutschland und die EU. Normen sind von unmittelbar geltendem Recht und national umzusetzenden Richtlinien zu unterscheiden. Eine im EU-Amtsblatt gelistete harmonisierte Norm begründet nur für die tatsächlich abgedeckten Anforderungen eine Konformitätsvermutung; Veröffentlichungen und Einschränkungen sind für das konkrete Produkt zu prüfen. [8, 14–18]

Energie-Effizienz	Verordnungen (EU) 2019/2020 (Ökodesign für Lichtquellen und separate Betriebsgeräte) und 2019/2015 (Energiekennzeichnung von Lichtquellen, A bis G); Produktdaten in EPREL. Es ist eine allgemeine Pflicht „Leuchten mindestens Klasse A“. [1]
Zuverlässigkeit, Sicherheit	EN IEC 60598-1 und zutreffende Teile 2 für Leuchten; EN 62560 für bestimmte LED-Lampen; EN 62471 zur photobiologischen Sicherheit sowie passende EMV-Normen. Für Funkprodukte RED 2014/53/EU, sonst je nach Produkt Niederspannungs- und EMV-Recht. Die GPSR (EU) 2023/988 gilt seit 13.12.2024 ergänzend, soweit Aspekte und Risiken nicht bereits durch spezielles EU-Recht erfasst sind. [8, 14, 29]
Visuelle Wirkung	Arbeitsstättenverordnung mit ASR A3.4 (Mai 2023) sowie DIN EN 12464-1:2021-11 für Arbeitsstätten in Innenräumen. Anforderungen sind tätigkeits- und raumbezogen; bei Sicherheitsbeleuchtung gelten zusätzliche Regeln. [13]
Biologische Wirkung	CIE S 026:2018 definiert Messgrößen für α -optische Wirkungen. CIE PS 001:2024 ordnet integrative Beleuchtung ein. Messner und Planungsempfehlung sind von verbindlichen Mindestanforderungen zu unterscheiden. [2]
Emotionale Wirkung	Keine quantitativen Vorgaben. Gestalterische Ziele wie Orientierung, Atmosphäre und individuelle Steuerbarkeit sind projektspezifisch. Eine Farb- oder Helligkeitseinstellung garantiert keine bestimmte Emotion, Gesundheit oder Produktivität. [2]
Vernetzung	Passende Spezifikationen und Zertifizierungen für DALI-2/D4i, Zigbee, Bluetooth Mesh, Z-Wave, Thread und Matter. Die Versionsnummer allein belegt keine Systemkompatibilität. [3, 7, 9–12]
Datenschutz Datensicherheit	DSGVO, ergänzend BDSG und gegebenenfalls TDDDg. RED-Cybersecurity nach (EU) 2022/30 seit 01.08.2025; EN 18031-1/-2/-3:2024 mit Einschränkungen harmonisiert. CRA (EU) 2024/2847: Art.-14-Meldepflichten seit 11.09.2026, zentrale Produktpflichten ab 11.12.2027. ETSI EN 303 645 bietet eine technische Basis, keine pauschale CRA-Konformität. [4–6, 14–18, 25, 26]

Tabelle 2: Wichtige Regelwerke und ihre Einordnung, Stand 17. September 2026. Die Auswahl ersetzt keine produkt- und anlagenbezogene Konformitätsbewertung.

Für Lichtquellen und separate Betriebsgeräte sind insbesondere die Ökodesign-Verordnung (EU) 2019/2020 und die Energiekennzeichnung nach (EU) 2019/2015 maßgeblich. Die frühere Behauptung, Leuchten müssten generell mindestens Klasse A erreichen, trifft nicht zu. Zur elektrischen und mechanischen Sicherheit gehört die Normenreihe EN IEC 60598; für bestimmte LED-Lampen ist EN 62560 relevant. Photobiologische Sicherheit und elektromagnetische Verträglichkeit sind zusätzlich zu berücksichtigen. Bei Funkanlagen erfasst die RED neben Funkanforderungen auch Sicherheits- und EMV-Schutzziele. [1, 8, 14]

Für Arbeitsstätten gelten die Arbeitsstättenverordnung und die konkretisierende ASR A3.4 „Beleuchtung und Sichtverbindung“ in der Ausgabe Mai 2023. DIN EN 12464-1:2021-11 behandelt die Beleuchtung von Arbeitsstätten in Innenräumen. Maßgeblich sind unter anderem Sehauflage, Beleuchtungsstärke, Gleichmäßigkeit, Blendungsbegrenzung und Farbwiedergabe. Eine pauschale Empfehlung, deutlich heller als vorgeschrieben zu beleuchten, ist ungeeignet: Mehr Licht kann auch blenden und unnötig Energie verbrauchen. [13]

Für nichtvisuelle Wirkungen ist CIE S 026:2018 eine messtechnische Grundlage, keine allgemeine Zusage gesundheitlicher Wirkungen. Bei vernetzter Beleuchtung kommen Datenschutz und Cybersecurity hinzu. Seit 1. August 2025 gelten für die von der Delegierten Verordnung (EU) 2022/30 erfassten Funkanlagen zusätzliche RED-Anforderungen an Netzschutz, Datenschutz und gegebenenfalls Betrugsschutz. Dazu gehören auch bestimmte Geräte, **die** nur mittelbar über ein Gateway mit dem Internet kommunizieren. EN 18031-1/-2/-3:2024 wurden mit Einschränkungen harmonisiert. Die Aufhebung von (EU) 2022/30 durch (EU) 2026/339 wirkt erst ab 11. Dezember 2027. [2, 14–16]

4 Welche Einsatzfelder gibt es?

Präsenz-, Radar-, Infrarot- oder optische Sensoren können die Beleuchtung an die Raumnutzung anpassen. Je nach Technik sind auch Personenzählung und Bewegungsinformationen möglich. Ein kleiner Mikrochip, 5 x 5 mm, reicht aus und schon weiß die Leuchte, wie viele Personen im Raum sind, ob sie sich bewegen und, falls ja, in welche Richtung und mit welcher Geschwindigkeit. Die benachbarten Leuchten erhalten die Information und können sich bereits einschalten, wenn voraussichtlich gleich jemand den Raum betritt. Klassische Bewegungsmelder, die erst reagieren, wenn man schon im Raum ist, und die das Licht abschalten, wenn man sich nicht mehr bewegt, haben ausgedient.

