



Forschung für
energieoptimierte
Gebäude und Quartiere



Universität der Künste Berlin

Berlin Career College



Effiziente Datenminimierung im Gebäude- und Quartierssektor

Wissenschaftliche Begleitforschung
Energiewendebauen: Modul 4 Digitalisierung
Stand: Juni 2022

EFFIZIENTE DATENMINIMIERUNG IM GEBÄUDE- UND QUARTIERSEKTOR

von Valentin Rupp, Julie Heumüller,
Maximilian von Grafenstein

Einleitung

Beim Einsatz digitaler Anwendungen im Gebäude- und Quartierssektor lassen in diesem Rahmen verarbeitete Datensätze zu Raumklima, Energieverbrauch und sonstigen gebäudebezogenen Daten häufig Rückschlüsse auf das Verhalten von Einzelpersonen oder Personengruppen zu. Beziehen sich diese Daten auf eine identifizierte oder identifizierbare Person, findet das nationale bzw. europäische Datenschutzrecht Anwendung und mit ihm die gesamte Bandbreite rechtlicher Verpflichtungen des Verantwortlichen. Ziel des Datenschutzrechts ist es dabei, die Betroffenen vor Risiken zu schützen, die durch die Datenverarbeitung verursacht werden und ihnen damit grundsätzlich die Entscheidung über das Maß und dem Umgang mit diesen Risiken zu gewähren.

Da das Datenschutzrecht dies an den sehr unbestimmten Begriff des personenbezogenen Datums knüpft, ist bei vielen Anwendungen dabei nicht von vornherein absehbar, welche tatsächlichen und rechtlichen Folgen im konkreten Fall an eine Verarbeitung der Daten geknüpft sind. Die vorliegende Visualisierung soll daher der Erläuterung dienen, wie anhand einer Berücksichtigung von Risiken für Betroffene der Personenbezug von Daten ermittelt und durch den Einsatz technisch-organisatorischer Maßnahmen möglichst weitgehend minimiert werden kann. Auf diese Weise wird einerseits der rechtlichen Verpflichtung eines effektiven Schutzes von Betroffenen Rechnung getragen. Andererseits können digitale Anwendungen mit einer höheren Rechts- und damit Planungssicherheit betrieben werden.

Datenkategorien, Verarbeitungszwecke und Kontext der Verarbeitung

Die Frage des Personenbezugs lässt sich anhand mehrerer Faktoren bestimmen, wobei ein naheliegender Anknüpfungspunkt die Art der verarbeiteten Daten ist. Ein eindeutiges Beispiel ist etwa das Sammeln von Eigenschaften und Verhaltensweisen einer Person: die Adresse auf dem Per-

sonalausweis ist deshalb ein personenbezogenes Datum, da sie schon ihrem Inhalt nach Informationen über die dort ausgewiesene Person enthält, nämlich den aktuellen Wohnort der Person (unabhängig davon, ob die Information stimmt oder nicht). Auch bei Energieverbrauchsdaten auf einer Stromabrechnung eines Einpersonenhaushaltes ist diese Logik nachvollziehbar, da hier der Energieverbrauch klar einer Einzelperson zugewiesen werden kann. Da die Kombination von Name und Adresse auf der Rechnung einen einzigartigen Identifikator darstellt, handelt es sich hierbei ebenso um eine identifizierte Person.

Schon bei dem Beispiel des Energieverbrauchs zeigt sich aber, dass neben der Art der verarbeiteten Daten für die Frage des Personenbezugs weitere Aspekte viel erheblicher sein können. Zu einer Information über eine (identifizierte) Person wird der über eine Messeinrichtung erhobene Stromverbrauch doch erst, sobald er zu dem Zweck verarbeitet wird, die Abwicklung des Versorgungsvertrages (d.h. hier die Bezahlung durch den Abnehmer) zu ermöglichen, da hierfür eine Verknüpfung der Verbrauchsdaten mit den beim Stromanbieter hinterlegten Kundendaten (Name, Adresse) erfolgen muss. Auch bereits bevor die Daten mit dem Identifikator verknüpft werden, kann es sich aber schon um personenbezogene Daten handeln, nämlich solange die Person zwar noch nicht identifiziert ist, aufgrund der theoretischen Möglichkeit der Verknüpfung aber mit einiger Wahrscheinlichkeit identifiziert werden könnte. Die Person ist dann identifizierbar (vgl. Art. 4 Nr. 1 DSGVO).

Um dieses Kriterium entstehen aufgrund seiner schwierigen Abgrenzbarkeit erhebliche Rechtsunsicherheiten, insbesondere bei der Erhebung von Daten, die eine räumliche oder sachliche Nähe zu Menschen aufweisen. So lassen sich Ortsangaben, die den Standort eines Mobiltelefons zu einer bestimmten Zeit erfassen natürlich auch zu einem Bewegungsprofil des Handybesitzers zusam-

menfassen, der seinerseits z.B. über die IP- und/oder MAC-Adresse seines Gerätes identifiziert werden könnte. Ebenso können auch Messdaten zum Raumklima, wie CO₂-Gehalt, Temperatur und Feuchte, auf Personen bezogen werden, die sich in den Räumen aufhalten und so Rückschlüsse auf ihre An- und Abwesenheit zulassen. Wann die theoretische Möglichkeit solcher Vorgänge konkrete Risiken für die Betroffenen auslöst, hängt, wie noch zu zeigen ist, aber stark vom konkreten Zweck und dem Kontext der Verarbeitung ab. Anhand von Beispielen soll in dieser Darstellung daher demonstriert werden, wie durch die Vornahme kleiner ‚Risikoprüfungen‘ ermittelt werden kann, ob im Rahmen einer digitalen Anwendung personenbezogene Daten verarbeitet werden und wie die Vornahme bestimmter (Datenminimierungs-) Maßnahmen zu einer Reduzierung dieser Risiken führen kann. Risiko meint hier immer die mehr oder weniger konkrete Möglichkeit, dass eine Datenverarbeitung potenziell in die Beeinträchtigung von Grundrechten betroffener Personen umschlagen kann. Die vorgestellten Maßnahmen sollen dabei zu einer möglichst weitgehenden Reduzierung dieser Risiken führen, ggf. hin bis zur Verarbeitung ausschließlich anonymer Daten.

Raumklimadaten

Abstrakt lassen sich aus der Verarbeitung von Raumklimadaten Risiken ableiten, die stets aus der Möglichkeit resultieren, Rückschlüsse auf das Verhalten von Personen zu ziehen, insbesondere hinsichtlich ihrer An- oder Abwesenheit an einem Ort. Der Kontext der Verarbeitung ist dabei mitentscheidend dafür, welche Risiken entstehen.

Im Einfamilienhaus ließe sich etwa rückschließen, zu welcher Uhrzeit Personen gewöhnlich abwesend sind. Das bedeutet konkret, dass all jene mit Zugriff auf diese Daten, potenziell Einblicke in diese Lebensgewohnheiten der Betroffenen erhalten – ungeachtet dessen, wofür die Daten-

empfänger diese Information (zusätzlich) nutzen könnten. Damit sind die Bewohner in jedem Fall in ihrer Privatsphäre in der Ausprägung des eigenen Wohnraums betroffen. Abstrakt droht zudem stets das Risiko, dass diese Information darüber hinaus zum Nachteil der Betroffenen eingesetzt wird. In den falschen Händen könnte sie etwa zur Begehung eines Einbruchs genutzt werden.

In einem großen Verwaltungsbau entstehen wiederum andere Risiken. Hier handelt es sich um einen öffentlichen Raum, in dem eine Beeinträchtigung des Privatlebens unter Umständen zwar möglich ist (etwa im Fall eines abgeschlossenen Büros oder auf Mitarbeiter Toiletten), aber seltener und tendenziell weniger intensiv auftritt. Dafür besteht die Möglichkeit, dass die Daten vom Arbeitgeber genutzt werden, um ohne das Wissen der Beschäftigten ihre Anwesenheitszeiten zu kontrollieren. Hier wäre primär nicht die Privatsphäre der Betroffenen, sondern ihre Berufsfreiheit betroffen. Ein (extremes) Beispiel für das Verwirklichen eines solchen Risikos ist etwa die Sanktionierung des Arbeitnehmers aufgrund fehlerhafter Messdaten, die auf vermeintliche Fehlzeiten hindeuten.

