EU DATA ACT POLICY - ENGLISH

WWW.ABLEAUTOMATION.COM

INFORMATION PROVIDED PURSUANT TO Article 3(2) (Connected Product) and Article 3(3) (Related Service) of Regulation (EU) 2023/2854 ("Data Act")

Summary

INFORMATION PROVIDED PURSUANT TO Article 3(2) (Connected Product) and Article 3(3) (Related Service) of Regulation (EU) 2023/2854 ("Data Act")

- The Services offered pursuant to Articles 3(2) (Connected Products) and 3(3) (Related Services) may generate the following types of data.
- Types of data accessible to the user – Data Act (Access, Legal basis, Restrictions, Format, Interoperability)
- Table – Data not accessible to the user (pursuant to the Data Act)

1. Introduction.

NICE S.p.A. and its subsidiaries and affiliates belonging to the Nice Group (hereinafter referred to as **NICE**) offer a wide range of products and services in the field **of Home and Building Automation**, which can also be managed via dedicated apps. NICE provides the following information in accordance with the provisions of Regulation (EU) 2023/2854 (**"Data Act**") with reference to both the product directly connected pursuant to Art. 3, paragraph 2 of the Data Act and the related service ("Service") which provides the possibility, through apps (the **"APP")** and the use of Cloud services, to remotely perform a series of functions connected with the automation systems produced by NICE S.p.A. (the **"Products")**. This information is provided here by NICE in its role as Service provider.

2. Definitions.

Connected product (Article 3, paragraph 2): This is the physical device (e.g., gate automation, smart roller shutter, connected sensor) that collects or generates data during its operation.

NICE undertakes to ensure that the end user has access to the data generated by the product, either directly or via an interface, within the limits of the data processed by the product.

Related service (Art. 3, para. 3): This is a digital service or software, such as the apps provided by NICE or the cloud platform, which interacts with the connected product, collecting or processing its data.

3. Identity of the data controller and contact details

The **Data Holder** pursuant to Art. 2 (13) of the Data Act is NICE S.p.A., with registered office in Via Callalta, 1, 31046 Oderzo (TV) (the "Company") and/or a subsidiary or affiliate belonging to the Nice Group. The Data Holder acts directly or through companies belonging to the Nice Group.

For any request concerning data, the Company may be contacted through the purchased device (for instance, via the dedicated App and/or front-end) using the relevant account, so that the identity of the requester can be duly verified, or, alternatively, by e-mail at the following address: eudataact@niceforyou.com

In the latter case, it is necessary that the e-mail include the details of the requester's identity as well as the serial number of the product subject to the request, and that a file containing a copy of a valid identification document be attached. Failure to provide, within the e-mail, unambiguous elements allowing for the verification of the requester's identity and its association with the product and/or service to which the data request refers shall necessarily result in the impossibility to process the request, which therefore cannot be granted.

4. Data generated by the Products: nature, estimated volume, frequency of collection and access

Following installation and activation, the Products may generate technical data relating to their operation. Such data may include, but is not limited to:

- Usage information, such as number and frequency of activations, opening and closing times, logs and data generated by the product and/or related to the use of the product (e.g., temperature), etc.;
- Technical information, such as device model and version, type of internet connection, battery status, and diagnostic data.

Data collection may take place:

- on an ongoing basis;
- at regular intervals;
- or during specific events related to the use of the device and/or particular stages of its life cycle (e.g., system updates, resets, or status changes).

The data is transmitted to the Service via an internet connection and may be:

- stored locally on the device itself;
- or, if the device is associated with an online service, stored in cloud databases located in data centers in the European Union and managed in accordance with European regulations on the protection of personal data.

The duration of data storage is determined based on the type of product, depending on which the data may be available for a certain period of time depending on the technical characteristics of the product as indicated in the instruction manual for each product. In the case of a device associated with an online service and linked to an account, without prejudice to the storage time limits specific to the product and/or service costs, the duration may never exceed the validity period of the User's account.

When the account is deleted and the device is subsequently disconnected, the data is permanently and irreversibly deleted. After such deletion, any requests for access or transfer of data cannot be processed.

It should also be noted that the data may no longer be available even in the event of a device reset or deletion of data stored in the cloud.

Access is granted to the user after authentication and verification in read-only mode using the supported methods (e.g., reference app, dedicated website, panel, etc.) and allows the user to view the status of the automations in real time and consult the data produced by the automations according to the technical specifications of each device as indicated in the operating and installation manuals of each product, to which reference must necessarily be made.

