

**INFORMATIONEN GEMÄSS Artikel 3 Absatz 2
(vernetztes Produkt) und Artikel 3 Absatz 3 (verbundene
Dienstleistung) der Verordnung (EU) 2023/2854 („Datengesetz“)**

Zusammenfassung

INFORMATIONEN GEMÄSS Artikel 3 Absatz 2 (vernetztes Produkt) und Artikel 3 Absatz 3 (damit verbundene Dienstleistung) der Verordnung (EU) 2023/2854 („Datengesetz“)	1
1. Einleitung	2
2. Begriffsbestimmungen	2
3. Identität des für die Datenverarbeitung Verantwortlichen und Kontaktdaten	2
4. Produktgenerierte Daten: Art, geschätztes Volumen, Erfassungshäufigkeit und Zugriff	2
5. Verbundene Dienstleistungsdaten: Art, geschätztes Volumen und Zugriffsmethoden	4
6. Verwendung durch den Datenverantwortlichen	5
7. Recht des Nutzers auf Zugang	5
8. Erweiterung auf zugehörige Dienstdaten	6
9. Übertragbarkeit auf Dritte	6
10. Weitergabe an Dritte und Recht auf Widerruf der Weitergabe	6
11. Einschränkungen, Bedingungen und Schutz von Geschäftsgeheimnissen und Unternehmens-Know-how	6
11.1 – Beschränkungen gemäß dem Datenschutzgesetz	6
11.2 – Transparenz hinsichtlich der Verweigerung des Zugriffs oder der Weitergabe	7
11.3 – Ausnahmen und Garantien	7
11.4 – Schutz von Geschäftsgeheimnissen	7
12. Beschwerden	8
Die gemäß Artikel 3 Absatz 2 (verbundene Produkte) und Artikel 3 Absatz 3 (verbundene Dienste) angebotenen Dienste können die folgenden Arten von Daten generieren	8
Für den Nutzer zugängliche Datenarten – Datengesetz (Zugang, Rechtsgrundlage, Einschränkungen, Format, Interoperabilität)	8
Tabelle – Daten, die für den Nutzer nicht zugänglich sind (gemäß dem Datengesetz)	10

1. Einleitung

NICE S.p.A. und ihre Tochtergesellschaften und verbundenen Unternehmen, die zur Nice-Gruppe gehören (im Folgenden als „NICE“ bezeichnet), bieten eine breite Palette von Produkten und Dienstleistungen im Bereich **der Haus- und Gebäudeautomation** an, die auch über spezielle Apps verwaltet werden können. NICE stellt die folgenden Informationen gemäß den Bestimmungen der Verordnung (EU) 2023/2854 („Datengesetz“) in Bezug auf das gemäß Art. 3, Absatz 2 des Datengesetzes direkt angeschlossene Produkt und den damit verbundenen Dienst („Dienst“) bereit, der die Möglichkeit bietet, über Apps (die „APP“) und die Nutzung von Cloud-Diensten eine Reihe von Funktionen im Zusammenhang mit den von NICE S.p.A. hergestellten Automatisierungssystemen (die „Produkte“) aus der Ferne auszuführen. Diese Informationen werden hier von NICE in seiner Rolle als Dienstleister bereitgestellt.

2. Definitionen

Vernetztes Produkt (Artikel 3, Absatz 2): Hierbei handelt es sich um das physische Gerät (z. B. Torautomatik, intelligenter Rollladen, vernetzter Sensor), das während seines Betriebs Daten erfasst oder generiert.

NICE verpflichtet sich, sicherzustellen, dass der Endnutzer innerhalb der Grenzen der vom Produkt verarbeiteten Daten entweder direkt oder über eine Schnittstelle Zugriff auf die vom Produkt generierten Daten hat.

Verbundener Dienst (Art. 3, Abs. 3): Hierbei handelt es sich um einen digitalen Dienst oder eine Software, wie z. B. die von NICE bereitgestellten Apps oder die Cloud-Plattform, die mit dem vernetzten Produkt interagiert und dessen Daten erfasst oder verarbeitet.

