

EU Data Information Notice	Information Notice Category	Date updated	Version
InVue Access Portal, InVue Connected Solutions	Connected product and related service(s) to a connected product].	23/07/2026	01

Manufacturer/Distributor	Service Provider
InVue Security Products, Inc.	InVue Security Products, Inc.
Geographical/physical address	Geographical/physical address
9201 Baybrook Lane, Charlotte, NC, 28277, United States	9201 Baybrook Lane, Charlotte, NC, 28277, United States

Data Information Notice

Introduction

General

This information notice explains how data generated by, or collected through, InVue's Access Portal (the “**Product**”) is accessed, used, and shared [(including to provide event data collected from InVue connected solutions (the “**Service**”))] and how the data is otherwise processed, in line with the requirements under Article 3 of the EU Data Act.

Product and service description

InVue's Access Portal (the "Portal") is a software-as-a-service (SaaS) solution designed for retail companies and intended to provide access control capabilities to better manage access to secured retail merchandise and streamline the consumer experience.

The Portal allows retailers to manage the access that their employees have to security devices and the merchandise these devices are securing. In doing so, the Portal gives retailers a means to limit internal merchandise loss, monitor activity related to security devices, and evaluate opportunities to drive efficiency within store operations.

Additionally, retailers may optionally allow consumers the ability to self-access merchandise through the issuance to temporary digitally issued keys. The issuance and ability to track the utilization of those keys and the security devices they are associated with is provided via the Portal.

InVue's connected solutions (ie: LIVE Locks product family or similar Bluetooth, NFC, or other technically enabled products) generate event data which is captured within the Portal for customers who subscribe to

the Portal SaaS offering. The data includes, but is not limited to, lock / unlock activity, device settings, firmware settings on the device(s), battery status, diagnostic indicators, and details on the retail employees who have engaged with the connected solution.

Data holders

The following parties receive data from the Product and/or the Service and may use the data for their own purposes ('data holders'):

InVue Security Products, Inc.

Retail customer of the product and related services

Terms of use and quality of service

InVue's Access Portal and related connected solutions are covered by Terms of Use, including SLA and Privacy Statements, provided to the customer upon purchase of the product and service.

Data which the Product is capable of generating

Nature of data	Format	Estimated volume	Collection frequency	Data retention
User login activity, key issuance detail, audit activity of changes to user profiles, device meta data, roles and permissions	JSON, Txt	Minimal kb per usage	In real-time	Event data is maintained for the lift of the retailer's subscription. Other data is retained for a default value of 90 days, to a minimum of 30 days, and a maximum of 365 days, as defined by the retailer.

Data obtained by Related Service

Nature of data	Format	Estimated volume	Data retention
Event data including activity logs. Diagnostic data, firmware version, battery status, error	JSON, Txt	Minimal kb per usage	Event data is maintained for the lift of the retailer's subscription.

Nature of data	Format	Estimated volume	Data retention
codes, and related information operational information			Other data is retained for a default value of 90 days, to a minimum of 30 days, and a maximum of 365 days, as defined by the retailer.

Data sharing and use

Type of data	Data use	Sharing of data	Identity of data recipient
User data	None - for retailer's use only	Not shared with 3rd parties	N/A
Diagnostic and technical data and logs	Data can be shared with service provider for internal development of technical improvements to product and services, or via initiated support request by retail customer / user	Not shared with 3rd parties	N/a

Data access and user capabilities

Direct access to data	Indirect access to data	Erasure of data
Retail customer has access to all data generated by, and captured within, the Product	Retail customers can access data directly from within the Product. Data accessible within the Product's screens, as downloadable CSVs and PDFs, and/or via direct API access	The system allows a customizable retention period for non-event data, to a minimum of 30 days and a maximum of 365 days, defaulting to 90 days, until customer ends contract and SaaS subscription

How to request data sharing

As policy, InVue Security Products, Inc does not share customer data with third parties. Our customers are able to share data with third parties directly on their own, based upon the ability to download and extract their data from the Product, as provided by InVue.

Right to lodge a complaint

If you believe our handling of your data infringes your rights under applicable legislation, you have the right to lodge a complaint with the competent authority in your jurisdiction.

Trade secrets

In some cases, data from the connected products or related services may include trade secrets that we or our partners own. Trade secrets shall be preserved and disclosed only where all necessary measures prior to preserve their confidentiality are taken, in particular regarding third parties. In exceptional circumstances, our ability to grant access to data may be limited due to trade secrets.

Term and termination

Your contract with the Service Provider is valid per the effective date and term of the applicable agreement.

You may end the contract by following the steps set forth in the termination clause of you're applicable agreement.

Contact information

Should you have any questions regarding the data generated by the Product or the Service, do not hesitate to contact us at Legal@invue.com.