5. Related service data: nature, estimated volume, and access methods

In the context of providing the related service (e.g., mobile application, cloud infrastructure for home automation), data relating to the use of the app and the operation of the devices is generated, including:

- App usage information: number of commands sent, user sessions (times and duration), options selected, frequency of interaction;
- Technical device information: model, firmware version, connection type, battery status, and diagnostic logs.

Data collection may take place:

- continuously;
- at regular intervals;

or as a result of specific events related to user usage or the device's life cycle (e.g., updates, resets, status changes).

Data collection and transmission follow the product's operating procedures and reflect its technical characteristics.

The collected data is transmitted to the Service via an Internet connection and stored:

- locally on the device;
- in the cloud, if the device is associated with the service, in cloud databases located within the European Union, managed in accordance with personal data protection regulations.

Data retention is determined based on the type of product and the user account lifecycle.

Furthermore, if the user removes the App from their device, some local data may be lost due to the nature of the operating system backups.

When the user deletes their account, resets, and/or disconnects the device, all collected data is irreversibly deleted. After that point, any requests for access or data transfer cannot be fulfilled.

6. Use by the data controller

The Data Holder may use the data generated by the products, readily available and collected through the service, for the following purposes in accordance with the contractual terms and the information provided to the user:

- continuous improvement of the Service and Products;
- predictive maintenance and technical diagnostics;
- IT security and prevention of abuse;
- aggregate statistical analysis and development of new features;
- resolution of malfunctions reported by the user
- User profiling if authorized in accordance with EU Regulation 2016/679.

The data may be shared with the following third parties:

- cloud infrastructure providers;
- technical support companies authorized by NICE S.p.A. or Group companies;
- technology partners and developers involved in the development, testing, or updating of products and the App;
- cybersecurity consultants, for audit and security purposes;
- installers of Nice S.p.A. products or Group companies.

Such sharing will take place exclusively for purposes compatible with those declared to the user for purposes related to the proper functioning of the service and compliance with current legislation on data and personal data that guarantees compliance with applicable legislation, including the protection of personal data.

7. User's right of access

The User has the right to access the data generated by the use of the connected Product and the related Service (the "Data"), including the metadata necessary for their interpretation and usability, in accordance

with Articles 4 and 5 of the Data Act. This right is not absolute and may be subject to limitations based on the provisions of the law as indicated in this policy.

If the Data is not directly accessible from the device or application, the Data Holder may make it available without undue delay, in a complete, structured, commonly used, and readable format.

Where technically feasible, the data will be provided in a timely manner, in conditions of security, integrity, and equal quality to those available to the holder.

The Data will be provided in the format indicated above, together with metadata, in accordance with the interoperability requirements of the Data Act (Article 4(1)).

8 . Extension to related service data

The above rights also extend to data generated or processed by the related service (such as mobile apps, cloud interfaces, or other local/remote systems), within the limits of the provisions for "related service data" in the Data Act.

9. Portability to third parties

The User also has the right to obtain the direct transmission of the Data contained in the Cloud to a third party indicated by him/her, without undue delay, in a structured, interoperable, commonly used and machine-readable format and, where technically possible or where it does not involve a manifestly disproportionate effort, in real time (Article 5(1) of the Data Act).

The transmission methods, as well as the availability of historical data, depend on the type and model of the device, the connection used, and the communication protocols implemented.

Any requests for clarification or to exercise your rights may be submitted through the official technical support channel by emailing the following address: eudataact@niceforyou.com.

The limitations provided for by applicable law and the paragraph on restrictions remain unaffected.

10. Sharing with third parties and right to revoke sharing

The user may request the sharing of data generated by automations and the Service, as well as related metadata, with third parties selected by the user within the limits set forth in Article 5 of the Data Act, through a specific feature available in the App in accordance with the product's technical specifications. Users may **revoke** their consent to sharing **at any time** using the same method. Revocation takes effect **immediately,** without prejudice to the lawfulness of processing based on consent given prior to revocation.

11. Limitations, conditions, and protection of trade secrets and company know-how

11.1 – Restrictions under the Data Act

NICE, as the Data Holder, data holder), while respecting the User's rights under the Data Act, may limit or refuse access, portability, or sharing of certain Data in the following cases:

- if the disclosure of the Data may result in a violation of the fundamental rights or freedoms of third parties, including the protection of the personal data of other individuals (Article 4, paragraph 6);
- if the requested access may lead to the disclosure of trade secrets, confidential know-how, or strategic information, or compromise the cybersecurity or integrity of digital infrastructure (Art. 4, paras. 6 and 7);
- if processing the request involves a technical effort that is manifestly disproportionate to what is reasonably necessary to extract and provide the requested Data (Art. 4, paras. 3 and 7).
- If disclosure of the data is not possible due to the fact that the data is not stored by NICE based on the technical characteristics of the product, or due to the fact that the data has been permanently deleted

as a result of the product being disconnected from the user's account or the user's account being deleted.