3. Identität des Datenverantwortlichen und Kontaktdaten

Der **Dateninhaber** gemäß Art. 2 (13) des Datenschutzgesetzes ist NICE S.p.A. mit Sitz in Via Callalta, 1, 31046 Oderzo (TV) (das „Unternehmen“) und/oder eine Tochtergesellschaft oder ein verbundenes Unternehmen der Nice-Gruppe. Der Dateninhaber handelt direkt oder über Unternehmen der Nice-Gruppe.

Für Anfragen bezüglich der Daten können Sie sich über das gekaufte Gerät (z. B. über die spezielle App und/oder das Frontend) oder gegebenenfalls per E-Mail an folgende Adresse an das Unternehmen wenden: eudataact@niceforyou.com

4. Von den Produkten generierte Daten: Art, geschätztes Volumen, Häufigkeit der Erfassung und Zugriff

Nach der Installation und Aktivierung können die Produkte technische Daten zu ihrem Betrieb generieren. Diese Daten können unter anderem Folgendes umfassen:

- Nutzungsinformationen, wie Anzahl und Häufigkeit der Aktivierungen, Öffnungs- und Schließzeiten, Protokolle und Daten, die vom Produkt generiert werden und/oder sich auf die Nutzung des Produkts beziehen (z. B. Temperatur) usw.;
- Technische Informationen, wie z. B. Gerätemodell und -version, Art der Internetverbindung, Batteriestatus und Diagnosedaten.

Die Datenerfassung kann erfolgen:

- kontinuierlich;
- in regelmäßigen Abständen;
- oder während bestimmter Ereignisse im Zusammenhang mit der Nutzung des Geräts und/oder bestimmten Phasen seines Lebenszyklus (z. B. Systemaktualisierungen, Zurücksetzen oder Statusänderungen).

Die Daten werden über eine Internetverbindung an den Dienst übertragen und können:

- lokal auf dem Gerät selbst gespeichert werden;
- oder, wenn das Gerät mit einem Onlinedienst verbunden ist, in Cloud-Datenbanken gespeichert werden, die sich in Rechenzentren in der Europäischen Union befinden und gemäß den europäischen Vorschriften zum Schutz personenbezogener Daten verwaltet werden.

Die Dauer der Datenspeicherung richtet sich nach der Art des Produkts, je nachdem, ob die Daten für einen bestimmten Zeitraum verfügbar sind, abhängig von den technischen Eigenschaften des Produkts, wie in der Bedienungsanleitung für jedes Produkt angegeben. Bei einem Gerät, das mit einem Online-Dienst verbunden und mit einem Konto verknüpft ist, darf die Dauer unbeschadet der für das Produkt und/oder die Dienstleistungskosten geltenden Speicherfristen niemals die Gültigkeitsdauer des Kontos des Benutzers überschreiten.

Wenn das Konto gelöscht und das Gerät anschließend getrennt wird, werden die Daten dauerhaft und unwiderruflich gelöscht. Nach einer solchen Löschung können keine Anträge auf Zugriff oder Übertragung von Daten mehr bearbeitet werden.

Es ist auch zu beachten, dass die Daten möglicherweise auch im Falle einer Zurücksetzung des Geräts oder einer Löschung der in der Cloud gespeicherten Daten nicht mehr verfügbar sind.

Der Zugriff wird dem Benutzer nach Authentifizierung und Verifizierung im schreibgeschützten Modus unter Verwendung der unterstützten Methoden (z. B. Referenz-App, spezielle Website, Panel usw.) gewährt und ermöglicht es dem Benutzer, den Status der Automatisierungen in Echtzeit anzuzeigen und die von den Automatisierungen erzeugten Daten gemäß den technischen Spezifikationen der einzelnen Geräte einzusehen, wie sie in den Betriebs- und Installationshandbüchern der einzelnen Produkte angegeben sind, auf die unbedingt Bezug genommen werden muss.

