12th September 2025 – Version 1

Data Information Notice

Information notice for SecureWave and SecureComm.

Manufacturer: HKC Security Ltd., Parkway Business Centre, Ballymount, D24 WY49, Ireland

Service provider: Security & Risk Communications Ltd., Parkway Business Centre, Ballymount, D24 WY49, Ireland

Introduction

General

This information notice explains how data generated by, or collected through, the SecureWave (the "**Product**") is accessed, used, and shared (including to provide SecureComm (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

HKC SecureWave is a family of hybrid control panels, keypads, expanders, and wired/wireless detection devices using the SecureWave two-way wireless protocol, designed for EN Grade 2 professional security installations. It supports intruder and life safety detection, partitioned system configurations, and integration with monitoring services. HKC SecureComm is the associated managed cloud service providing secure IP/GSM connectivity for alarm signalling, remote user access, event notifications, video verification, configuration, diagnostics, and over-the-air updates. Together, SecureWave hardware and SecureComm cloud services form an end-to-end security solution combining reliable on-premises detection with remote connectivity, management, and maintenance. Data is generated as the Product and Service is used, with data being stored in the SecureComm cloud service.

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'):

- HKC Security Ltd., Parkway Business Centre, Ballymount, D24 WY49, Ireland
- Security & Risk Communications Ltd., Parkway Business Centre, Ballymount, D24 WY49, Ireland

The product can also be maintained, updated and configured by an installation provider at the request of the product owner. In such cases, the installation provider may also be a data holder.

Terms of use and quality of service

SecureComm T&Cs are provided upon signup, SecureWave T&Cs can be provided by the installation provider during installation.

Data which the Product is capable of generating:

Product name	Nature of data	Format	Estimated volume	Collection frequency	Data retention
SecureWave family of products, SW-10270, Quantum 70 & SecureHub,	Activity logs, arm and disarm events, system faults, remote access, firmware upgrades, communication faults, Alarm and tamper events, remote maintenance.	Text. PDF.	10KB of data generated per week is typical for the product.	The system generates and logs new data as it is interacted with, and depending on the service level of the remote service.	Data is stored on the device until overwritten using the first-in, first-out (FIFO) method.

Data obtained by the Service:

Service name	Nature of data	Format	Estimated volume	Data retention
SecureComm	User interaction logs, system status and diagnostic logs.	Text. PDF.	Up to 10KB of data generated per week is typical for the product if requested by the user.	Indefinitely

Data sharing and use:

Type of data	Data use	Sharing of data	Identity of data recipient
Performance and diagnostic data	The data is used to assist in technical support queries during installation or maintenance.	The data is shared with a third party only as outlined in the Data Use section.	The installation provider.

Data access and user capabilities

Direct access to data	Indirect access to data	Erasure of data
The system owner can view activity logs, arm and disarm events, system faults, remote access, firmware upgrades, communication faults, alarm and tamper events, remote maintenance from within the end user app. These can be extracted from within the end user app.	The system owner can request data from the manufacturer for data obtained by the service. The installation provider can provide data generated by the product.	The system owner can request data be removed from the service by the service provider. The installation provider can erase data generated by the product.

How to request data sharing

You may request that data obtained by the service be shared with a specific third party by submitting a formal written request to dataact@hkc.ie. Your request should include:

- The service concerned including installation reference.

Please note:

- **Limitations** – Requests may be refused or restricted where sharing would compromise system security, expose sensitive infrastructure details, breach contractual obligations, or conflict with applicable law.
- **Response time** – We will acknowledge your request promptly.

You may request that data generated by the product be shared with a specific third party by submitting a formal written request to your installation provider.

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.

We maintain confidentiality obligations to protect any trade secrets contained within your data.

Term and termination

Your End User License Agreement for the Service is valid for the duration you use the Service, beginning on the date you sign up or otherwise agree to the Terms of Use of the Service.

You may end the contract by following the steps set out in the Termination clause of your 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 dataact@hkc.ie.