11.2 – Transparency regarding refusal of access or sharing

In the event of total or partial refusal of access, transfer, or sharing of the requested Data, the Data Holder will provide the User with a written and reasoned communication containing:

- the specific reasons for the refusal;
- an indication of the categories of data affected by the restriction;
- the regulatory and technical references on which the decision is based.

11.3 – Exceptions and guarantees

Any restrictions will be adopted in accordance with the principle of proportionality, assessing on a case-by-case basis the balance between the User's rights and the interests protected by the Data Holder , with adequate internal documentation of the reasons.

The User retains the right to:

- receive a documented response to the request;
- lodge a complaint in accordance with the internal procedure for exercising rights;
- refer the matter, where applicable, to the competent supervisory or judicial authorities.

11.4 – Protection of trade secrets

If the Data generated by the Products and the Service includes, in aggregate or structured form, information covered by trade secrets pursuant to applicable law and Article 4 of the Data Act, NICE will adopt appropriate technical and contractual measures to ensure the protection of such secrets, including (by way of example):

- signing of confidentiality agreements (NDAs);
- adoption of secure and profiled access protocols;
- application of sector-specific codes of conduct or selective authorization procedures;
- selective filtering of shared Data, using pseudonymization or anonymization techniques

If the User fails to comply with the agreed measures or engages in conduct that compromises the confidentiality of trade secrets, the Data Holdermay suspend or limit the sharing and access of the Data concerned, subject to written notice.

12. Complaints

The user has the right to lodge a complaint with AgID, as the competent national agency designated pursuant to Article 37 of the Data Act, if they believe that there has been a violation of the provisions of Chapter II of the Data Act.

The Services offered pursuant to Articles 3(2) (Connected Products) and 3(3) (Related Services) may generate the following types of data.

See table below.

Type of data accessible to the user – Data Act (Access, Legal basis, Restrictions, Format, Interoperability)

DATA CATEGORY	DESCRIPTION	EXPECTED ACCESS to the user	LEGAL BASIS	REASON FOR THE RESTRICTION	FORMAT	INTEROPERABILITY
Data from the hub endpoint (Swagger/API)	Technical data accessible via API	User	Articles 4 and 5 of the Data Act + user agreement	None	JSON or any other user-readable format	REST API or GraphQL
Endpoint for analysis	Collection point for system analysis	User	Art. 4 and 5 Data Act + user	None	JSON or any other user-	REST API or GraphQL

DATA CATEGORY	DESCRIPTION	EXPECTED ACCESS to the user	LEGAL BASIS	REASON FOR THE RESTRICTION	FORMAT	INTEROPERABILITY
			agreement		readable format	
List of recorded events: **A. Device status** **B. Energy data** **C. Action-related events** **D. Alarm events** **E. Installer events (for hub admin)**	Device event log	User	Art. 4 and 5 Data Act + user agreement	None	JSON or any other user-readable format	REST API or GraphQL
	Operating status (on/off, temp, batteries)	User	Art. 4 and 5 Data Act + user contract	None	JSON or any other user-readable format	REST API or GraphQL
	Power, consumption,	User	Art. 4 and 5 Data Act + user contract	None	JSON or any other user-readable format	REST API or GraphQL
	Deleted/modified scenes/images	User	Art. 4 and 5 Data Act + user agreement	None	JSON or any other user-readable format	REST API or GraphQL
	Security notifications or events	User/installer	Art. 4 and 5 Data Act + user agreement	None	JSON or any other user-readable format	REST API or GraphQL
	Installer activity log	Admin hub + Installer End users cannot access logs; logs can be provided in pseudonymized or aggregated form	Contract or legitimate interest of the controller to track activity	These logs contain personal data (name, email, activity) and potentially security information (administrative access).	JSON or any other user-readable format	REST API or GraphQL
List of devices and configurations	Name, room, parameters, notification sets, connections to other devices,	User	Art. 4 and 5 Data Act + user contract	None	JSON or any other user-readable format	REST API or GraphQL
List of automations	Automation name, room (e.g., living room, garden), status (active/inactive), type (security, lighting, etc.), blocks, or scene sequences, or scenes representing actions	User	Art. 4 and 5 Data Act + user contract	None	JSON or any other user-readable format	REST API or GraphQL

