



Transparente Kommunikation



Ein offener Austausch zwischen allen Beteiligten über die Ziele der Techniknutzung.
Transparenz darüber, welche Daten wo erhoben werden, schafft Vertrauen und gemeinsame Verantwortung.





Checklisten



Strukturierte Übersichten zur technischen Überprüfung (Welche Sensoren senden wohin?) sowie zur Reflexion des persönlichen und gemeinschaftlichen Umgangs mit Daten. Sie helfen, Risiken sichtbar zu machen.





Konsens-Protokoll

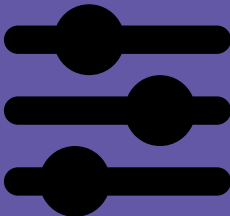


Eine (schriftliche) Vereinbarung, die festhält, welche Technik an welchem Ort installiert wird und welchen Aktivitäten die Stakeholder zugestimmt haben, um Privatsphäre verbindlich auszuhandeln.





Richtige Einstellungen



Die gezielte Konfiguration von Geräten, um die Datenerfassung auf das absolut notwendige Minimum zu beschränken und den Schutz der Privatsphäre technisch zu erzwingen.





Daten löschen

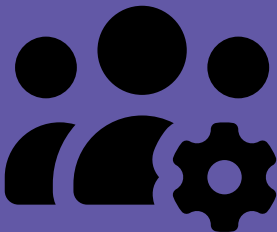


Das regelmäßige und bewusste Entfernen nicht mehr benötigter Daten, um das Risiko einer missbräuchlichen Einsichtnahme oder Zweckentfremdung zu minimieren.





Zusätzlicher Admin Account



Es sollten mehrere administrative Accounts für jedes Gerät eingerichtet werden, welches von mehreren Haushaltsmitgliedern benutzt und nicht ausschließlich für den persönlichen Gebrauch verwendet wird.





Nutzung eines Gast-WLAN



Mit einem separaten Gast-Netzwerk können Geräte von Gästen von anderen, persönlichen Geräten oder Smart Devices getrennt werden, auf denen sensible Dienste wie Onlinebanking oder HomeofficeAnwendungen genutzt werden bzw. persönliche Daten geteilt werden. Gleiches gilt für IoT-Geräte die sich in einem seperatem IoT-WLAN befinden sollten.





Komfort



Die Erleichterung des Alltags
durch automatisierte Abläufe,
personalisierte Einstellungen
und eine vereinfachte
Bedienung der Haustechnik.





Sicherheit



Der Schutz vor Einbrüchen, technischen Defekten oder gesundheitlichen Risiken durch vernetzte Warnsysteme und Überwachung.





Effizienz



Die Einsparung von Energie und Ressourcen durch präzise Datenerfassung und automatisierte Steuerung, was zu nachhaltigerem Verbrauch und geringeren Kosten führen kann.





Digitale Gewalt

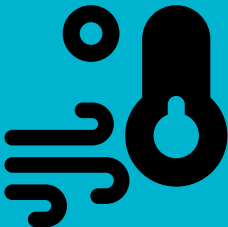


Nutzung technischer Systeme zur Überwachung, Kontrolle, Einschüchterung oder Erpressung von Personen. Dies kann zu psychischem Druck und einem massiven Verlust des Sicherheitsgefühls führen und (Cyber-)Stalking und andere Straftaten ermöglichen.





Raumklima-Daten



Messwerte zu Temperatur, Luftfeuchtigkeit oder CO₂-Gehalt der Luft. Diese wirken harmlos, geben aber detaillierte Einblicke in die Raumnutzung und ermöglichen Rückschlüsse auf Anwesenheit und Gewohnheiten.





Bewegungsmelder- Daten



Informationen über
Bewegungen im Haus / in der
Wohnung.





Andere einfache Sensordaten



Grundlegende Messwerte wie Lichteinfall, Geräuschpegel oder der Status von Türen und Fenstern (offen/zu). Diese Daten können die Anzahl der Personen im Haushalt und deren Aktivitäten präzise abbilden.





Haustiere



Tiere im Haushalt, die durch ihre Anwesenheit Sensoren (z. B. Bewegungsmelder) auslösen. Dies erzeugt indirekt Daten, die Rückschlüsse auf z.B. Fütterungszeiten oder Aktivitätsmuster zulassen.





Nachbarn



Personen in unmittelbarer räumlicher Nähe, die Informationen aus dem Haushalt (z. B. WLAN-Signale, Geräusche) wahrnehmen oder durch vernetzte Geräte (z. B. Außenkameras) beeinflusst werden können.





Dienstleister



Externe Fachkräfte, die die Wohnung regelmäßig oder zeitlich begrenzt besuchen (z.B. Pflegekräfte). Sie kommen potenziell mit den installierten Systemen oder deren Datenerhebung in Berührung.





Hausmeister



Zuständig für die
Gebäudebetreuung mit
regelmäßigem Zugang zu
technischen Anlagen und
Gemeinschaftsbereichen.
Dadurch können sie indirekt mit
Smart-Home-Daten in Kontakt
kommen.





Verwandtschaft



Familienmitglieder, die zeitweise
zu Besuch sind.





Vermieter



Eigentümer der Wohnräume, die ein berechtigtes Interesse am Zustand der Immobilie haben.
Sie können in bestimmten Situationen Einblick in technische Systeme erhalten.





Mitbewohner



Personen, die den Wohnraum teilen (oft ohne Verwandtschaftsverhältnis), die Geräte mitnutzen und dadurch sowohl aktiv Daten erzeugen als auch passiv von der Überwachung betroffen sind.





Kleinkinder

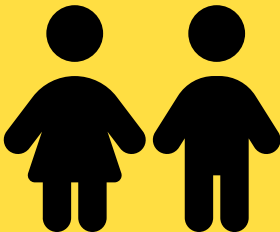


Sehr junge Kinder bei denen Eltern ein berechtigtes Interesse haben diese zu ihrem eigenen Wohle zu überwachen.
Erwachsene müssen hier stellvertretend über deren Privatsphäre entscheiden.





Kinder



Minderjährige Haushaltsmitglieder oder deren Freunde, die mit der Technik aufwachsen. Sie sind besonders schutzbedürftig, da sie oft nicht verstehen, welche Daten im Hintergrund gesammelt werden oder welche Tragweite ihr Handeln hat. Erwachsene müssen hier stellvertretend über deren Privatsphäre entscheiden.





Eltern



Sie sorgen für den Lebensunterhalt von Minderjährigen und sind für die Einrichtung der Wohnung samt Technik zuständig. Als Verantwortliche für Sicherheit und Wohlbefinden treffen sie zentrale Entscheidungen über die Datenverarbeitung im Haushalt.





Heimadministratoren



Diese Personen tragen die technische Verantwortung, konfigurieren die Systeme und führen Wartungsarbeiten durch. Sie besitzen dadurch einen umfassenden Zugriff auf alle gesammelten Daten und technischen Einstellungen.





Partner



Eine Person, die in einer festen, oft intimen Beziehung mit einer anderen Person steht und im selben Haushalt lebt. Mit dieser Person werden oft die vertraulichsten Dinge geteilt.





Senioren



Senior bezeichnet einen älteren Menschen, beispielsweise im Rentenalter oder Ruheständler der z.b. im selben Haushalt wohnt und auf ggf. auf Zuwendung angewiesen ist. Der Einsatz smarter Technik soll sie dabei ebenfalls unterstützen.