5. Verwandte Dienstdaten: Art, geschätztes Volumen und Zugriffsmethoden

Im Zusammenhang mit der Bereitstellung des zugehörigen Dienstes (z. B. mobile Anwendung, Cloud-Infrastruktur für die Hausautomation) werden Daten über die Nutzung der App und den Betrieb der Geräte generiert, darunter:

- Informationen zur App-Nutzung: Anzahl der gesendeten Befehle, Benutzersitzungen (Zeiten und Dauer), ausgewählte Optionen, Häufigkeit der Interaktion;
- Technische Geräteinformationen: Modell, Firmware-Version, Verbindungstyp, Batteriestatus und Diagnoseprotokolle.

Die Datenerfassung kann erfolgen:

- kontinuierlich;
- in regelmäßigen Abständen;

oder aufgrund bestimmter Ereignisse im Zusammenhang mit der Nutzung durch den Benutzer oder dem Lebenszyklus des Geräts (z. B. Updates, Zurücksetzen, Statusänderungen).

Die Datenerfassung und -übertragung erfolgt gemäß den Betriebsverfahren des Produkts und spiegelt dessen technische Eigenschaften wider.

Die gesammelten Daten werden über eine Internetverbindung an den Dienst übertragen und gespeichert:

- lokal auf dem Gerät;
- in der Cloud, wenn das Gerät mit dem Dienst verbunden ist, in Cloud-Datenbanken innerhalb der Europäischen Union, die gemäß den Datenschutzbestimmungen verwaltet werden.

Die Aufbewahrungsdauer der Daten richtet sich nach der Art des Produkts und dem Lebenszyklus des Benutzerkontos.

Wenn der Benutzer die App von seinem Gerät entfernt, können aufgrund der Art der Betriebssystem-Backups außerdem einige lokale Daten verloren gehen.

Wenn der Benutzer sein Konto löscht, zurücksetzt und/oder das Gerät trennt, werden alle gesammelten Daten unwiderruflich gelöscht. Danach können keine Anfragen für Zugriff oder Datenübertragung mehr erfüllt werden.

6. Verwendung durch den Datenverantwortlichen

Der Dateninhaber kann die von den Produkten generierten, über den Dienst verfügbaren und gesammelten Daten gemäß den Vertragsbedingungen und den dem Nutzer zur Verfügung gestellten Informationen für folgende Zwecke verwenden:

- kontinuierliche Verbesserung des Dienstes und der Produkte;
- vorausschauende Wartung und technische Diagnose;
- IT-Sicherheit und Missbrauchsverhinderung;
- aggregierte statistische Analyse und Entwicklung neuer Funktionen;
- Behebung von durch den Nutzer gemeldeten Störungen
- Erstellung von Nutzerprofilen, sofern dies gemäß der EU-

Verordnung 2016/679 zulässig ist. Die Daten können an folgende Dritte weitergegeben werden:

- Anbieter von Cloud-Infrastrukturen;
- von NICE S.p.A. oder Konzernunternehmen autorisierte technische Supportunternehmen;
- Technologiepartner und Entwickler, die an der Entwicklung, dem Testen oder der Aktualisierung von Produkten und der App beteiligt sind;
- Cybersicherheitsberater zu Audit- und Sicherheitszwecken;
- Installateure von Produkten der Nice S.p.A. oder von Unternehmen der Gruppe.

Diese Weitergabe erfolgt ausschließlich zu Zwecken, die mit den dem Nutzer angegebenen Zwecken vereinbar sind, die mit dem ordnungsgemäßen Funktionieren des Dienstes und der Einhaltung der geltenden Rechtsvorschriften über Daten und personenbezogene Daten zusammenhängen, die die Einhaltung der geltenden Rechtsvorschriften, einschließlich des Schutzes personenbezogener Daten, gewährleisten.

7. Recht des Nutzers auf Zugang

Der Nutzer hat das Recht, auf die durch die Nutzung des verbundenen Produkts und des damit verbundenen Dienstes generierten Daten (die „Daten“) zuzugreifen, einschließlich der für ihre Interpretation und Verwendbarkeit erforderlichen Metadaten, gemäß den Artikeln 4 und 5 des Datenschutzgesetzes. Dieses Recht ist nicht absolut und kann Einschränkungen unterliegen, die auf den in dieser Richtlinie angegebenen gesetzlichen Bestimmungen beruhen.