DATA CATEGORY	DESCRIPTION	EXPECTED ACCESS to the user	LEGAL BASIS	REASON FOR THE RESTRICTION	FORMAT	INTEROPERABILITY
List of installed integrations	Integration name Manufacturer Active/inactive status	User/Installer	Art. 4 and 5 Data Act + user contract	In the case of NDAs with third-party suppliers, only the functional description is provided.	JSON or any other user-readable format	REST API or GraphQL
Programming list	Timers, event time slots	User	Art. 4 and 5 Data Act + user contract	None	JSON or any other user-readable format	REST API or GraphQL
Climate data	Temperature/humidity readings humidity	User	Art. 4 and 5 Data Act + user contract	None	JSON or any other user-readable format	REST API or GraphQL
Irrigation data	Irrigation frequency and consumption (verification)	User	Art. 4 and 5 Data Act + user contract	None	JSON or any other user-readable format	REST API or GraphQL
Network settings	IP, DNS, Wi-Fi...	User Installer/administrator	Art. 4 and 5 Data Act + user agreement	IT security Possible IT security risk	JSON or any other user-readable format	REST API or GraphQL
User settings (hub)	ID, preferences, email hash	User, data is only available to the account holder and cannot be transferred to third parties.	Art. 4 and 5 Data Act + user agreement	None	JSON or any other user-readable format	REST API or GraphQL
Normal user data	Basic preferences and scene history	User	Art. 4 and 5 Data Act + user agreement	None	JSON or any other user-readable format	REST API or GraphQL
Hub data (admin)	Hub data + ID + locale + cloud + phones added to the account with the associated hash and name.	Admin and Owner	Art. 4 and 5 Data Act + user agreement	None	JSON or any other user-readable format	REST API or GraphQL
Backup list	Configuration copies What else is in the backups	User + Installer	Art. 4 and 5 Data Act + user agreement	None	Depends on the device	None; each device supports its own format
List of installers and monitoring	Names, emails, logged accesses	Nice, if it is necessary to provide data, it will be pseudonymized	Contract and security obligations	Access only by NICE as data controller, protection of installers' privacy	JSON or any other user-readable format	REST API or GraphQL

Table – Data not accessible to the user (pursuant to the Data Act)

DATA CATEGORY	DESCRIPTION	EXPECTED ACCESS	LEGAL BASIS	REASON FOR RESTRICTION	EXPECTED FORMAT	INTEROPERABILITY
Low-level logs (operating system)	Technical logs generated by operating system components.	Not accessible to the user	Art. 4(6)-(7) Data Act + NDA/confidentiality	Know-how	N/A	Not applicable
Chip data	Information about integrated chips and firmware	Not accessible to the user	Art. 4(6)-(7) + Third-party NDAs	Know-how: subject to NDA for advanced support	Not disclosable	Not applicable
Integration/automation code	Source code for scenes or automations	Not accessible to the user	Art. 4(6)-(7)	Know-how: includes proprietary API calls, encrypted elements	Not disclosable	Not applicable
Uncompressed backups (cloud/hub)	Archived system copies without compression	Not accessible because they include sensitive configurations and authentication data	Art. 4(7) + security	Security:	Not disclosable	The user does not have the decryption key
Information about passwords, PINs, or hashes	Encrypted authentication data	Not accessible	Art. 4(6)-(7) + security	Security: access permitted only via login	Not disclosable	Not accessible
Installer data	Personal and professional data (e.g., telephone, email, installed hubs)	Not accessible to the end user	GDPR + Art. 4(6) Data Act	Privacy protection (GDPR)	No legal basis for disclosure	Access restricted to administrator
Certificates	Digital certificates used for authentication or encryption	Not accessible	Art. 4(7) + security	Security	Not disclosable	Not accessible
Token	API or session authentication token	Not accessible	Art. 4(7) + security	Security:	Not disclosable	Not accessible
Aggregated analytical data	Anonymous data aggregated from multiple users	Not accessible after irreversible anonymization process Not traceable to the user	Art. 4(6) Data Act	Know-how	Not disclosable	Internal company use
Data not stored or irreversibly deleted after the retention period	Device data not stored, data stored and deleted after the maximum	Not accessible because it has been irreversibly	Art. 4(7) + security	Data no longer present based on the specifications of individual	Not applicable	Not applicable

DATA CATEGORY	DESCRIPTION	EXPECTED ACCESS	LEGAL BASIS	REASON FOR RESTRICTION	EXPECTED FORMAT	INTEROPERABILITY
	retention period, data relating to users who have dissociated devices from their account, have not associated the device with their account, have deleted their account resulting in the irreversible deletion of data.	deleted or is present in an anonymous aggregate form and therefore cannot be attributed to the user		devices or users' deletion choices. If present, the data has been irreversibly anonymized.		