Verbrauchsdaten

Auch anhand von Energieverbrauchsdaten lassen sich Informationen über die Bewohner eines Einfamilienhauses ableiten. Zunächst ist hier der Verbrauch selbst schon eine Information, die von der Öffentlichkeit grundsätzlich abgeschirmt und damit dem Kreis des Privaten zuzuordnen ist. So kann das Anliegen der Bewohner bestehen, den Nachbarn keinen Einblick in ihren erheblich höheren Energieverbrauch zu gewähren, um z.B. sozialer Ächtung zu entgehen. Eine Verarbeitung von Energieverbrauchsdaten stellt also auch in diesem Kontext einen Eingriff in das Privatleben der Betroffenen dar. Bei zeitlich hochaufgelösten Daten lassen sich neben der Anwesenheit ggf. sogar Rückschlüsse auf weitere Gewohnheiten der Bewohner ziehen,

bis hin zu einer genauen Bestimmung, wann gewöhnlich zu Mittag gegessen wird, welche Geräte im Haus vorhanden sind und welche Fernsehsendungen geschaut werden.

Demgegenüber lassen sich aus dem Gesamtgebäudeverbrauch eines größeren Wohngebäudes oder Verwaltungsbaus keine Informationen über einzelne Personen ableiten. Diese Datenverarbeitungen sind damit grundsätzlich unproblematisch.

Ein Sonderfall ist die Verwendung von Energieverbrauchsdaten zum Zweck der Verhaltensbeeinflussung z.B. mittels Gamification-Anwendungen. Treten etwa zwei Stockwerke eines Verwaltungsbaus spielerisch gegeneinander um den niedrigsten Energieverbrauch an, lassen sich zwar keine detaillierten Informationen über Einzelpersonen ableiten, die Wettbewerbssituation kann aber (auch abhängig von der Gruppengröße) einen Konformitätszwang schaffen, dem gewünschten (energiesparsamen) Verhalten zu entsprechen. Dies kann durch ein abstraktes Gefühl von Überwachung begleitet und verstärkt werden, wodurch die Autonomie der Personen beeinträchtigt wird, freie Entscheidungen zu treffen. Indem die Betroffenen ausdrücklich über die bezweckte Verhaltensbeeinflussung aufgeklärt werden, kann ihnen wiederum die Möglichkeit der Reflexion eingeräumt und so ein Stück ihrer Autonomie zurückgegeben werden. Sind Umfang und Zweck der Verarbeitung bekannt und können sich die Betroffenen ggf. sogar mit dem dahinterliegenden Ziel eines verringerten Energieverbrauchs identifizieren, ist zudem auch eine Überwindung des Gefühls der Überwachung möglich.

Gebäudedaten

Aufgrund von Daten zur Gebäudegeometrie und -historie lassen sich insbesondere Rückschlüsse auf das Vermögen des Eigentümers ziehen. Dieser kann dabei mithilfe des Grundbuchs identifiziert werden. Zwar wird das Privatleben des Eigentümers durch eine Offenlegung dieser In-

formationen, wenn überhaupt, nur in geringem Maße beeinträchtigt, allerdings könnten sie dazu verwendet werden, seine Kreditwürdigkeit zu bewerten. Fehlerhafte Daten könnten dann zu Nachteilen bei der Beantragung von Krediten führen.

Maßnahmen

Wesentlich für das Auftreten eben beschriebener Risiken, ist zum einen die Auflösung der Daten. Ein erster Schritt ist daher die Überlegung, in welcher Frequenz Messungen erfolgen müssen, um ein Funktionieren der Anwendung (gerade noch) zu gewährleisten und ob zumindest eine nachträgliche zeitliche oder örtliche Aggregation der Daten in Betracht kommt. Relevant ist außerdem die Frage der Speicherung der Daten. Grundsätzlich ist eine zentrale Speicherung stets mit höheren Risiken verbunden als eine dezentrale Speicherung, z.B. auf den jeweiligen Endgeräten. Denn umso höher der Aufwand, der für die Verknüpfung der Messdaten mit Identifikatoren (wie dem Belegplan) erforderlich ist, desto geringer sind die Risiken einer Zusammenführung dieser Einblicke in das Privatleben bzw. einer missbräuchlichen Verwendung dieser Daten. Unmittelbar risikomindernd ist dabei vor allem die zeitige Löschung (oder Aggregation) der Daten. Eine zentrale Speicherung kann wiederum in Teilen durch das Einführen eines funktionierenden Identitäts- und Berechtigungsmanagements kompensiert werden, das mittels passwortgesicherten Zugangs nur jenen Personen Zugriff auf Datensatz oder Identifikatoren (z.B. Belegungsplan) gewährt, die diese zur Erfüllung des Verarbeitungszwecks zwingend benötigen. Daran anknüpfend können interne Arbeitsanweisungen und Policies innerhalb eines Unternehmens oder sonstiger Organisationsstrukturen sicherstellen, dass Daten nur zu abschließend definierten Zwecken von einem abschließenden Personenkreis verarbeitet werden können.

BEISPIEL 1: GEBÄUDEDATEN

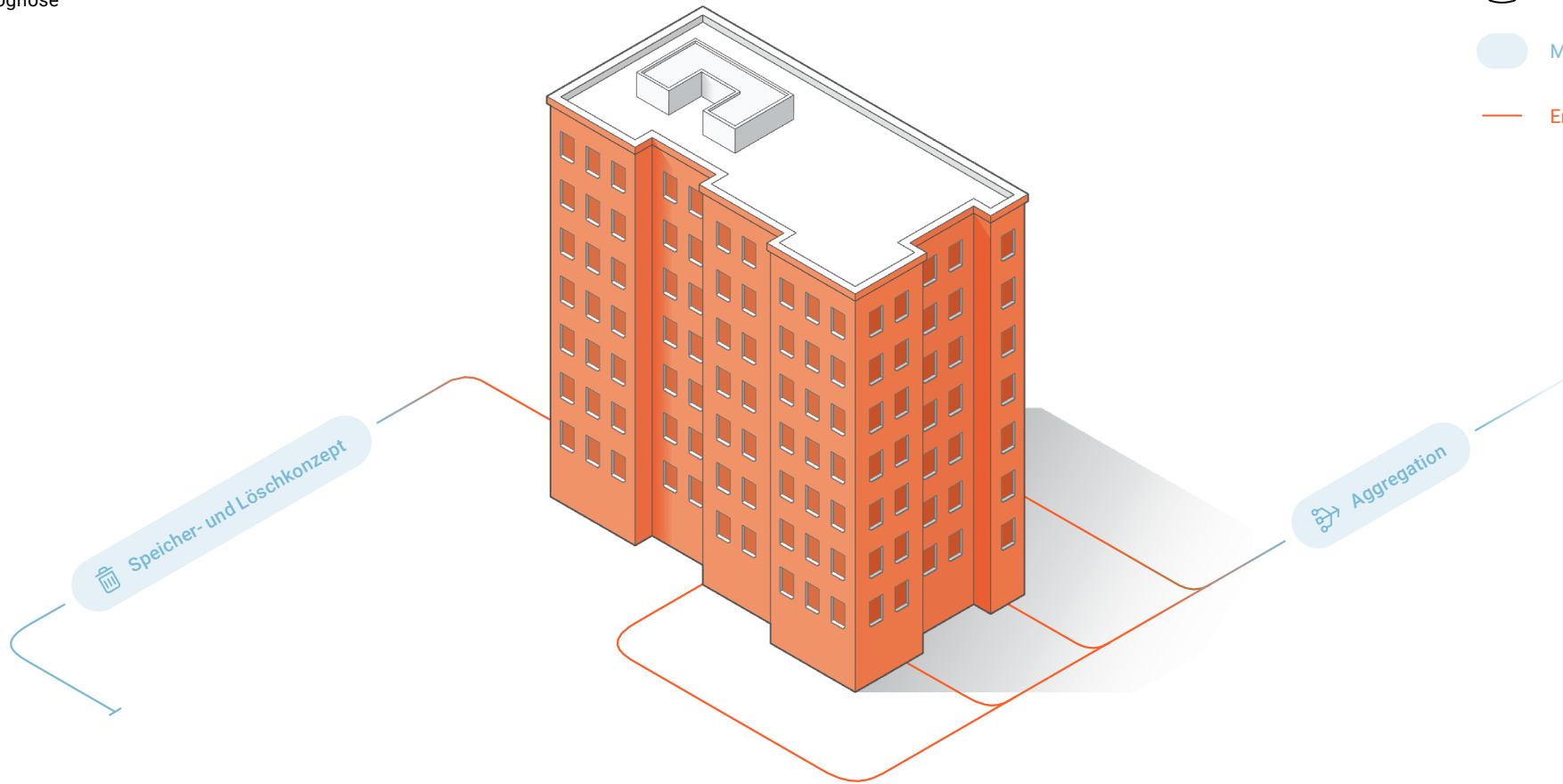
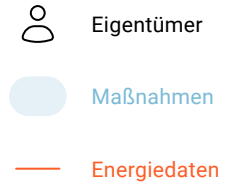
Risiken