Im Büro lassen sich beispielsweise Belegung und Nutzungsdauer von Besprechungsräumen auswerten, um Flächen und Reinigung besser zu planen. Dafür reichen oft zeitlich und räumlich aggregierte Informationen. Die Lichtsteuerung sollte auch ohne einen zentralen Cloud-Server schnell und zuverlässig reagieren. Eine kontinuierliche personenbezogene Bewegungsverfolgung ist für diesen Zweck regelmäßig nicht erforderlich.

Zu Hause kann eine zeitgesteuerte Lichtszene den Morgen mit langsam steigender Helligkeit begleiten. Tageslichtabhängige Regelung ergänzt das natürliche Licht, während abends geringere Intensität und eine passende Lichtverteilung sinnvoll sein können. Solche Komfortfunktionen lassen sich mit Heizung oder Verschattung verbinden. Sie sind jedoch weder eine medizinische Behandlung noch ein Beleg für eine bestimmte Leistungssteigerung. Nutzer sollten Automatikfunktionen nachvollziehen, ändern und bei Bedarf manuell übersteuern können. [2]

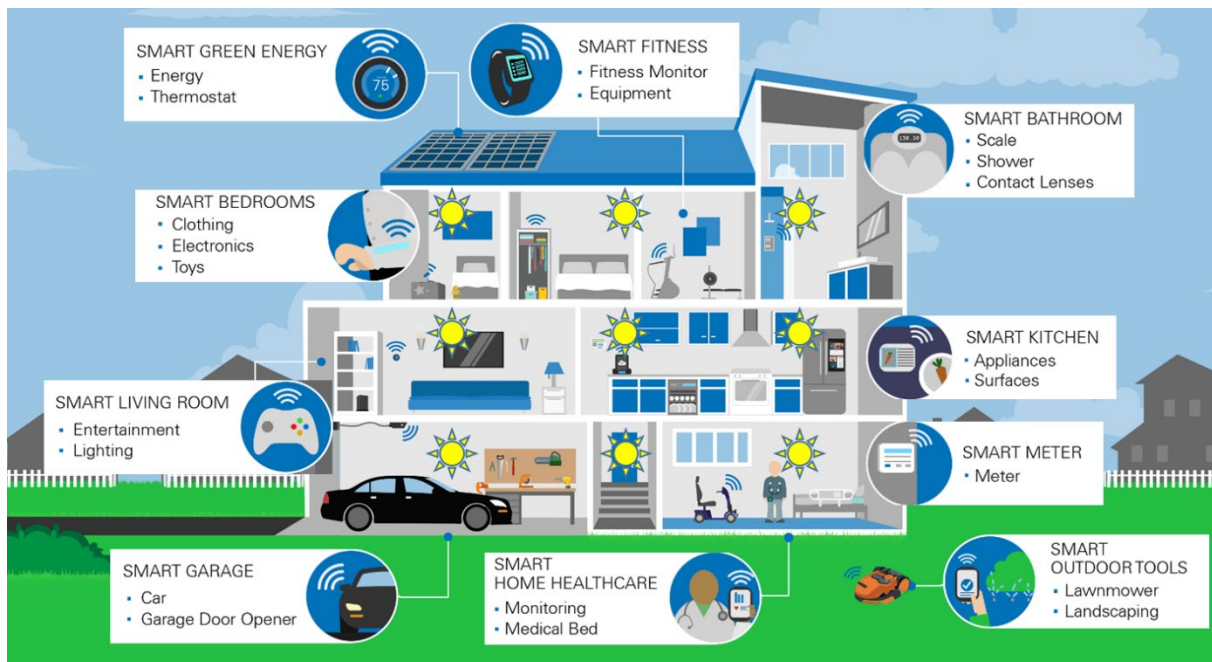


Abbildung 3: Illustration eines Smart Home. Die dargestellten Anwendungen sind Beispiele

Vernetzte Leuchten können lokal bedient und, soweit eingerichtet, aus der Ferne gesteuert werden. Internetdienste können beispielsweise Wetter- oder Verkehrsdaten für Automatisierungen liefern. Solche Zusatzfunktionen sollten bewusst aktiviert werden. Ihre Verfügbarkeit und die dafür benötigte Verarbeitung von Standort- oder Nutzungsdaten sind getrennt von der grundlegenden Beleuchtungsfunktion zu bewerten. [4–6]

Auch beim Einkaufen im Supermarkt oder im Einkaufs-Zentrum soll das Licht eine einladende Atmosphäre bieten. Die Lichtfarben sind auf die Warengruppen, wie Obst, Gemüse, Brot, Käse und Fleisch abgestimmt, damit die Waren attraktiv wirken. Das Licht kann aber noch mehr: Besonders im Einkaufszentren und großen Märkten wäre ein Navigationssystem auf dem Smartphone hilfreich, dass den eigenen Standort exakt kennt und einen zur gewünschten Ware führt. Das heißt „Lighting indoor positioning“. Jede Leuchte sendet mit dem Licht permanent einen individuellen Datenstrom aus, quasi die Adresse der Leuchte. Für das Auge ist diese Modulation des Lichtes nicht wahrnehmbar, aber für die Kameras im Smartphone. Eine App im Smartphone berechnet daraus, in Verbindung mit einem zentralen Server, jederzeit die eigene Position und zeigt sie auf einer Karte des Supermarktes auf dem Smartphone an. Gibt man ein, was man sucht, wird man zum Ziel navigiert.

Die Einsatzfelder reichen vom Wohnhaus über Büros und Produktionsstätten bis zur Straßenbeleuchtung. Für Außenanlagen zählen zusätzlich Lichtimmissionen, Umweltschutz und ein bedarfsgerechter Nachtbetrieb. Anwendungen im Straßenverkehr, in medizinischen Einrichtungen oder mit Sicherheitsfunktion unterliegen zusätzlichen Anforderungen und dürfen nicht allein nach Smart-Home-Kriterien ausgelegt werden.