Wenn die Daten nicht direkt vom Gerät oder der Anwendung aus zugänglich sind, kann der Dateninhaber sie unverzüglich in einem vollständigen, strukturierten, gängigen und lesbaren Format zur Verfügung stellen.

Soweit technisch möglich, werden die Daten zeitnah unter Bedingungen der Sicherheit, Integrität und gleichen Qualität wie für den Inhaber bereitgestellt.

Die Daten werden in dem oben genannten Format zusammen mit Metadaten gemäß den Interoperabilitätsanforderungen des Datenrechtsgesetzes (Artikel 4 Absatz 1) bereitgestellt.

8. Erweiterung auf Daten aus verbundenen Diensten

Die oben genannten Rechte erstrecken sich auch auf Daten, die von dem zugehörigen Dienst (z. B. mobile Apps, Cloud-Schnittstellen oder andere lokale/remote Systeme) generiert oder verarbeitet werden, innerhalb der Grenzen der Bestimmungen für „Daten zugehöriger Dienste“ im Datengesetz.

9. Übertragbarkeit an Dritte

Der Nutzer hat außerdem das Recht, die in der Cloud gespeicherten Daten unverzüglich in einem strukturierten, interoperablen, gängigen und maschinenlesbaren Format an einen von ihm benannten Dritten übermitteln zu lassen, und zwar in Echtzeit, sofern dies technisch möglich ist und keinen offensichtlich unverhältnismäßigen Aufwand erfordert (Artikel 5 Absatz 1 des Datenschutzgesetzes).

Die Übertragungsmethoden sowie die Verfügbarkeit historischer Daten hängen vom Typ und Modell des Geräts, der verwendeten Verbindung und den implementierten Kommunikationsprotokollen ab.

Anfragen zur Klärung oder zur Ausübung Ihrer Rechte können über den offiziellen technischen Support-Kanal per E-Mail an folgende Adresse gerichtet werden: eudataact@niceforyou.com.

Die durch geltendes Recht und den Absatz über Einschränkungen vorgesehenen Beschränkungen bleiben unberührt.

10. Weitergabe an Dritte und Recht auf Widerruf der Weitergabe

Der Nutzer kann die Weitergabe von Daten, die durch Automatisierungen und den Dienst generiert wurden, sowie der damit verbundenen Metadaten an vom Nutzer ausgewählte Dritte innerhalb der in Artikel 5 des Datenschutzgesetzes festgelegten Grenzen über eine spezielle Funktion in der App gemäß den technischen Spezifikationen des Produkts beantragen. Nutzer können ihre Zustimmung zur Weitergabe **jederzeit** auf die gleiche Weise **widerrufen**. Der Widerruf wird **sofort** wirksam, unbeschadet der Rechtmäßigkeit der Verarbeitung auf der Grundlage der vor dem Widerruf erteilten Einwilligung.

11. Einschränkungen, Bedingungen und Schutz von Geschäftsgeheimnissen und Unternehmens-Know-how

11.1 – Beschränkungen gemäß dem Datenschutzgesetz

NICE als Dateninhaber (Data Holder) kann unter Wahrung der Rechte des Nutzers gemäß dem Datenschutzgesetz in den folgenden Fällen den Zugriff, die Übertragbarkeit oder die Weitergabe bestimmter Daten einschränken oder verweigern:

- wenn die Offenlegung der Daten zu einer Verletzung der Grundrechte oder Grundfreiheiten Dritter führen kann, einschließlich des Schutzes der personenbezogenen Daten anderer Personen (Artikel 4 Absatz 6);
- wenn der beantragte Zugang zur Offenlegung von Geschäftsgeheimnissen, vertraulichem Know-how oder strategischen Informationen führen oder die Cybersicherheit oder Integrität der digitalen Infrastruktur gefährden könnte (Art. 4 Abs. 6 und 7);
- wenn die Bearbeitung der Anfrage einen technischen Aufwand erfordert, der in keinem Verhältnis zu dem steht, was zum Abrufen und Bereitstellen der angeforderten Daten erforderlich ist (Art. 4 Abs. 3 und 7).
- Wenn die Offenlegung der Daten nicht möglich ist, weil die Daten aufgrund der technischen Eigenschaften des Produkts nicht von NICE gespeichert werden oder weil die Daten aufgrund der Trennung des Produkts vom Benutzerkonto oder der Löschung des Benutzerkontos dauerhaft gelöscht wurden.

11.2 – Transparenz hinsichtlich der Verweigerung des Zugriffs oder der Weitergabe

Im Falle einer vollständigen oder teilweisen Verweigerung des Zugriffs, der Übertragung oder der Weitergabe der angeforderten Daten stellt der Dateninhaber dem Nutzer eine schriftliche und begründete Mitteilung zur Verfügung, die Folgendes enthält:

- die konkreten Gründe für die Verweigerung;
- eine Angabe der von der Einschränkung betroffenen Datenkategorien;
- die rechtlichen und technischen Referenzen, auf denen die Entscheidung basiert.

11.3 – Ausnahmen und Garantien

Jegliche Einschränkungen werden nach dem Grundsatz der Verhältnismäßigkeit vorgenommen, wobei von Fall zu Fall das Gleichgewicht zwischen den Rechten des Nutzers und den vom Dateninhaber geschützten Interessen bewertet wird und die Gründe angemessen intern dokumentiert werden.

Der Nutzer behält das Recht:

- eine dokumentierte Antwort auf die Anfrage zu erhalten;
- eine Beschwerde gemäß dem internen Verfahren zur Ausübung von Rechten einreichen;
- die Angelegenheit gegebenenfalls an die zuständigen Aufsichts- oder Justizbehörden weiterleiten.

11.4 – Schutz von Geschäftsgeheimnissen

Wenn die von den Produkten und dem Dienst generierten Daten in aggregierter oder strukturierter Form Informationen enthalten, die gemäß geltendem Recht und Artikel 4 des Datenschutzgesetzes als Geschäftsgeheimnisse gelten, ergreift NICE geeignete technische und vertragliche Maßnahmen, um den Schutz dieser Geheimnisse zu gewährleisten, darunter (beispielsweise):

- Unterzeichnung von Vertraulichkeitsvereinbarungen (NDAs);
- Einführung sicherer und profilierter Zugangsprotokolle;
- Anwendung branchenspezifischer Verhaltenskodizes oder selektiver Genehmigungsverfahren;
- selektive Filterung gemeinsam genutzter Daten unter Verwendung von Pseudonymisierungs- oder Anonymisierungstechniken

Wenn der Nutzer die vereinbarten Maßnahmen nicht einhält oder sich in einer Weise verhält, die die Vertraulichkeit von Geschäftsgeheimnissen gefährdet, kann der Dateninhaber die Weitergabe und den Zugriff auf die betreffenden Daten nach schriftlicher Mitteilung aussetzen oder einschränken.

12. Beschwerden

Der Nutzer hat das Recht, bei der AgID, der gemäß Artikel 37 des Datenschutzgesetzes zuständigen nationalen Behörde, eine Beschwerde einzureichen, wenn er der Ansicht ist, dass gegen die Bestimmungen von Kapitel II des Datenschutzgesetzes verstoßen wurde.

Die gemäß Artikel 3 Absatz 2 (verbundene Produkte) und Artikel 3 Absatz 3 (verbundene Dienste) angebotenen Dienste können die folgenden Arten von Daten generieren.

Siehe Tabelle unten.