- Das Offenlegen von Gebäudedaten ist i. d. R. keine Beeinträchtigung des Rechts auf Privatleben.
Bsp: Zwar könnte u.U. die genaue Zusammensetzung des privaten Vermögens dem privaten, abgeschirmten Lebensbereich zuzuordnen sein; nicht aber Daten zur Bauwerksgeometrie, bauteilbezogene Attribute oder die Gebäudehistorie.
- Unabhängig von einer möglichen Beeinträchtigung des Privatlebens kann das Offenlegen der Informationen aber andere Risiken verursachen.
Bsp: Eine auf falschen Gebäudedaten beruhende Vermögensbewertung könnte dazu führen, dass dem Eigentümer ein Kredit verwehrt wird, was einem Risiko für das Eigentum entspricht.
- Problematisch wird die Datenverarbeitung hier also immer erst, sobald geschützte Informationen potenziell offengelegt werden.
Bsp: Offengelegt wird die Information über den Eigentümer erst, sobald die Gebäudedaten mit dem Eigentümer verknüpft werden (z.B. durch den Abgleich mit dem Grundbuch)
- Insoweit durch technisch-organisatorische Maßnahmen sichergestellt werden kann, dass eine Verknüpfung der Daten nicht erfolgt, bleiben die beschriebenen Risiken abstrakt und kontrollierbar.
Bsp: Indem die Verknüpfung mit dem Eigentümer verhindert wird, bleibt der Informationsgehalt der Gebäudedaten darauf beschränkt, was für die Erfüllung des Verarbeitungszwecks erforderlich ist.



BEISPIEL 1.1: GEBÄUDEDATEN (VERWALTUNGSBAU)

Erstellen einer gebäude- oder quartierspezifischen
Verbrauchsprognose



RISIKEN

Verknüpfung

Gebäudedaten werden mit Identifikatoren (z.B. aus dem Grundbuch) verknüpft und lassen so Rückschlüsse auf den Eigentümer zu.

Datenmissbrauch

Die Daten werden genutzt, um den Wert des Gebäudes zu ermitteln und damit die Solvenz des Eigentümers zu bewerten.

MASSNAHMEN

Aggregation

Die Daten werden z.B. auf Straßenzugesebene aggregiert.

Speicher- und Löschkonzept

Die Daten werden mit Erreichung des Verarbeitungszwecks gelöscht oder aggregiert.

ERGEBNIS

Keine Offenlegung privater Information

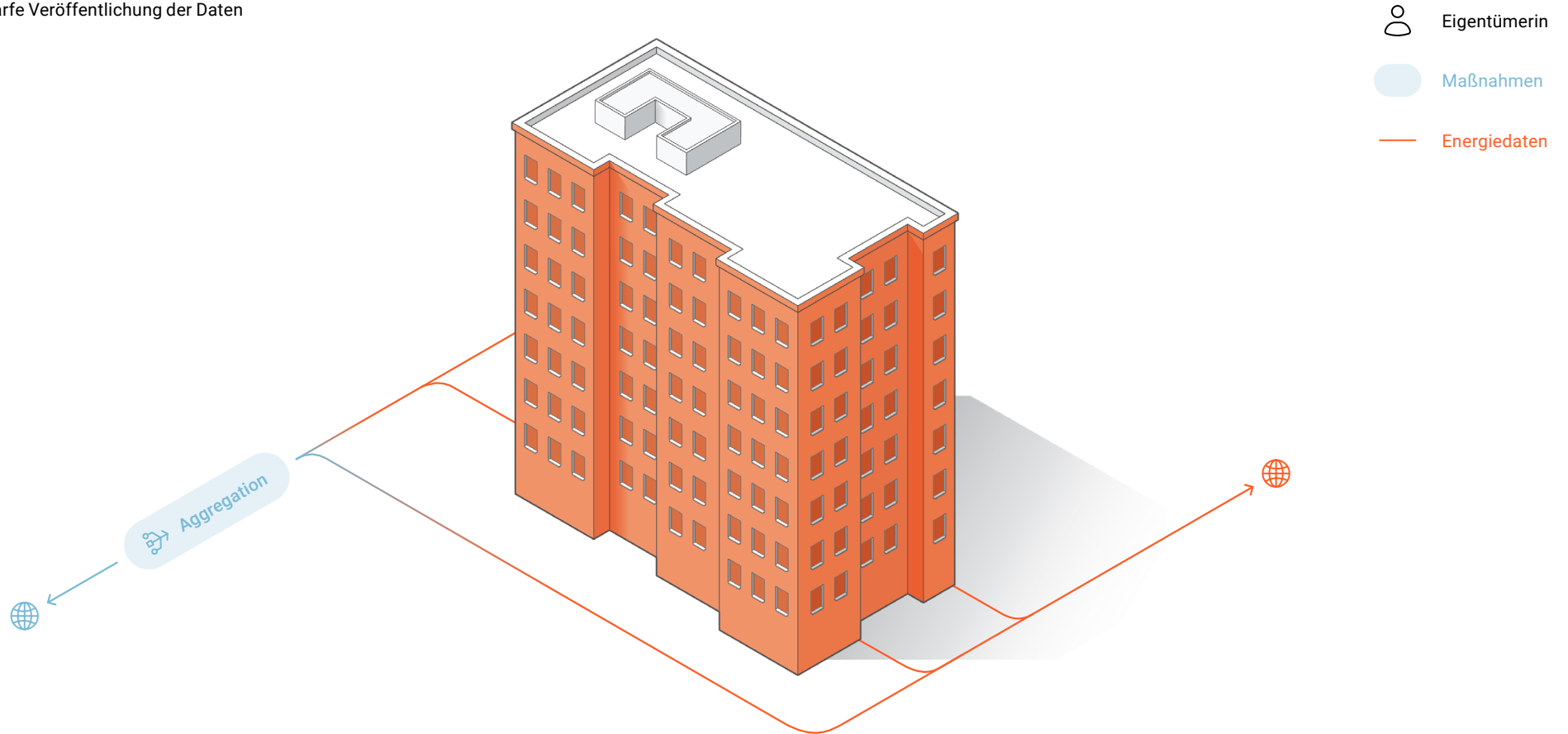
Gebäudedaten sind nicht dem abgeschirmten *privaten* Lebensbereich zuzuordnen.

Keine konkreten Risiken für Kreditwürdigkeit

Maßnahmen können missbräuchliche Verknüpfung mit den Identifikatoren verhindern.

BEISPIEL 1.2: GEBÄUDEDATEN (VERWALTUNGSBAU)

Gebäudescharfe Veröffentlichung der Daten



RISIKEN

Verknüpfung

Die Daten werden mit Identifikatoren verknüpft.

ermöglicht

Datenmissbrauch

Die Daten werden genutzt, um den Wert des Gebäudes zu ermitteln und damit die Solvenz der Eigentümerin zu bewerten.

MASSNAHMEN

Aggregation

Die Daten werden vor der Veröffentlichung z.B. auf Straßenzugesebene aggregiert.

ERGEBNIS

Konkretes Risiko für Eigentum

Ohne hinreichende Aggregation der Daten kann bei Veröffentlichung eine Kontrolle der Risiken nicht gewährleistet werden.

BEISPIEL 2: ENERGIEVERBRAUCHSDATEN

Risiken

- Das Offenlegen des Energieverbrauchs einer Einzelperson ist schon für sich genommen eine Beeinträchtigung des Privatlebens.
Bsp: Der Energieverbrauch einer Einzelperson ist schon für sich genommen eine grds. vor öffentlicher Einsichtnahme abgeschirmte Information, gegen deren Offenlegung (z.B. ggü. den Nachbarn) die betroffene Person ein schützenswertes Interesse haben kann. Des weiteren sind Rückschlüsse auf Gewohnheiten und Eigenschaften und damit die Offenlegung weiterer »privater« Informationen möglich.
- Unabhängig von einer möglichen Beeinträchtigung des Privatlebens kann das Offenlegen des Energieverbrauchs weitere Risiken verursachen.
Bsp: Je nach Auflösung der Daten können detaillierte Rückschlüsse auf das Verhalten von Personen abgeleitet werden (z.B. wann sie üblicherweise das Haus verlassen). Diese Informationen können zur Durchführung von Hauseinbrüchen verwendet werden, was eine Bedrohung für das Eigentum der Personen darstellt.
- Offengelegt wird die private Information erst, sobald die Daten mit z.B. den Bewohnerinnen verknüpft werden.
Bsp: Durch den Abgleich mit dem Klingelschild.
- Insoweit sichergestellt werden kann, dass eine Verknüpfung der Daten nicht erfolgt, bleiben die beschriebenen Risiken abstrakt und damit kontrollierbar.
Bsp: Kann die Verknüpfung verhindert werden, ist auch keine Offenlegung weiterer Informationen möglich.