5 Warum Datensicherheit?

Datensicherheit schützt Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen. Cybersecurity umfasst dabei auch den Schutz vor digitalen Angriffen und deren Folgen für reale Funktionen. Bei Smart Lighting reichen Risiken von gestohlenen Zugangsdaten und manipulierten Szenen bis zum Ausfall von Beleuchtung oder einem Einstieg in andere Gebäudenetze. IoT-Geräte können außerdem für verteilte Überlastungsangriffe (DDoS) missbraucht werden. Neben vorsätzlichen Angriffen müssen Fehlkonfigurationen, technische Defekte und der Ausfall von Diensten berücksichtigt werden. [6, 19]

Dass eine Leuchte nicht direkt mit dem Internet verbunden ist, macht sie nicht unangreifbar. Ein dokumentiertes Beispiel ist die 2020 veröffentlichte Schwachstelle CVE-2020-6007 der Philips Hue Bridge: Forschende zeigten einen Angriff über eine manipulierte ZigBee-Leuchte auf die Brücke. Der Hersteller stellte eine Korrektur bereit. Das Beispiel belegt einen konkreten Implementierungsfehler; es rechtfertigt weder die Aussage, ZigBee sei insgesamt unsicher, noch die Behauptung, alle früheren Lücken seien dauerhaft behoben. Funkzugang, Bridge und angeschlossenes IP-Netz sind gemeinsam zu betrachten. [20]

Weitere Angriffsflächen entstehen durch Apps, Cloud-Schnittstellen, Benutzerkonten, Router und Fernwartungszugänge. Automatisierte Angriffe suchen nach wiederverwendeten Kennwörtern, veralteter Software und erreichbaren Diensten. Auch kompromittierte Softwarekomponenten oder Update-Infrastrukturen können viele Anlagen gleichzeitig betreffen. Die Risikoanalyse muss daher das gesamte Ökosystem und seine Lieferkette erfassen. [6, 19, 21]

Vollständige Sicherheit gibt es nicht. Ein nachvollziehbares Schutzniveau entsteht aus vorbeugenden Maßnahmen, laufender Überwachung, einer geübten Reaktion auf Vorfälle und der Fähigkeit, einen sicheren Betrieb wiederherzustellen. Wie hoch der Aufwand sein muss, hängt auch von den Folgen eines Beleuchtungsausfalls ab. [6, 19]

6 Wie wird Datensicherheit erreicht?

Datensicherheit ist Teamwork. Hersteller, Planer und Installateure sowie Betreiber und Nutzer müssen ihre Aufgaben abstimmen. Ein sicher entwickeltes Produkt kann durch fehlerhafte Installation oder ausbleibende Updates unsicher werden. Gerade bei langlebiger Beleuchtung sind Wartung, Finanzierung des Supports und ein kontrollierter Austausch frühzeitig zu planen. Die folgende Tabelle zeigt, was die einzelnen Parteien dazu beitragen können.

Verantwortliche	Entwicklung und Planung	Markteinführung und Inbetriebnahme	Betrieb und Wartung
Hersteller	- Risiken analysieren; Datenbedarf begrenzen - Geräte, Schnittstellen und Updates sicher entwerfen - Softwarebestandteile und Supportdauer festlegen	- Gerät, App, Cloud und Updateverfahren prüfen - Befunde beheben; Konformität nachweisen - Support und Meldestelle transparent bereitstellen	- Schwachstellen bewerten; Sicherheitsupdates liefern - Vorfälle behandeln; CRA-Meldepflichten prüfen - Supportende und Migration rechtzeitig kommunizieren
Planer und Installateure	- Protokolle, Produkte und Supportzusagen prüfen - Netztrennung, Fernzugriff und Ausfallbetrieb planen - Zuständigkeiten und Datenflüsse festlegen	- Netze und Geräte absichern; individuelle Zugänge setzen - Funktionen und Wiederanlauf testen - Dokumentation und sichere Administration übergeben	- Updates kontrolliert installieren und prüfen - Konfiguration und Dokumentation pflegen - Supportende überwachen; Austausch vorbereiten
Betreiber und Nutzer	- Funktionen, Schutzbedarf und Datenbedarf festlegen - Lokalen Betrieb und Ausfallsicherheit verlangen - Budget und Verantwortung für Wartung vereinbaren	- Konten und Rechte prüfen; Mehrfaktorschutz nutzen* - Bediengeräte schützen; Notbetrieb erproben - Übergabe, Kontaktwege und Wartungsplan abstimmen	- Updates, Konten und Berechtigungen kontrollieren - Vorfälle erkennen; Meldewege klären - Bei Wechsel: Zugänge widerrufen, Daten löschen

Abbildung 4: Maßnahmen für Datensicherheit

6.1 Hersteller

Für Hersteller beginnt Cybersecurity beim Entwurf: Bedrohungen modellieren, Angriffsflächen begrenzen, individuelle Geräteidentitäten vorsehen und Schnittstellen absichern. Sichere Voreinstellungen, geschützte Schlüssel, authentifizierte Kommunikation und überprüfbare Updates gehören in die Architektur. ETSI EN 303 645 V3.1.3 (2024-09) bietet eine Basis für Verbraucher-IoT; NISTIR 8259A beschreibt grundlegende Gerätefähigkeiten. Für Apps und Webdienste helfen OWASP MASVS beziehungsweise ASVS. Diese Hilfen ersetzen keine gesetzliche Konformitätsbewertung. Art. 25 DSGVO adressiert die Verantwortlichen für die Verarbeitung; Hersteller müssen die Umsetzung technisch ermöglichen. Art. 32 verlangt risikogerechte Maßnahmen, nicht ausnahmslos dieselbe Verschlüsselungslösung. [4, 6, 19, 21]

Sicherheitsprüfungen sollten Gerät, Gateway, Apps, Schnittstellen und Cloud-Dienste umfassen. Penetrationstests ergänzen Codeprüfung, Abhängigkeitsanalyse und Tests der Update- und Wiederherstellungsfunktionen. Prüfziel, Systemgrenzen, Softwarestände und die Behebung der Befunde sind zu dokumentieren. Ein Test ist eine Momentaufnahme und muss nach wesentlichen Änderungen beziehungsweise neuen Bedrohungen angemessen wiederholt werden. [19, 21]

Zertifikate können geprüfte Eigenschaften transparent machen. Entscheidend sind jedoch Prüfgrundlage, Geltungsbereich, Produktversion und Gültigkeitsdauer. Ein freiwilliges Sicherheitszeichen ist keine pauschale Bestätigung vollständiger DSGVO-Konformität und ersetzt weder die EU-Konformitätserklärung noch die Pflichten des Betreibers. Für Apps und Cloud-Dienste muss erkennbar sein, ob und wie sie in die Prüfung einbezogen wurden.