Art der für den Nutzer zugänglichen Daten – Datenschutzgesetz (Zugang, Rechtsgrundlage, Einschränkungen, Format, Interoperabilität)

DATENKATEGORIE	BESCHREIBUNG	ERWARTETER ZUGRIFF für den Nutzer	RECHTSGRUNDLAGE	GRUND FÜR DIE BESCHRÄNKUNG	FORM	INTEROPERABILITÄT
Daten vom Hub-Endpunkt (Swagger/API)	Über API zugängliche technische Daten	Benutzer	Artikel 4 und 5 des Datenschutzgesetzes + Nutzungsvereinbarung	Keine	JSON oder jedes andere benutzerlesbare Format	REST-API oder GraphQL
Endpunkt für die Analyse	Sammelstelle für Systemanalyse	Benutzer	Art. 4 und 5 Datenschutzgesetz + Nutzungsvereinbarung	Keine	JSON oder jedes andere für Benutzer lesbare Format	REST API oder GraphQL
Liste der aufgezeichneten Ereignisse: A. Gerätestatus B. Energiedaten	Geräteereignisprotokoll	Benutzer	Art. 4 und 5 des Datenschutzgesetzes + Nutzungsvereinbarung	Keine	JSON oder jedes andere für Benutzer lesbare Format	REST-API oder GraphQL
	Betriebsstatus (ein/aus, Temperatur, Batterien)	Benutzer	Art. 4 und 5 Datenschutzgesetz + Benutzervertrag	Keine	JSON oder jedes andere benutzerfreundliche lesbare Format	REST-API oder GraphQL
DATENKATEGORIE	BESCHREIBUNG	ERWARTETER ZUGRIFF für den Nutzer	RECHTSGRUNDLAGE	GRUND FÜR DIE BESCHRÄNKUNG	FORM	INTEROPERABILITÄT
C. Aktionsbezogene Ereignisse D. Alarmereignisse E. Installationsereignisse (für Hub-Administratoren)	Strom, Verbrauch,	Benutzer	Art. 4 und 5 Datenschutzgesetz + Benutzervertrag	Keine	JSON oder jedes andere für Benutzer lesbare Format	REST-API oder GraphQL
	Gelöschte/geänderte Szenen/Bilder	Benutzer	Art. 4 und 5 Datenschutzgesetz + Nutzungsvereinbarung	Keine	JSON oder jedes andere für Benutzer lesbare Format	REST API oder GraphQL

	Sicherheitsbenachrichtigungen oder Ereignisse	Benutzer/Installateur	Art. 4 und 5 Datengesetz + Nutzungsvereinbarung	Keine	JSON oder jedes andere für Benutzer lesbare Format	REST API oder GraphQL
	Installationsprotokoll	Admin-Hub + Installer Endbenutzer haben keinen Zugriff auf Protokolle; Protokolle können in pseudonymisierter oder aggregierter Form bereitgestellt werden	Vertrag oder berechtigtes Interesse des Verantwortlichen zur Nachverfolgung von Aktivitäten	Diese Protokolle enthalten personenbezogene Daten (Name, E-Mail- Adresse, Aktivitäten) und möglicherweise Sicherheitsinformationen (administrativer Zugriff).	JSON oder jedes andere für Benutzer lesbare Format	REST-API oder GraphQL
Liste der Geräte und Konfigurationen	Name, Raum, Parameter, Benachrichtigungssätze, Verbindungen zu anderen Geräten,	Benutzer	Art. 4 und 5 Datengesetz + Benutzervertrag	Keine	JSON oder jedes andere für Benutzer lesbare Format	REST-API oder GraphQL
Liste der Automatisierungen	Name der Automatisierung, Raum (z. B. Wohnzimmer, Garten), Status (aktiv/inaktiv), Typ (Sicherheit, Beleuchtung usw.), Blöcke oder Szenensequenzen oder Szenen, die Aktionen darstellen	Benutzer	Art. 4 und 5 Datengesetz + Benutzervertrag	Keine	JSON oder jedes andere für Benutzer lesbare Format	REST-API oder GraphQL
Liste der installierten Integrationen	Name der Integration Hersteller Aktiv/inaktiv- Status	Benutzer/Installateur	Art. 4 und 5 des Datenrechts + Benutzervertrag	Bei NDAs mit Drittanbietern wird nur die Funktionsbeschreibung bereitgestellt.	JSON oder jedes andere für Benutzer lesbare Format	REST-API oder GraphQL
Programmierliste Klimadaten	Timer, Zeitfenster für Ereignisse	Benutzer	Art. 4 und 5 des Datenschutzgesetzes + Benutzervertrag	Keine	JSON oder ein anderes benutzerlesbares Format	REST-API oder GraphQL
DATENKATEGORIE	BESCHREIBUNG	ERWARTETER ZUGRIFF für den Nutzer	RECHTSGRUNDLAGE	GRUND FÜR DIE BESCHRÄNKUNG	FORM	INTEROPERABILITÄT