BEISPIEL 2.1: ENERGIEVERBRAUCHSDATEN (EFH)

Variante 1: Jahresverbrauch

Erstellen einer gebäude- oder quartierspezifischen Verbrauchsprognose



RISIKEN

Offenlegung privater Information

Der Energieverbrauch legt private Informationen offen.

Verknüpfung

Daten werden mit weiteren Datenquellen verschnitten und legen noch mehr private Information offen.

Datenmissbrauch

Ein Mitarbeiter im Facility Management möchte wissen, wie viel Energie der neue Pool seines Nachbarn verbraucht.

MASSNAHMEN

Aggregation

Werden die Daten räumlich aggregiert (z.B. auf Straßenzugsebene), ist eine Rückführung auf Einzelpersonen nicht (mehr) möglich.

Identitäts- und Berechtigungsmanagement

Die Auswahl der Personen mit Zugriff auf die Daten oder Identifikatoren ist strikt begrenzt.

Arbeitsanweisung und Policies

Innerhalb einer Organisationsstruktur gelten klare Regeln, wie und zu welchen Zwecken die Daten verarbeitet werden dürfen.

ERGEBNIS

Geringe Beeinträchtigung des Privatlebens

Ohne Aggregation ist Energieverbrauch schon für sich genommen eine *private* Information. Bei interner Verarbeitung liegt aber nur eine geringe Beeinträchtigung vor.

Keine Verknüpfung von Datensätzen

Ein Berechtigungsmanagement verhindert das Verschneiden mehrerer Datenquellen.

Risikosenkung

Es besteht ein reduziertes Risiko missbräuchlicher Verwendung der Daten.

BEISPIEL 2.1: ENERGIEVERBRAUCHSDATEN (EFH)

Variante 2: 15-Minuten-Schlüssel

Erstellen einer gebäude- oder quartierspezifischen Verbrauchsprognose



4-5 Personen

Maßnahmen

Energiedaten

RISIKEN

Offenlegung weiterer privater Information

Ableitung von Nutzerverhalten, zum Beispiel:

- Wann sind Bewohner*Innen zuhause?
- Wann läuft gewöhnlich der Fernseher?
- Wann essen Bewohner*Innen für gewöhnlich zu Abend?

Weiterer Datenmissbrauch

Die Information wird z.B. dafür missbraucht, einen Einbruch zu planen.

MASSNAHMEN

Aggregation

Werden die Daten zeitlich und räumlich aggregiert (z.B. auf der Straßenzugesebene), ist eine Rückführung auf Einzelpersonen nicht (mehr) möglich.

Speicher- und Löschkonzept

Es wird z.B. geprüft, ob ausschließlich eine lokale Speicherung der Daten möglich ist.

ERGEBNIS

Weitergehende Beeinträchtigung des Privatlebens

- Liegen hinreichende Gewährleistungen vor, dass Informationen nicht offengelegt werden?
- Ist hohe Auflösung wirklich erforderlich zur Erreichung des Zwecks?

Ggf. weiterer Datenmissbrauch

Bei lokaler, verschlüsselter und begrenzter Speicherung ist Missbrauchsrisiko sehr gering.

BEISPIEL 2.1: ENERGIEVERBRAUCHSDATEN (VERWALTUNGSBAU)

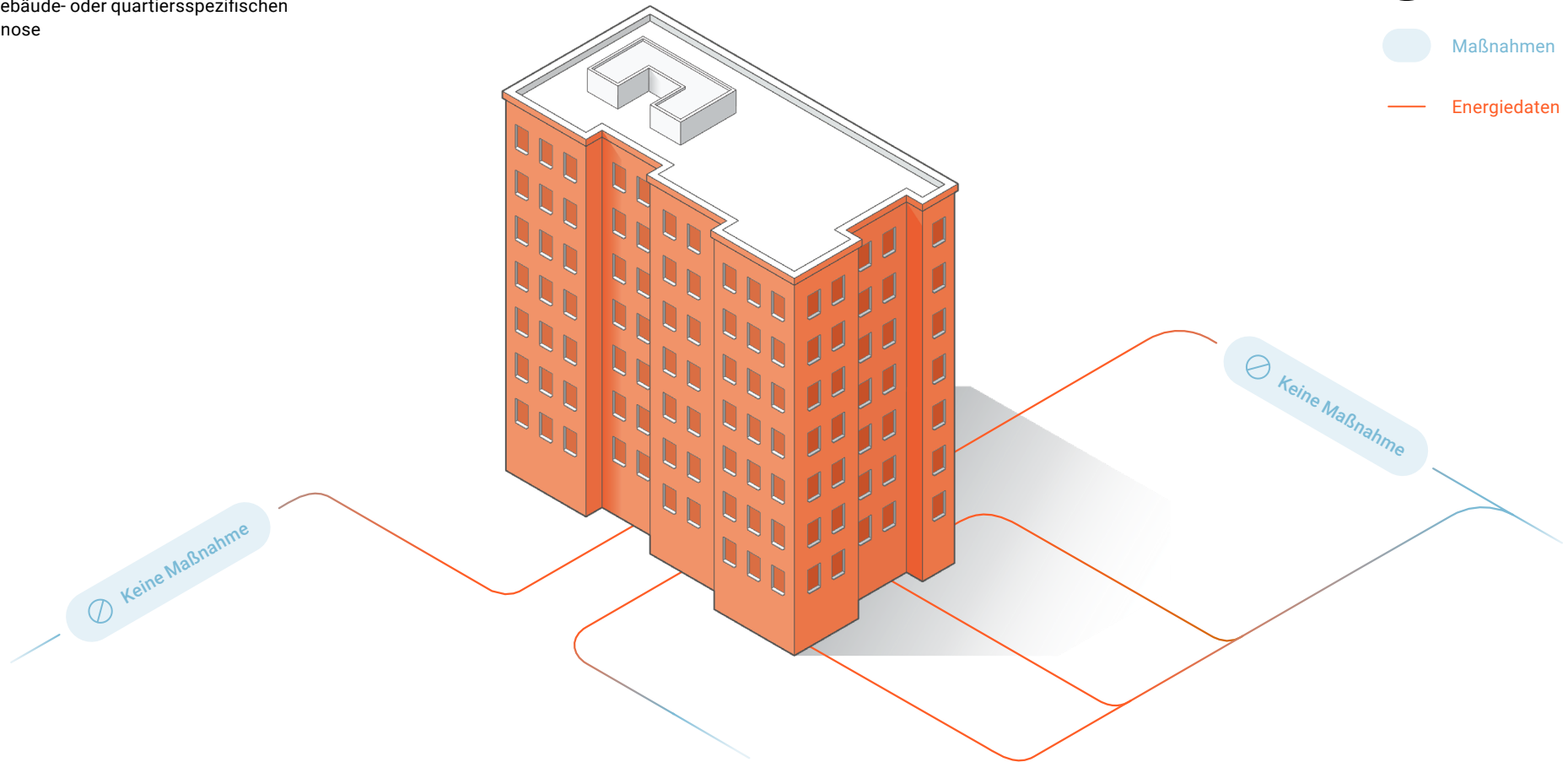
Variante 1 und 2: Jahresverbrauch und 15-Minuten-Schlüssel

Erstellen einer gebäude- oder quartierspezifischen
Verbrauchsprognose

 Gebäude

 Maßnahmen

 Energiedaten



RISIKEN

Verknüpfung mit Belegungsplan

Es wird versucht Rückschlüsse auf das Verhalten der gesamten Belegschaft des Gebäudes zu ziehen.

MASSNAHMEN

Kein Maßnahmen erforderlich

Aufgrund der bereits bei Erhebung hohen Aggregation der Daten sind keine Maßnahmen notwendig.

ERGEBNIS

Mangels konkreter Risiken kein Personenbezug

- Es sind keine Informationen über einzelne Nutzer*Innen ableitbar.
- Informationen über diese gesamte Belegschaft des Gebäudes beeinträchtigt nicht das Privatleben.
- Es sind außerdem keine weiteren Risiken ersichtlich.

BEISPIEL 2.2: ENERGIEVERBRAUCHSDATEN (EFH)

Variante 1: Gebäudescharfe Veröffentlichung der Verbrauchsdaten



RISIKEN

Offenlegung (weiterer) privater Information

- Die Nachbarn bekommen Einblick in den genauen Energieverbrauch
- Ableitung von Nutzerverhalten, zum Beispiel:
Wann sind BewohnerInnen zuhause?
Wann läuft für gewöhnlich der Fernseher?