Abbildung 5: Beispiel eines abgestimmten Penetrationstests. Ergänzend sind unter anderem Softwarelieferkette, Updates und Wiederherstellung zu prüfen.

Nach der Markteinführung bleiben Produktbeobachtung und die Behandlung sicherheitsrelevanter Fehler erforderlich. Produkthaftung ist von vertraglichen Updatepflichten und öffentlich-rechtlichen Sicherheitsanforderungen zu unterscheiden. Die neue Produkthaftungsrichtlinie (EU) 2024/2853 erfasst ausdrücklich auch Software; ihre Umsetzungsfrist endet am 9. Dezember 2026 und sie betrifft Produkte, die nach diesem Datum in Verkehr gebracht oder in Betrieb genommen werden. Sie ist zum Stichtag dieses Beitrags daher nicht als bereits vollständig anwendbares deutsches Haftungsregime darzustellen. [22]

Schwachstellen können durch interne Tests, unabhängige Forschung, Kundenmeldungen oder Warnungen zu eingebauten Komponenten bekannt werden. Hersteller benötigen eine erreichbare Meldestelle, eine koordinierte Offenlegung und einen geregelten Prozess zur Bewertung und Behebung. Eine gepflegte Übersicht der Softwarebestandteile erleichtert die Feststellung, welche Produkte von einer Schwachstelle in einer Bibliothek betroffen sind. [6, 19]

Schwachstellenmanagement und Vorfallreaktion gehören zusammen, sind aber unterschiedliche Aufgaben. Seit 11. September 2026 verlangt Art. 14 des Cyber Resilience Act (CRA) Meldungen über aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle: eine Frühwarnung binnen 24 Stunden und eine Meldung binnen 72 Stunden nach Kenntnis. Abschlussberichte folgen bei

Schwachstellen spätestens 14 Tage nach Verfügbarkeit einer Abhilfemaßnahme, bei schwerwiegenden Vorfällen binnen eines Monats nach der 72-Stunden-Meldung. Gemeldet wird über die zentrale Plattform an den zuständigen CSIRT-Koordinator und ENISA. Diese Pflicht erfasst auch einschlägige Produkte, die bereits vor Dezember 2027 in Verkehr gebracht wurden. [17]

Die zentralen Produkt- und Lebenszyklusplichten des CRA gelten grundsätzlich ab 11. Dezember 2027. Der Unterstützungszeitraum richtet sich nach der erwarteten Nutzungsdauer und beträgt grundsätzlich mindestens fünf Jahre, außer bei kürzerer erwarteter Nutzung. Fünf Jahre sind damit keine pauschale Obergrenze für langlebige Leuchten. Sicherheitsupdates müssen während dieses Zeitraums bereitgestellt werden. Schon heute bestehen im Verbrauchervertragsrecht Aktualisierungspflichten, insbesondere nach §§ 475b, 475c beziehungsweise 327f BGB; diese treffen je nach Vertrag Verkäufer oder Anbieter digitaler Produkte und sind von den Herstellerpflichten des CRA zu trennen. [18, 23]

6.2 Planer und Installateur

Die Planung von Smart Lighting erfolgt häufig gemeinsam mit weiteren Gebäudefunktionen. Neben Funktionalität und Kosten müssen Ausfallsicherheit, Wartung, Datenschutz und Cybersecurity als Anforderungen festgelegt werden. Dazu gehören der Betrieb ohne Internet, eine lokale Bedienmöglichkeit und Verantwortlichkeiten für die gesamte Nutzungsdauer.

Die Technologieauswahl beginnt mit Anforderungen an Reichweite, Zuverlässigkeit, Reaktionszeit, Gerätezahlen und Integration. Weniger Schnittstellen können die Wartung vereinfachen, doch ein einziges Funkprotokoll ist kein allgemeines Sicherheitsrezept. Getrennte Netze und gezielt abgesicherte Übergänge können Risiken reduzieren. Zu prüfen sind konkrete Produktzertifizierungen und gemeinsame Funktionen, nicht nur Protokollnamen oder Versionsnummern. [3, 7, 9–12]

Bei der Herstellerwahl zählen nachprüfbar Zusagen: veröffentlichter Supportzeitraum, Verfahren für Sicherheitsmeldungen, Updatefunktion, lokale Betriebsfähigkeit, Datenexport und ein Vorgehen bei Dienstende. Auch ein bekannter Markenname ersetzt diese Prüfung nicht. Für langlebige Anlagen sind Ersatzgeräte, Übernahme von Konfigurationen und die Folgen eines Anbieterwechsels einzukalkulieren. [6, 18, 19]

Was im Schiffbau die Schotten sind, sind im Datennetz kontrollierte Segmente. Beleuchtungs- und sonstige Gebäudenetze sollten nach Schutzbedarf von Büro-IT und Gastzugängen getrennt werden. Der Austausch erfolgt über ausdrücklich erlaubte Verbindungen, etwa mit VLANs und Firewall-Regeln. Andere IP-Adressen oder Funk-Domainnamen allein schaffen keine wirksame Segmentierung; auch ein VPN ersetzt keine Zugriffskontrolle. Bei Matter und Thread müssen erforderliche IPv6- und Diensterkennungsfunktionen gezielt berücksichtigt werden. [7, 9, 19]