Bewässerungsdaten	Temperatur-/Feuchtigkeitsmesswerte Feuchtigkeit	Benutzer	Art. 4 und 5 Datengesetz + Benutzervertrag	Keine	JSON oder jedes andere für Benutzer lesbare Format	REST-API oder GraphQL
	Bewässerungshäufigkeit und Verbrauch (Überprüfung)	Benutzer	Art. 4 und 5 Datengesetz + Benutzervertrag	Keine	JSON oder jedes andere für Benutzer lesbare Format	REST-API oder GraphQL
Netzwerkeinstellungen	IP, DNS, WLAN...	Benutzerinstallateur/Administrator	Art. 4 und 5 Datengesetz + Nutzungsvereinbarung	IT-Sicherheit Mögliches IT-Sicherheitsrisiko	JSON oder jedes andere benutzerlesbare Format	REST-API oder GraphQL
Benutzereinstellungen (Hub)	ID, Präferenzen, E-Mail-Hash	Benutzerdaten sind nur für den Kontoinhaber verfügbar und dürfen nicht an Dritte weitergegeben werden.	Art. 4 und 5 des Datenschutzgesetzes + Nutzungsvereinbarung	Keine	JSON oder jedes andere für Benutzer lesbare Format	REST-API oder GraphQL
Normale Benutzerdaten	Grundeinstellungen und Szenenverlauf	Benutzer	Art. 4 und 5 des Datenschutzgesetzes + Nutzungsvereinbarung	Keine	JSON oder jedes andere benutzerlesbare Format	REST API oder GraphQL
Hub-Daten (Admin)	Hub-Daten + ID + Locale + Cloud + dem Konto hinzugefügte Telefone mit dem zugehörigen Hash und Namen.	Admin und Eigentümer	Art. 4 und 5 Datengesetz + Nutzungsvereinbarung	Keine	JSON oder ein anderes benutzerlesbares Format	REST-API oder GraphQL
Sicherungsliste	Konfigurationskopien Was ist noch in den Backups enthalten?	Benutzer + Installateur	Art. 4 und 5 Datengesetz + Benutzervertrag	Keine	Abhängig vom Gerät	Keine; jedes Gerät unterstützt sein eigenes Format
Liste der Installateure und Überwachung	Namen, E-Mail-Adressen, protokollierte Zugriffe	Gut, wenn Daten bereitgestellt werden müssen, werden diese pseudonymisiert	Vertragliche und sicherheitsrelevante Verpflichtungen	Zugriff nur durch NICE als Datenverantwortlicher, Schutz der Privatsphäre der Installateure	JSON oder jedes andere benutzerlesbare Format	REST-API oder GraphQL

Tabelle – Daten, auf die der Nutzer keinen Zugriff hat (gemäß dem Datengesetz)