Datenmissbrauch

Übliche Abwesenheitszeiten der Bewohnerinnen werden verwendet, um einen Einbruch zu planen.

MASSNAHMEN

Aggregation

Ohne die Aggregation ist eine Kontrolle der Identifizierungsrisiken nach der Veröffentlichung nicht mehr möglich.

ERGEBNIS

Erhebliche Beeinträchtigung des Privatlebens

Abhängig von der Auflösung werden erhebliche Mengen privater Information offengelegt.

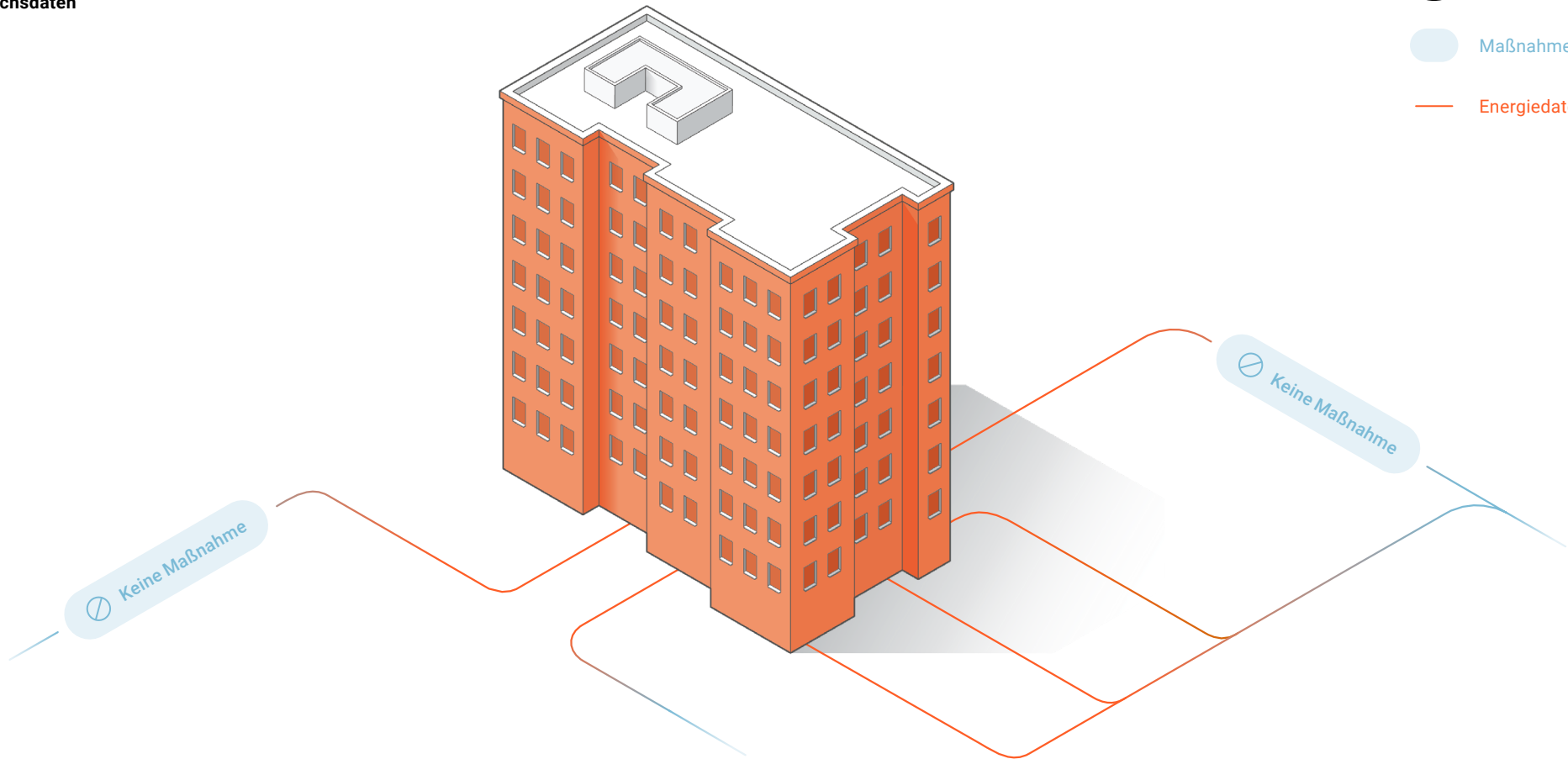
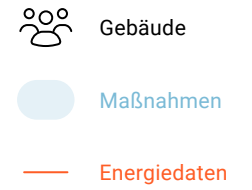
- Einwilligung zwingend erforderlich
- effektive Information über Risiken der Verarbeitung
- bei hoher Auflösung ist ggf. Erforderlichkeit problematisch

Datenmissbrauch durch Jedermann denkbar

Aufgrund des möglichen Datenmissbrauchs von beliebiger Seite ist auch keine Kontrolle der Risiken für das Eigentum möglich.

BEISPIEL 2.2: ENERGIEVERBRAUCHSDATEN (VERWALTUNGSBAU)

Variante 2: Gebäudescharfe Veröffentlichung der Verbrauchsdaten



RISIKEN

Offenlegung privater Information

Ist möglicherweise *group privacy* der gesamten Belegschaft betroffen?

MASSNAHMEN

Kein Maßnahmen erforderlich

Aufgrund der bereits bei Erhebung hohen Aggregation der Daten sind keine Maßnahmen notwendig.

ERGEBNIS

Keine Offenlegung privater Information

Der Energieverbrauch der gesamten Gebäudebelegschaft ist keine abgeschirmte *private* Information.

SONDERFALL: VERHALTENSBEEinFLUSSUNG

Risiken

- Neben der Offenbarung privater Informationen, kann eine mit der Datenverarbeitung bezweckte Verhaltensbeeinflussung ein eigenes Risiko begründen, insoweit dadurch die Autonomie der betroffenen Personen eingeschränkt wird.

Bsp: Insoweit Entscheidungsarchitekturen eine so starke Lenkungswirkung aufweisen, dass sie substantielle Kontrolle über den Entscheidungsprozess der Betroffenen ausüben, werden diese in ihrer Autonomie beschränkt, freie und selbstbestimmte Entscheidungen zu treffen. So kann etwa das Nutzbarmachen sozialen Drucks in Gamification-Anwendungen dazu führen, dass der Widerstand gegen die Lenkungswirkung deutlich erschwert oder mit weiteren Nachteilen für die Person verbunden ist.

- Insoweit durch technisch-organisatorische Maßnahmen sichergestellt werden kann, dass eine Verknüpfung der Daten nicht erfolgt, bleiben die beschriebenen Risiken abstrakt und damit kontrollierbar.

Bsp: Indem sichergestellt wird, dass sich die Informationen nicht auf Einzelpersonen beziehen lassen, können autonomiebeeinträchtigende Faktoren wie sozialer Druck verringert werden. Effektive Information der Betroffenen über den Zweck der Verarbeitung fördert zudem eine selbstbestimmte Entscheidungsfindung der Personen.



BEISPIEL 2.3: ENERGIEVERBRAUCHSDATEN (VERWALTUNGSBAU)