Zur physischen Sicherheit gehören geschützte Verteiler, Gateways und Netzwerkanschlüsse sowie angemessener Schutz öffentlich erreichbarer Geräte. Wartungs- und Debug-Schnittstellen dürfen keine einfache Umgehung der Authentisierung ermöglichen. Für Außenanlagen sind zusätzlich Umgebungsbedingungen und Manipulationsrisiken zu berücksichtigen. Eine anschauliche Anekdote ersetzt keine dokumentierte Risikoanalyse. [19]

Router und Fernzugriffe sind restriktiv zu konfigurieren. Unnötige Portfreigaben und von außen erreichbare Verwaltungsoberflächen sind zu vermeiden; automatische Freigaben sind zu prüfen. Erforderliche Fernwartung sollte über einen abgesicherten Zugang mit starker Authentisierung, begrenzten Rechten und Protokollierung erfolgen. Auch Verbindungen, die ein Gerät selbst zu einer Cloud aufbaut, benötigen eine Sicherheitsbewertung. [6, 19]

Bei der Installation sind individuelle Zugangsdaten und, soweit unterstützt, Multifaktor-Authentisierung für Administrator- und Cloud-Konten einzurichten. Wiederverwendete Installateur Kennwörter sind ungeeignet. Temporäre Zugänge müssen bei der Übergabe entfernt oder eindeutig geregelt werden. Schlüssel und Wiederherstellungscodes gehören in eine geschützte Verwaltung. [6, 19]

Eine belastbare Dokumentation enthält Gerätebestand, Firmwarestände, Netzstruktur, freigegebene Datenflüsse, Zuständigkeiten und Wiederherstellungsverfahren. Passwörter und Schlüssel sollten getrennt in einer geeigneten geschützten Ablage verwaltet werden. Die Übergabe muss sicherstellen, dass der Betreiber seine Anlage administrieren kann und nicht dauerhaft von einem einzelnen Installateur Konto abhängig bleibt. [19]

Wartung umfasst Elektronik, Sensorik und Software. Updates benötigen geeignete Wartungsfenster, Funktionsprüfungen und ein Wiederherstellungsverfahren. Das Supportende ist rechtzeitig zu überwachen. Wenn ein Produkt keine Sicherheitskorrekturen mehr erhält, sind Ersatz, kontrollierte Isolation oder Außerbetriebnahme zu bewerten. Vor einem Austausch müssen Konfiguration und notwendige Daten gesichert sowie alte Zugänge und personenbezogene Daten entfernt werden. [6, 19]

6.3 Betreiber und Nutzer

Betreiber und Nutzer sollten bereits bei der Beschaffung festlegen, welche Funktionen benötigt werden und welche Daten dafür erforderlich sind. Lokaler Betrieb kann die Abhängigkeit von Cloud-Diensten und bestimmte Angriffsflächen reduzieren. Er beseitigt jedoch weder Funkangriffe noch unsichere Apps oder Risiken im lokalen Netz. Für wichtige Beleuchtungsfunktionen empfiehlt sich ein praktisch getesteter Betrieb bei Ausfall von Internet und Zentrale.

Benutzerkonten erhalten nur die für ihre Aufgabe nötigen Rechte. Administrationsrechte sollten getrennt von der täglichen Bedienung eingesetzt werden, soweit das System dies ermöglicht. Einzigartige Kennwörter, Mehrfaktor-Authentisierung und geschützte, aktuell gehaltene Smartphones reduzieren das Risiko eines Kontomissbrauchs. Geteilte Administratorzugänge erschweren die Nachvollziehbarkeit und sollten vermieden werden. [6, 19]

Der sichere Betrieb erfordert zeitnahe **Updates** und eine Kontrolle, ob sie tatsächlich installiert wurden. Automatische Sicherheitsupdates sind sinnvoll, wenn das System sie zuverlässig unterstützt; bei betriebskritischen Anlagen sind abgestimmte Test- und Freigabeprozesse erforderlich. Auffällige Netzaktivität oder unbekannte Geräte sind Hinweise, aber weder ein sicherer Angriffsnachweis noch ein Ersatz für Überwachung. Für Störungen sind Zuständigkeiten, Kontaktwege und Wiederanlaufverfahren festzulegen. [6, 19]

Konten und Berechtigungen sind regelmäßig zu überprüfen. Beim Ausscheiden von Beschäftigten, Wechsel eines Dienstleisters oder Verkauf eines Geräts müssen Zugänge widerrufen und gegebenenfalls Schlüssel erneuert werden. Für Einrichtungen im Anwendungsbereich des deutschen NIS-2-Umsetzungsgesetzes bestehen seit 6. Dezember 2025 zusätzliche Pflichten. Ob sie greifen, richtet sich nach Einrichtung, Sektor und weiteren gesetzlichen Kriterien, nicht allein nach dem Einsatz smarter Leuchten. [24]

Die Dokumentation muss mit der Anlage fortgeschrieben werden. Dazu gehören Änderungen an Konfiguration, Datenflüssen, Dienstleistern und Supportfristen. Bei einem Sicherheitsvorfall sind neben technischen Maßnahmen die jeweils einschlägigen Meldewege zu prüfen. Für Verletzungen des Schutzes personenbezogener Daten gelten eigenständige Regeln nach Art. 33 und 34 DSGVO; die Behördenmeldung ist grundsätzlich binnen 72 Stunden nach Bekanntwerden erforderlich, sofern ein Risiko für Betroffene nicht unwahrscheinlich ist. [4, 5]

7 Warum Datenschutz?

Smart Lighting kann personenbezogene Daten erzeugen, muss dafür aber nicht zwingend Namen erfassen. Nutzungszeiten, Raumzuordnung und Gerätekennungen können in Verbindung mit weiteren Informationen Rückschlüsse auf einzelne Personen erlauben. Je nach System kann ein Anbieter solche Daten erhalten; bei lokaler Verarbeitung ist dies nicht zwangsläufig der Fall. Zu prüfen sind tatsächliche Datenflüsse statt der Annahme, der Hersteller kenne jederzeit jeden Lichtzustand. [4, 5]