DATENKATEGORIE	BESCHREIBUNG	ERWARTETER ZUGRIFF	RECHTSGRUNDLAGE	GRUND FÜR DIE EINSCHRÄNKUNG	ERWARTETES FORMAT	INTEROPERABILITÄT
Low-Level-Protokolle (Betriebssystem)	Technische Protokolle, die von Betriebssystemkomponenten generiert werden.	Für den Benutzer nicht zugänglich	Art. 4 Abs. 6-7 Datenschutzgesetz + NDA/Vertraulichkeit Wesentlichkeit	Know-how	Nicht zutreffend	Nicht zutreffend
DATENKATEGORIE	BESCHREIBUNG	ERWARTETER ZUGRIFF	RECHTSGRUNDLAGE	GRUND FÜR DIE EINSCHRÄNKUNG	ERWARTETES FORMAT	INTEROPERABILITÄT
Chipdaten	Informationen über integrierte Chips und Firmware	Für den Benutzer nicht zugänglich	Art. 4 Abs. 6-7 + Vertraulichkeitsvereinbarungen mit Dritten	Know-how: unterliegt einer Vertraulichkeitsvereinbarung für erweiterten Support	Nicht offenlegbar	Nicht zutreffend
Integrations-/Automatisierungsgcode	Quellcode für Szenen oder Automatisierungen	Für den Benutzer nicht zugänglich	Art. 4(6)-(7)	Know-how: umfasst proprietäre API-Aufrufe, verschlüsselte Elemente	Nicht offenlegbar	Nicht zutreffend
Unkomprimierte Backups (Cloud/Hub)	Archivierte Systemkopien ohne Komprimierung	Nicht zugänglich, da sie sensible Konfigurationen und Authentifizierungsdaten enthalten	Art. 4(7) + Sicherheit	Sicherheit:	Nicht offenlegbar	Der Benutzer verfügt nicht über den Entschlüsselungscode
Informationen zu Passwörtern, PINs oder Hashes	Verschlüsselte Authentifizierungsdaten	Nicht zugänglich	Art. 4 Abs. 6-7 + Sicherheit	Sicherheit: Zugriff nur nach Anmeldung	Nicht offenlegbar	Nicht zugänglich
Installationsdateien	Persönliche und berufliche Daten (z. B. Telefon, E-Mail, installierte Hubs)	Für den Endnutzer nicht zugänglich	DSGVO + Art. 4(6) Datenschutzgesetz	Datenschutz (DSGVO)	Keine Rechtsgrundlage für die Offenlegung	Zugriff auf Administrator beschränkt
Zertifikate	Digitale Zertifikate für Authentifizierung oder Verschlüsselung	Nicht zugänglich	Art. 4(7) + Sicherheit	Sicherheit	Nicht offenlegbar	Nicht zugänglich
Token	API- oder Sitzungsauthentifizierungstoken	Nicht zugänglich	Art. 4(7) + Sicherheit	Sicherheit:	Nicht offenlegbar	Nicht zugänglich
Aggregierte Analysedaten	Anonyme Daten, die von mehreren Benutzern aggregiert wurden	Nach irreversiblen Anonymisierungsprozess nicht zugänglich Nicht zum Nutzer zurückverfolgbar	Art. 4(6) Datengesetz	Know-how	Nicht offenlegbar	Interne Verwendung innerhalb des Unternehmens

<p>Daten werden nach Ablauf der Aufbewahrungsfrist nicht gespeichert oder unwiderruflich gelöscht</p>	<p>Gerätedaten, die nicht gespeichert sind, Daten, die nach Ablauf der maximalen Aufbewahrungsfrist gespeichert und gelöscht wurden, Daten von Benutzern, die Geräte von ihrem Konto getrennt haben, das Gerät nicht mit ihrem Konto verknüpft haben oder ihr Konto gelöscht haben, was zur unwiderruflichen Löschung der Daten geführt hat.</p>	<p>Nicht zugänglich, da sie unwiderruflich gelöscht wurden oder in anonymisierter Form vorliegen und daher nicht dem Nutzer zugeordnet werden können.</p>	<p>Art. 4(7) + Sicherheit</p>	<p>Daten, die aufgrund der Spezifikationen einzelner Geräte oder der Löschentscheidungen der Benutzer nicht mehr vorhanden sind. Falls vorhanden, wurden die Daten unwiderruflich anonymisiert.</p>	<p>Nicht zutreffend</p>	<p>Nicht zutreffend</p>
--	--	---	-------------------------------	---	-------------------------	-------------------------