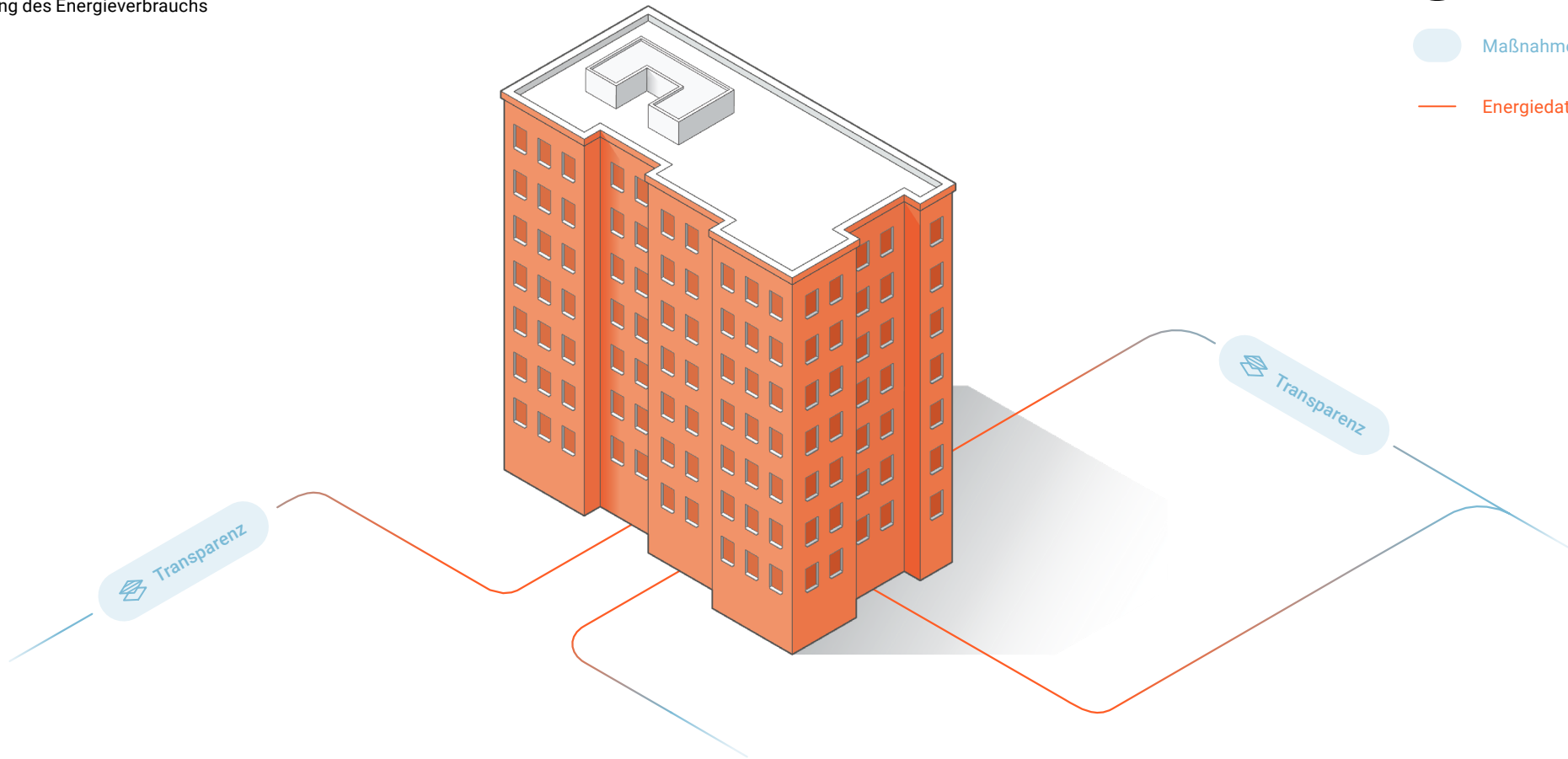
Variante 1: Visualisierung des Gesamtgebäudeverbrauchs

Visualisierung des Energieverbrauchs

 Gebäude

 Maßnahmen

 Energiedaten



RISIKEN

Keine Offenlegung privater Information

Da nur die Identifizierung der gesamten Belegschaft möglich ist, können keine Informationen über den abgeschirmten Bereich privater Lebensführung abgeleitet werden.

Einschränkung autonomer Entscheidungsfindung

Zwar entsteht beim Gesamtgebäudeverbrauch kein sozialer Druck im Sinne eines Konformitätszwangs, dafür kann jedoch bei den Betroffenen ein Gefühl der Überwachung entstehen.

MASSNAHMEN

Transparenzmaßnahmen

Effektive Information über Verhaltensbeeinflussung begünstigt die autonome Entscheidungsfindung bei den Betroffenen.

ERGEBNIS

Keine Offenlegung privater Information

Als Teil der Gesamtbelegschaft identifizierbar zu sein, genügt hier nicht für eine Beeinträchtigung des Privatlebens.

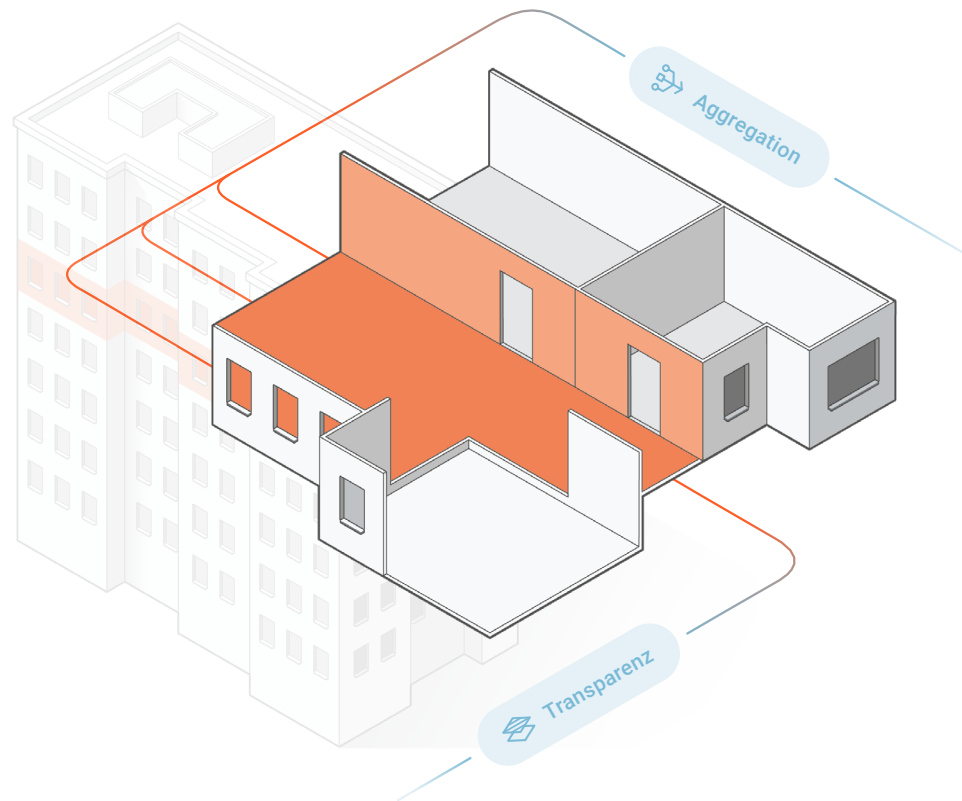
Keine Einschränkung autonomer Entscheidungsfindung


Insoweit über Ausmaß und Zweck der Datenerhebung und -visualisierung informiert wird, kann auch das Gefühl der Überwachung verhindert werden.

BEISPIEL 2.3: ENERGIEVERBRAUCHSDATEN (VERWALTUNGSBAU)

Variante 2: Visualisierung des Verbrauchs einzelner Stockwerke

Visualisierung des Energieverbrauchs



 Stockwerk

 Maßnahmen

 Energiedaten

RISIKEN

Einschränkung autonomer Entscheidungsfindung

Der sozialer Druck, sich der Verhaltensbeeinflussung zu beugen, steigt, insoweit sich der Energieverbrauch auf kleine Gruppen zurückführen lässt (*group privacy*).

Offenlegung privater Information

Insoweit Informationen wie der Energieverbrauch Einzelpersonen (z.B. einzelnen Bürozimmern) zugeordnet werden können, ist zudem das Privatleben betroffen.

MASSNAHMEN

Aggregation

Lassen sich Informationen nicht auf eine Einzelperson beziehen, sinkt auch der soziale Druck.

Transparenzmaßnahmen

Effektive Information über Verhaltensbeeinflussung begünstigt die autonome Entscheidungsfindung bei den Betroffenen.

ERGEBNIS

Ggf. Beeinträchtigung autonomer Entscheidungsfindung

Sofern sich Informationen auf kleine Gruppen zurückführen lassen, kann die Autonomie der Gruppenmitglieder beeinträchtigt sein.

Keine Offenlegung privater Information

Rückschlüsse auf eine Personengruppe sind im Arbeitskontext keine abgeschirmten (privaten) Informationen.