Mit weiteren Quellen verknüpfte Nutzungsdaten können aussagekräftige Verhaltensprofile ergeben. Die im Original beschriebene Erkennung einer konkreten Fernsehsendung aus Stromdaten ist jedoch keine allgemeine Eigenschaft üblicher Smart Meter; sie hängt unter anderem von Messauflösung und Referenzdaten ab. Für die Datenschutzbewertung genügt bereits das realistische Risiko, Anwesenheit, Tagesrhythmus oder Nutzungsgewohnheiten abzuleiten. Pseudonyme Kennungen sind dabei nicht automatisch anonym. [4, 5]

Am Arbeitsplatz kann schon die Verbindung einer Raumbellegung mit Arbeitsplänen Personen identifizierbar machen. Beschäftigtendaten erfordern eine tragfähige Rechtsgrundlage und eine Prüfung der Erforderlichkeit, insbesondere nach § 26 BDSG in Verbindung mit der DSGVO. Bei zur Verhaltens- oder Leistungskontrolle bestimmten technischen Einrichtungen ist die Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG zu beachten. Eine Betriebsvereinbarung ersetzt weder Verhältnismäßigkeit noch technische Schutzmaßnahmen. Eine Einwilligung ist wegen des Abhängigkeitsverhältnisses nicht ohne Weiteres freiwillig. [25]

Auch eine Navigations-App im Geschäft kann Standortdaten mit einem Konto oder einer Gerätekennung verbinden. Bargeldzahlung verhindert diese Verknüpfung nicht automatisch. Umgekehrt beweisen Bewegungsdaten allein weder einen tatsächlichen Kauf noch sämtliche Interessen einer Person. Standortübermittlung, Analysezwecke und Speicherdauer müssen transparent sein; für optionale Analysen ist eine eigene rechtliche Bewertung notwendig. [4, 5]

8 Wie wird Datenschutz erreicht?

Während bei der Datensicherheit Anbieter und Nutzer an einem Strang ziehen - beide wollen keine Hacker - gibt es beim Datenschutz einen natürlichen Interessengegensatz. Der Anbieter möchte alles über seinen Kunden wissen und die Daten monetarisieren. Der Nutzer möchte seine Privatsphäre behalten. Wenn es einen Interessengegensatz gibt, müssen Gesetze her, die dies regeln. Dies ist hier die neue Datenschutzgrundverordnung (DSGVO).. Die DSGVO ist ein Verbraucherschutzgesetz. Sie räumt dem Verbraucher Rechte ein und legt dem Unternehmen Pflichten auf. Welche das im Wesentlichen sind, zeigt die folgende Abbildung.

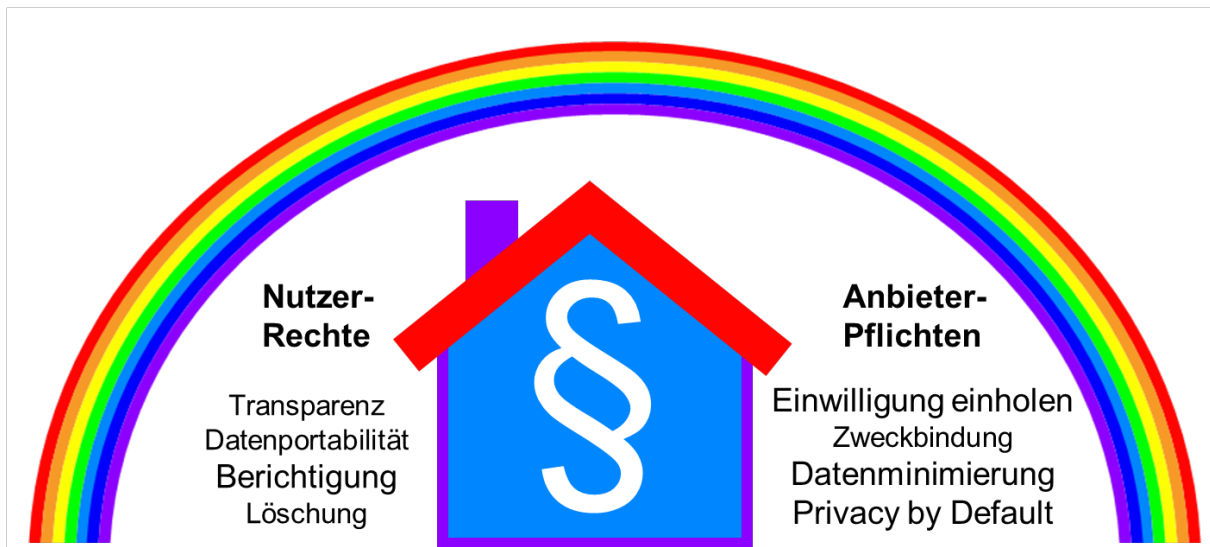


Abbildung 6: Datenschutz als Schutzrahmen. Maßgeblich sind die im Text erläuterten Betroffenenrechte und Pflichten der Verantwortlichen.

Transparenz bedeutet verständliche Informationen über Verantwortliche, Zwecke, Rechtsgrundlagen, Empfänger, Speicherdauer und Betroffenenrechte. Diese gehören in eine Datenschutzerklärung beziehungsweise in passende Hinweise am Einsatzort. Eine EULA ist ein Lizenzvertrag und ersetzt solche Informationen nicht. Bei Cloud-Diensten sind die Rollen als Verantwortlicher oder Auftragsverarbeiter, notwendige Verträge und mögliche Drittlandübermittlungen zu klären. [4, 5]

Das Auskunftsrecht nach Art. 15 DSGVO ist vom Recht auf Datenübertragbarkeit nach Art. 20 zu unterscheiden. Letzteres betrifft unter seinen Voraussetzungen bereitgestellte personenbezogene Daten bei automatisierter Verarbeitung auf Grundlage von Einwilligung oder Vertrag. Es verlangt ein strukturiertes, gängiges und maschinenlesbares Format. Nicht alle intern abgeleiteten Profile fallen darunter. Betroffene müssen ihre Rechte ohne unnötige Hürden ausüben können. [5]

