EXOR HMI - EU DATA ACT - ART.3.2

1. General Disclaimer

The EXOR HMI device is not an end-user product and it is not intended for direct sale as such to end-users, but should be completed with additional custom software applications, based on the specific needs and use cases of end-users, and integrated with existing equipment and machinery in different technical contexts. the EXOR HMI device must be appropriately configured, programmed, completed with additional custom software applications, and integrated into larger systems, exclusively by expert personnel.

The EXOR HMI device as such generates only base system and authentication logs, base system configuration files, and cryptographic keys and certificates to be used for secure communications and authentication purposes, as described in next section. No other data is generated, collected, or processed by the EXOR HMI device prior to its configuration and programming by expert personnel.

The heterogeneity of possible application scenarios for the EXOR HMI device, the different types of additional custom software applications that can be created and installed on the EXOR HMI device, and the different types of equipment and machinery with which the EXOR HMI device can be integrated, make it impossible to predict in advance the specific data that will be generated, collected, or processed by the EXOR HMI device after its configuration and programming by expert personnel; only who configures and programs the EXOR HMI device may determine the specific data that will be generated, collected, or processed by the device in each specific use case, through the additional custom software applications that they created and/or installed on the EXOR HMI device, and through the specific equipment and machinery with which the EXOR HMI device is integrated, including the cloud services that the expert personnel may decide to connect the EXOR HMI device to.

Therefore, through its configuration and programming, the EXOR HMI device transforms into a different product (either an end-user product or a component of an end-user product performing specific functions for specific use cases). If such product is placed on the market, it will be the responsibility of the party placing it on the market to comply with all applicable laws and regulations, including but not limited to the EU Data Act.

2. Data Generated, Collected, Or Processed By The Exor Hmi Device Prior to Its Configuration And Programming (Art. 3.2 EU Data Act)

2.1. *(a) The Type, Format And Estimated Volume Of Product Data Which The Connected Product Is Capable Of Generating.* The EXOR HMI device is capable of generating the following types of product data prior to its configuration and programming by expert personnel:

- Base system logs: text files in standard log format, containing information about system events, errors, and warnings. Estimated volume: approximately 1 MB per day, depending on system activity.
- Authentication logs: text files in standard log format, containing information about user login attempts, successful and failed authentications. Estimated volume: approximately 500 KB per day, depending on user activity.
- Base system configuration files: text files in standard configuration file format, containing information about system settings and parameters. Estimated volume: approximately 100 KB.
- Cryptographic keys and certificates: binary files in standard key and certificate formats (e.g., PEM, DER), used for secure communications and authentication purposes. Estimated volume: approximately 50 KB.

2.2. *(b) Whether The Connected Product Is Capable Of Generating Data Continuously And In Real-Time.* The EXOR HMI device is capable of generating base system logs and authentication logs continuously and in real-time, as system events and user activities occur. The generation of base system configuration files and cryptographic keys and certificates is not continuous or real-time, as these files are created or updated only when system settings are changed or new keys/certificates are generated.

2.3. *(c) Whether The Connected Product Is Capable Of Storing Data On-Device Or On A Remote Server, Including, Where Applicable, The Intended Duration Of Retention.* The EXOR HMI device is capable of storing data on-device. By default, system logs are not persistent and are stored in the device's RAM. They use a circular buffer, the size of which is visible through the System Settings (Logs section). These logs are lost when the device is shut down or restarted. Authentication logs, and more generally all security-related logs, are persistent by default and also configurable. They are stored in the device's internal storage, with a default retention period that depends on the size of the configurable circular buffer, accessible within the Logs section of the System Settings. These logs can be exported to an external device. The base system configuration files and cryptographic keys/certificates are also stored on-device, with no automatic deletion; these files remain until they are manually modified or deleted by expert personnel.

2.4. *(d) How The User May Access, Retrieve Or, Where Relevant, Erase The Data, Including The Technical Means To Do So, As Well As Their Terms Of Use And Quality Of Service.* Given their nature of programmable devices, EXOR HMI devices are provided with full access to the hardware and software features of the device, including the ability to access, retrieve, and erase data stored on the device by expert personnel through the following technical means:

- SSH access: Secure Shell (SSH) protocol can be used to remotely access the device's command line interface, allowing expert personnel to navigate the file system, retrieve log files, configuration files, and cryptographic keys/certificates, and delete or modify these files as needed
- web interface: The EXOR HMI device may provide a web-based interface that allows expert personnel to access and manage the device's data, and install and configure additional custom software applications

- USB connection: The device may support USB connections, allowing expert personnel to connect the device to a computer and access its internal storage directly to retrieve or erase data.

  It is the sole responsibility of expert personnel configuring and programming the device to disable or restrict access to these technical means for their end-users, pursuant to applicable laws and regulations, including but not limited to the EU Data Act, and depending on the specific use case and application scenario of the EXOR HMI device.