BEISPIEL 3: RAUMKLIMADATEN

Risiken

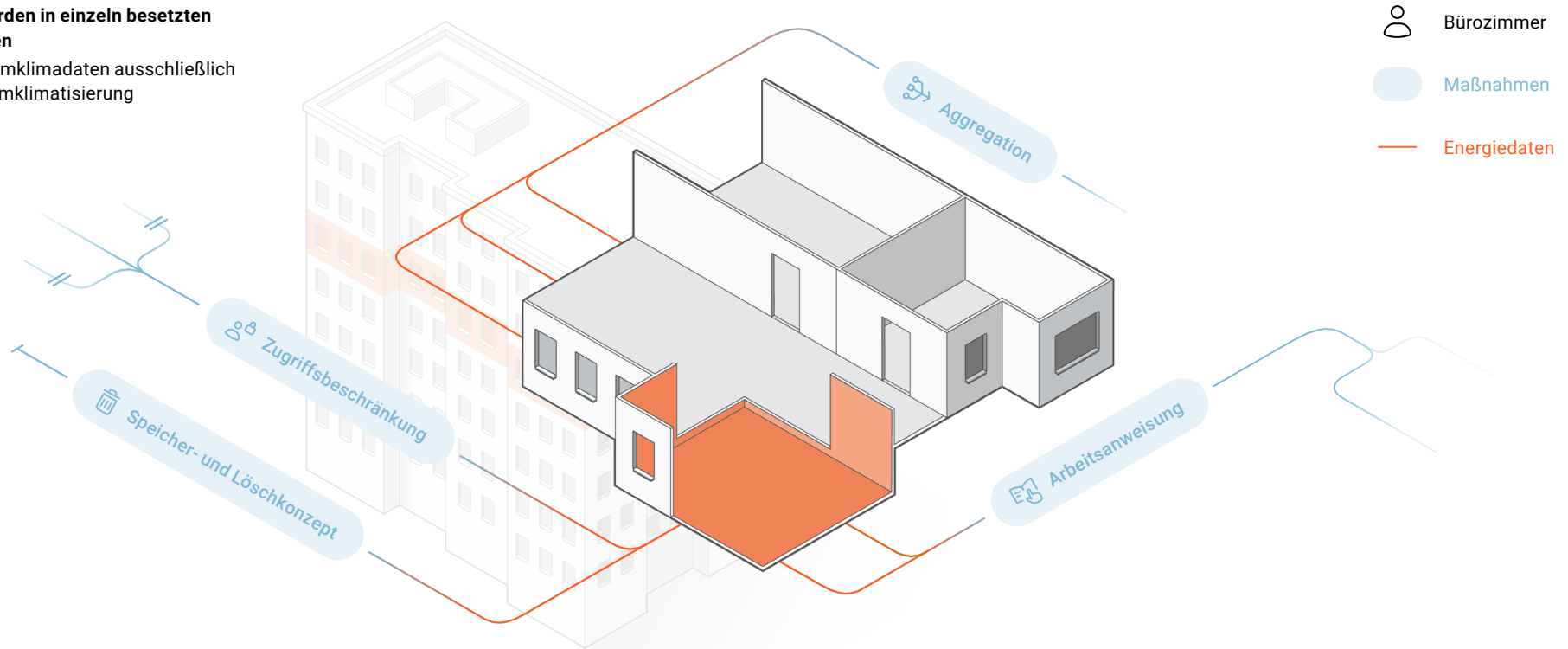
- Durch Schwankungen der Messwerte von CO₂ Gehalt, Raumtemperatur oder Luftfeuchtigkeit lassen sich abhängig von der Auflösung der Daten insbesondere Rückschlüsse auf die Anwesenheit von Personen ziehen. Insoweit das Zimmer einen vor Einsichtnahme Dritter grundsätzlich abgeschirmten Raum bildet, ist das Privatleben der Personen betroffen.
Bsp: Dies setzt ein Verknüpfen der Daten mit Identifikatoren voraus (z.B. Raumebelegungspläne).
- Unabhängig von einer möglichen Beeinträchtigung des Privatlebens kann das Ableiten der Anwesenheit von Personen weitere Risiken verursachen.
Bsp: So können insbesondere Raumklimadaten zu einer genauen Überwachung der Anwesenheit durch den Arbeitgeber herangezogen werden. Insoweit hieraus Konsequenzen für den Arbeitnehmer entstehen, verwirklichen sich Risiken für das Arbeitsleben der betroffenen Personen.
- Insoweit durch technisch-organisatorische Maßnahmen sichergestellt werden kann, dass eine Verknüpfung der Daten nicht erfolgt, bleiben die beschriebenen Risiken abstrakt und damit kontrollierbar.
Bsp: Indem ein Verknüpfen mit den Rauminsassen verhindert wird, bleibt der Informationsgehalt der Gebäudedaten darauf beschränkt, was für die Erfüllung des Verarbeitungszwecks der Raumklimatisierung erforderlich ist.



BEISPIEL 3.1: RAUMKLIMADATEN (VERWALTUNGSBAU)

Variante 1: Daten werden in einzeln besetzten Bürozimmern erhoben

Verarbeitung von Raumklimadaten ausschließlich zur Regelung der Raumklimatisierung



RISIKEN

Offenlegung privater Information

Jeder Anstieg des CO₂-Gehalts lässt Rückschlüsse auf die Anwesenheit von Personen zu. Dies ist ein Risiko für das Privatleben, insoweit das Büro ein abgeschirmter Bereich ist.

Verknüpfung mit Belegplan

Wenn technisch-organisatorische Maßnahmen das Risiko einer abweichenden Verarbeitung hinreichend minimieren, liegt kein konkretes Risiko vor.

Überwachung am Arbeitsplatz

Durch die Information können die Arbeitszeit überwacht und hierauf basierend Kündigungen ausgesprochen werden. Es bestünde ein Risiko für das Berufsleben der Betroffenen.

MASSNAHMEN

Aggregation

Nach zeitlicher und/oder räumlicher Aggregation lassen sich keine Rückschlüsse mehr auf die Anwesenheit von Personen ziehen.

Arbeitsanweisung und Policies

In internem Regelwerk wird ausdrücklich die strikte Trennung von Daten und Identifikatoren geregelt.

Identitäts- und Berechtigungsmanagement

Die Auswahl der Personen mit Zugriff auf die Daten oder Identifikatoren ist strikt begrenzt.

Speicher- und Löschkonzept

Besteht die Möglichkeit, dass Daten nur lokal auf dem Endgerät gespeichert werden? Verwaltung des Belegungsplan durch organisatorisch getrennte Einheit.

ERGEBNIS

Ggf. drohende Beeinträchtigung des Privatlebens

Die Möglichkeit einer Offenlegung privater Information ist davon abhängig, ob dies durch technisch-organisatorische Maßnahmen verhindert werden kann.

Ggf. Verknüpfung mit Identifikatoren möglich

Offenlegung privater Information kann nur unter strengen Sicherheitsmaßnahmen verhindert werden.

Ggf. drohende Überwachung des Arbeitsplatzes

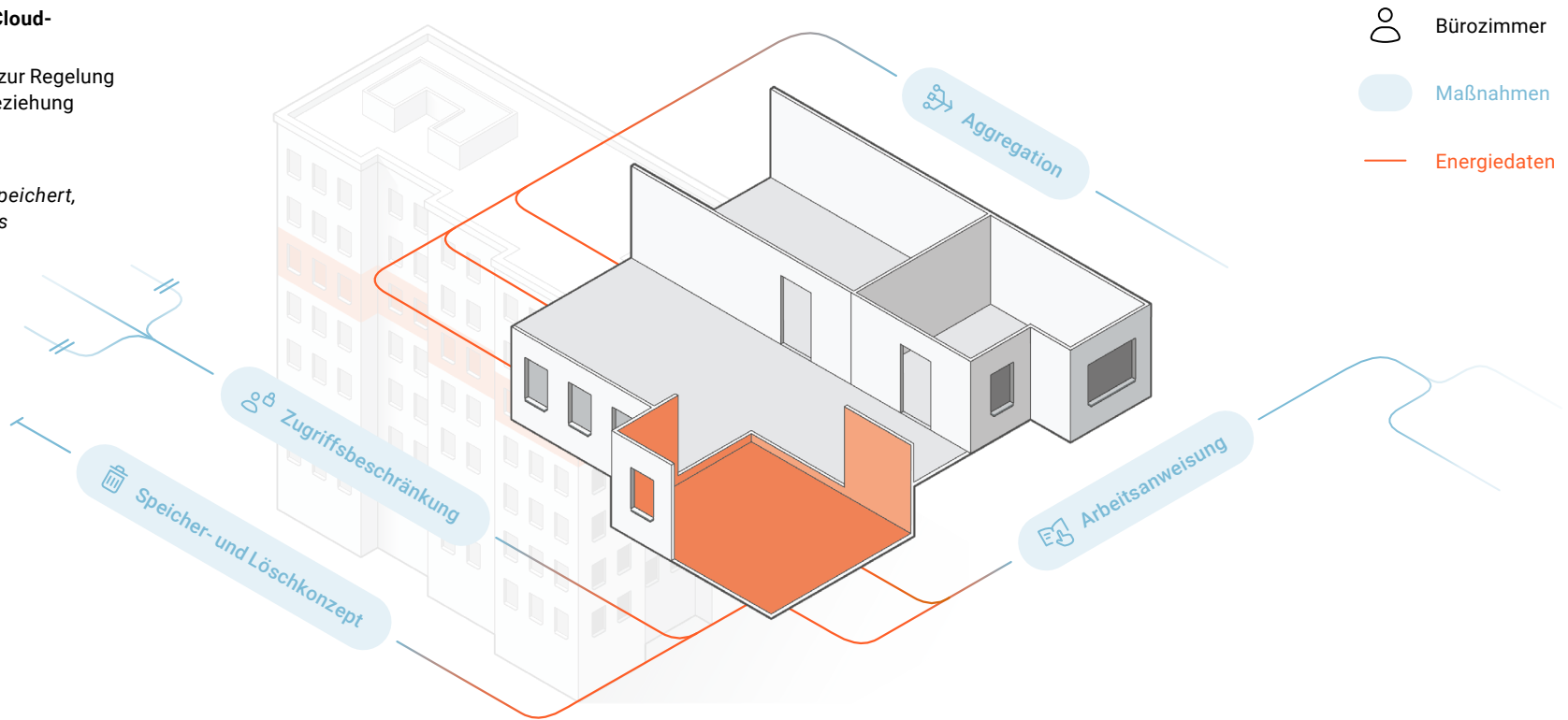
Die Überwachung am Arbeitsplatz (und damit verbunden die Arbeitszeit) kann durch striktes Identitätsmanagement verhindert werden.