Berichtigung, Löschung, Einschränkung und Widerspruch haben jeweils eigene Voraussetzungen und Grenzen. Eine Löschung kann beispielsweise gesetzlichen Aufbewahrungspflichten entgegenstehen. Anträge sind grundsätzlich unverzüglich, spätestens binnen eines Monats zu beantworten; bei zulässiger Verlängerung ist innerhalb dieser Frist darüber zu informieren. Empfänger sind bei Berichtigung, Löschung oder Einschränkung nach den gesetzlichen Voraussetzungen einzubeziehen. [5]

Jeder Verarbeitungszweck benötigt eine passende Rechtsgrundlage. Einwilligung ist eine Möglichkeit, aber nicht die einzige; sie muss freiwillig, informiert, bestimmt und widerruflich sein. Technisch notwendige Lichtsteuerung und optionale Werbung oder Profilbildung sind getrennt zu bewerten. Die Nutzung einer Anlage erlaubt nicht automatisch jede weitere Analyse. Für das Speichern oder Auslesen von Informationen auf Endgeräten ist zusätzlich § 25 TDDDG zu prüfen; auch dort bestehen eng gefasste Ausnahmen, etwa für unbedingt erforderliche Vorgänge eines ausdrücklich gewünschten Dienstes. [4, 5, 26]

Datensparsame Gestaltung beginnt bei der Sensorwahl. Wo ein Präsenzsignal genügt, sollten keine identifizierenden Bild- oder Bewegungsdaten dauerhaft gespeichert werden. Lokale Auswertung, kurze Löschrufen, Zugriffsbeschränkungen und ausreichend grobe Aggregation können Risiken senken. Bei voraussichtlich hohem Risiko ist vorab eine Datenschutz-Folgenabschätzung erforderlich. Ein bloßes Entfernen von Namen bewirkt noch keine Anonymisierung. [5]

Datenschutzfreundliche Voreinstellungen begrenzen Erhebung, Speicherung und Zugänglichkeit auf das Erforderliche. Optionale, einwilligungsbedürftige Analysen dürfen nicht vorausgewählt sein. Hinzu kommt der Data Act: Er gilt grundsätzlich seit 12. September 2025 und stärkt den Zugang zu Daten vernetzter Produkte. Die Gestaltungspflicht aus Art. 3 Abs. 1 betrifft Produkte und zugehörige Dienste, die nach dem 12. September 2026 in Verkehr gebracht werden. Sie verlangt zugängliche Daten und relevante Metadaten, soweit einschlägig auch unmittelbaren Zugriff. Der Data Act ersetzt weder die DSGVO noch eine erforderliche Rechtsgrundlage für personenbezogene Daten. [5, 27]

9 Was bringt die Zukunft?

Die Zukunft liegt weniger in möglichst vielen verbundenen Geräten als in interoperablen, wartbaren und bedarfsgerecht betriebenen Anlagen. Matter erleichtert die Integration im Smart Home; DALI-2/D4i und weitere Gebäudeprotokolle bleiben für professionelle Anwendungen relevant. Die frühere Prognose von 500 IoT-Geräten je Haushalt und die Behauptung, Smart Lighting sei 2022 bereits die Regel, werden nicht als Tatsachen fortgeführt. Künstliche Intelligenz kann Regelung und Wartung unterstützen, muss aber nach messbarem Nutzen, Zuverlässigkeit und Datenbedarf beurteilt werden. Eine Cloud ist dafür nicht in jedem Fall nötig. [3, 9]

Mit der Vernetzung wachsen die Anforderungen an den gesamten Lebenszyklus. Zum Stand September 2026 greifen bereits CRA-Meldepflichten und die neue Data-Act-Gestaltungspflicht für neu in Verkehr gebrachte Produkte; zentrale CRA-Produktpflichten folgen im Dezember 2027. Die 2018 erwartete ePrivacy-Verordnung ist nicht wie angekündigt in Kraft getreten: Der damalige Vorschlag wurde 2025 zurückgezogen. Maßgeblich bleiben die geltenden Datenschutz- und Kommunikationsregeln. Für verlässliches Smart Lighting sind damit lokale Grundfunktionen, klare Datenverantwortung, überprüfbare Updatezusagen und planbare Migration entscheidend. [17, 18, 26–28]

10 Quellenverzeichnis

Quellenstand und Abruf: 17.09.2026.

- [1] Europäische Kommission: Light Sources. Ökodesign, Energielabel und EPREL; Verordnungen (EU) 2019/2020 und 2019/2015. https://energy-efficient-products.ec.europa.eu/product-list/light-sources_en
- [2] CIE: Position Statement on Integrative Lighting, CIE PS 001:2024, 3. Auflage; mit Bezug auf CIE S 026:2018. DOI 10.25039/PS.b2twa77g. <https://www.cie.co.at/publications/cie-position-statement-integrative-lighting-recommending-proper-light-proper-time-3rd>
- [3] DALI Alliance: D4i overview; Überblick zu DALI-2, D4i und DALI+. <https://www.dali-alliance.org/d4i> | <https://www.dali-alliance.org/>
- [4] Europäische Union: Verordnung (EU) 2016/679 (DSGVO), insbesondere Art. 2, 5, 6, 12–22, 25, 28, 32–35 und 44 ff. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [5] Europäischer Datenschutzausschuss (EDPB): Data protection guide for small business; Grundlagen, Betroffenenrechte, Compliance und Datenschutz durch Technikgestaltung. https://www.edpb.europa.eu/sme/learn-the-basics/data-protection-basics_en | https://www.edpb.europa.eu/sme/be-compliant/respect-individuals-rights_en | https://www.edpb.europa.eu/sme/be-compliant/be-compliant_en
- [6] ETSI: EN 303 645 V3.1.3 (2024-09), Cyber Security for Consumer Internet of Things: Baseline Requirements. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
- [7] Thread Group: Thread 1.4 Paves The Path For Smart Devices To Work Together, 04.09.2024; Resources und Erläuterungen zum Border Router. <https://threadgroup.org/Newsroom/Blog/thread-14-paves-the-path-for-smart-devices-to-work-together-regardless-of-their-ecosystem-or-manufacturer> | <https://threadgroup.org/resources>
- [8] DIN Media: DIN EN IEC 60598-1:2022-03, Leuchten – Allgemeine Anforderungen und Prüfungen; mit A11:2023-01 und Berichtigung 1:2023-07. <https://www.dinmedia.de/de/norm/din-en-iec-60598-1/345804740>
- [9] Connectivity Standards Alliance: Matter FAQs; Matter 1.6 Enables More Intuitive Setup, Multi-Ecosystem Experiences, and Context-Driven Control, 17.06.2026. <https://csa-iot.org/all-solutions/matter/matter-faq/> | <https://csa-iot.org/newsroom/matter-1-6-enables-more-intuitive-setup-multi-ecosystem-experiences-and-context-driven-control/>
- [10] Connectivity Standards Alliance: The Connectivity Standards Alliance Announces Zigbee 4.0 and Suzi, 18.11.2025. <https://csa-iot.org/newsroom/the-connectivity-standards-alliance-announces-zigbee-4-0-and-suzi-empowering-the-next-generation-of-secure-interoperable-iot-devices/>
- [11] Bluetooth SIG: Mesh Protocol 1.1; Bluetooth Mesh Feature Enhancements Summary, 19.09.2023. <https://www.bluetooth.com/specifications/specs/mesh-protocol/> | <https://www.bluetooth.com/mesh-feature-enhancements-summary/>
- [12] Z-Wave Alliance: Z-Wave Long Range; Technical News, Zertifizierungsstand 06.05.2025 zu EU Long Range. <https://z-wavealliance.org/z-wave-long-range-technology/> | <https://z-wavealliance.org/zwa-certification-news/>
- [13] BAuA: ASR A3.4 Beleuchtung und Sichtverbindung, Mai 2023. DIN Media: DIN EN 12464-1:2021-11, Arbeitsstätten in Innenräumen. <https://www.baua.de/DE/Angebote/Regelwerk/ASR/ASR-A3-4> | <https://www.dinmedia.de/en/standard/din-en-12464-1/334047306>
- [14] Europäische Kommission: Radio Equipment Directive (RED), Rechtsgrundlagen und Übergang der Cybersecurity-Anforderungen; Richtlinie 2014/53/EU und Delegierte Verordnung (EU) 2022/30. https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en