BEISPIEL 3.2: RAUMKLIMADATEN (VERWALTUNGSBAU)

Variante 1: Daten werden in einer Cloud-Infrastruktur gespeichert

Verarbeitung von Raumklimadaten zur Regelung der Raumklimatisierung unter Einbeziehung des Nutzerverhaltens

Beispiel: An das Thermostat ist ein Bewegungsmelder gekoppelt, der speichert, wann eine Person üblicherweise das Zimmer betritt.



-  Bürozimmer
-  Maßnahmen
-  Energiedaten

RISIKEN

Verknüpfung mit Belegplan

Die Verknüpfung mit dem Belegplan ermöglicht das Zuordnen der Information zu Einzelpersonen und kleineren Personengruppen (z.B. geteiltes Bürozimmer).

ermöglicht

Offenlegung privater Information

Würden die Daten mit dem Belegplan verschnitten, ließen sie Rückschlüsse auf genaue Anwesenheitszeiten in Einzelbüros zu.

und

Überwachung am Arbeitsplatz

Überwachung der Arbeitszeit durch Arbeitgeber oder sonstige Verarbeitung zu abweichenden Zwecken.

MASSNAHMEN

Aggregation

Nach zeitlicher und/oder räumlicher Aggregation lassen sich keine Rückschlüsse mehr auf die Anwesenheit von Personen treffen.

Arbeitsanweisung und Policies

In internem Regelwerk wird ausdrücklich die strikte Trennung von Daten und Identifikatoren geregelt.

Identitäts- und Berechtigungsmanagement

Die Auswahl der Personen mit Zugriff auf die Daten oder Identifikatoren ist strikt begrenzt.

Speicher- und Löschkonzept

Können die Daten auch nur lokal auf dem Endgerät gespeichert werden? Verwaltung des Belegungsplans durch organisatorisch getrennte Einheit.

ERGEBNIS

Keine Verknüpfung mit Belegplan

Abhängig von der Effektivität vorliegender Datenminimierungsmaßnahmen ist eine Verknüpfung mit dem Belegplan theoretisch möglich oder nicht.

deshalb

Kein Einblick in Privatleben

Erst nachdem die Raumklimadaten mit den Identifikatoren verschnitten wurden, ergibt sich die Möglichkeit private Informationen abzuleiten.

und

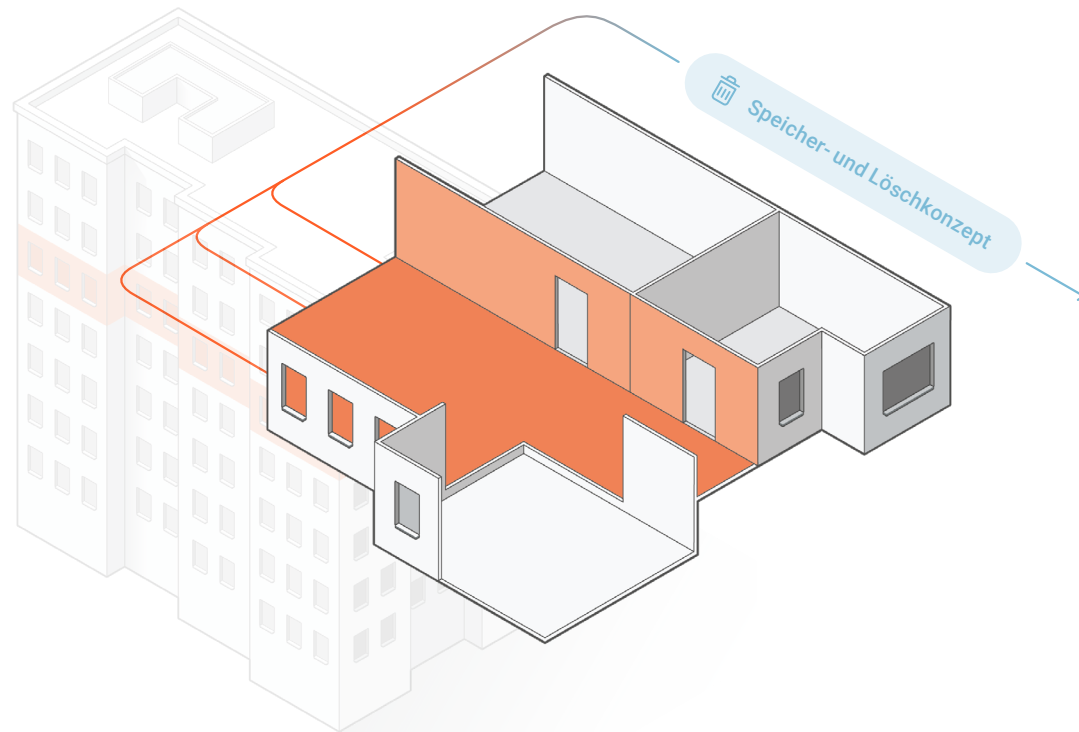
Keine Überwachung am Arbeitsplatz

Der Zugriff durch den Arbeitgeber ist durch die getroffenen Maßnahmen ausgeschlossen.

BEISPIEL 3.2: RAUMKLIMADATEN (VERWALTUNGSBAU)

Variante 2: Daten werden nur lokal auf dem Endgerät verarbeitet und gespeichert

Verarbeitung von Raumklimadaten zur Regelung der Raumklimatisierung unter Einbeziehung des Nutzerverhaltens



RISIKEN

Verknüpfung mit Belegplan

Eine Verknüpfung mit dem Belegplan ermöglicht die Zuordnung der Information zu Einzelpersonen und kleineren Personengruppen (z.B. geteiltes Bürozimmer).

ermöglicht

Offenlegung privater Information

Würden Daten mit dem Belegplan verschnitten, ließen sie Rückschlüsse auf genaue Anwesenheitszeiten in Einzelbüros zu.

und

Überwachung am Arbeitsplatz

Überwachung der Arbeitszeit durch den Arbeitgeber oder sonstige Verarbeitung zu abweichenden Zwecken.

MASSNAHMEN

Speicher- und Löschkonzept

Die nur auf den Endgeräten gespeicherten Daten werden zeitig aggregiert und/oder gelöscht.

ERGEBNIS

Keine Verknüpfung mit Belegplan

Eine Verknüpfung mit dem Belegplan ist nicht mehr möglich, da Daten und Identifikatoren strikt voneinander getrennt sind.

deshalb

Kein Einblick in Privatleben

Erst nachdem die Raumklimadaten mit den Identifikatoren verschnitten wurden, ergibt sich die Möglichkeit private Informationen abzuleiten.

und

Keine Überwachung am Arbeitsplatz

Ein Zugriff durch den Arbeitgeber ist dann ebenfalls ausgeschlossen.



Forschung für
energieoptimierte
Gebäude und Quartiere



Universität der Künste Berlin
Berlin Career College



Wissenschaftliche Begleitforschung
Energiewendebauen: Modul 4 Digitalisierung
Valentin Rupp, Julie Heumüller,
Maximilian von Grafenstein | Digitale Selbstbestimmung

Kontakt: v.rupp@udk-berlin.de | m.von-grafenstein@udk-berlin.de
Teilvorhaben: Datenschutz- und Sicherheitsaspekte
Förderkennzeichen: 03EWB004C
Projektlaufzeit: 10/2020 bis 9/2024
Themenschlagworte: Datenschutz, Datensicherheit, Data Governance,
Digitale Selbstbestimmung, Privacy
Projekttyp: Wissenschaftliche Begleitforschung

In den vorliegenden Ausführungen wurden bei der Nennung von Personengruppen in zufälliger Reihenfolge das generische Femininum oder Maskulinum benutzt. Gemeint sind dabei stets alle Geschlechter.



DOI: 10.5281/zenodo.6854465