- [15] Europäische Kommission: Durchführungsbeschluss (EU) 2025/138, Harmonisierung der EN 18031-1/-2/-3:2024 mit Einschränkungen. https://eur-lex.europa.eu/eli/dec_impl/2025/138/oj
- [16] Europäische Kommission: Delegierte Verordnung (EU) 2026/339 vom 16.02.2026 zur Aufhebung von (EU) 2022/30 mit Wirkung ab 11.12.2027. https://eur-lex.europa.eu/eli/reg_del/2026/339/oj
- [17] Europäische Kommission: Cyber Resilience Act – Reporting obligations; Umsetzung von Art. 14 der Verordnung (EU) 2024/2847. <https://digital-strategy.ec.europa.eu/en/policies/cra-reporting>
- [18] Europäische Union: Verordnung (EU) 2024/2847 (Cyber Resilience Act), insbesondere Art. 13, 14, 69 und 71. Kommission: Summary of the legislative text; Implementation, Stand 27.07.2026. <https://eur-lex.europa.eu/eli/reg/2024/2847/oj> | <https://digital-strategy.ec.europa.eu/en/policies/cra-summary> | <https://digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation>
- [19] NIST: NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline, Mai 2020; ergänzender Online-Katalog technischer und organisatorischer Herstellerfähigkeiten. <https://csrc.nist.gov/pubs/ir/8259/a/final> | <https://pages.nist.gov/IoT-Device-Cybersecurity-Requirement-Catalogs/>
- [20] Check Point Research: Don't be silly – it's only a lightbulb, 2020. Technischer Forschungsbericht zur Hue-Bridge-Schwachstelle CVE-2020-6007; historischer Nachweis. <https://research.checkpoint.com/2020/dont-be-silly-its-only-a-lightbulb/>
- [21] OWASP: Mobile Application Security Verification Standard (MASVS) und Application Security Verification Standard (ASVS 5.0.0). <https://mas.owasp.org/MASVS/> | <https://owasp.org/projects/asvs>
- [22] Europäische Union: Richtlinie (EU) 2024/2853 über die Haftung für fehlerhafte Produkte, insbesondere Art. 2, 21 und 22. <https://eur-lex.europa.eu/eli/dir/2024/2853/oj>
- [23] Bundesministerium der Justiz / Bundesamt für Justiz: BGB, §§ 327f, 475b und 475c, Aktualisierungspflichten bei digitalen Produkten und Waren mit digitalen Elementen. <https://www.gesetze-im-internet.de/bgb/>
- [24] Bundesamt für Sicherheit in der Informationstechnik: Informationen zu NIS-2 und zur Registrierung; Inkrafttreten des deutschen Umsetzungsgesetzes am 06.12.2025. <https://mip2.bsi.bund.de/de/info-nis2-registrierung/>
- [25] Bundesministerium der Justiz / Bundesamt für Justiz: BDSG, insbesondere § 26; BetrVG, § 87 Abs. 1 Nr. 6. https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html | https://www.gesetze-im-internet.de/betrvg/_87.html
- [26] Bundesministerium der Justiz / Bundesamt für Justiz: TDDDG, insbesondere § 25 zum Schutz der Privatsphäre bei Endeinrichtungen. <https://www.gesetze-im-internet.de/ttdsg/BJNR198210021.html>
- [27] Europäische Union: Verordnung (EU) 2023/2854 (Data Act), insbesondere Art. 1, 3–5 und 50. Europäische Kommission: Data Act explained. <https://eur-lex.europa.eu/eli/reg/2023/2854/oj> | <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained>
- [28] EUR-Lex: Gesetzgebungsverfahren 2017/0003(COD), Vorschlag einer ePrivacy-Verordnung; Rücknahme durch die Kommission am 06.10.2025. https://eur-lex.europa.eu/procedure/EN/2017_3
- [29] Europäische Kommission: Informationen zur General Product Safety Regulation, Verordnung (EU) 2023/988, anwendbar seit 13.12.2024. https://commission.europa.eu/topics/business-and-industry/product-safety_en | <https://eur-lex.europa.eu/eli/reg/2023/988/oj>