Product-Specific Notice

EVOLV EXPRESS® PRIVACY NOTICE

Last Updated: September 4, 2025

About this Notice

Evolv Express® (the "Product") is a concealed weapons detection solution with on-premises and cloud components. This Product-Specific Notice is intended to help Evolv users and customers better understand some of the Product's privacy-related features and functions. All information processing is carried out in accordance with our Data Processing Addendum ("DPA") and Privacy Policy, and aligns with applicable data protection laws. If there is a conflict between this Product-Specific Notice and the Privacy Policy, this Notice will prevail. For more information on Evolv's privacy practices, please visit: www.evolvtechnology.com/privacy.

Information Processing

The Product limits the amount of personal data collected and processed to what is necessary to provide the service. In fact, the Product only collects or processes three categories of Personal Data:

Category	How the Data is Obtained:	Purpose
Images	Images of individuals who walk through the Product's physical equipment towers are automatically collected with Product's use.	• The Product uses images to provide an on-screen indication of which individual alerted and the area of the potential threat. • Evolv Customers who opt-in can receive images in the MyEvolv Portal and mobile app. • With Customer consent, images may be collected and processed in a limited manner to improve product functionality. ***Visitor images are the only form of PII (as deemed by some privacy standards) collected by Evolv Express. Evolv does not associate any personal information with this image or use any biometric data or facial recognition technology.***
Customer User Information	Customer may provide name, email address, and phone number.	• Evolv uses contact information of Customer users to enable the creation of accounts and logins to the relevant Evolv Applications. • Evolv also collects phone numbers and emails from Customers who would like their personnel to receive notifications (including MFA notifications) about alerts from the Product.
Location Information	The location of the physical product may be assigned, designated, and/or accessed.	• The on-premise equipment location is assigned by Evolv on install, and a secondary location may be designated by the Customer to permit the Customer to understand where the equipment is located at the Customer's site. • Customers can also opt-in to turn on a GPS feature on Gen2 which will make the location visible to authorized Evolv service personnel.
Collectively, the above information is referred to as, "Customer Personal Data." Customer Personal Data is available for its intended purposes on the physical Product, its tablet, and/or through its applications, including the MyEvolv Portal, MyEvolv Mobile App, the Bridge Community, and Evolv Insights® ("Evolv Applications").		

Data Retention

Customers have a choice on what Personal Data to retain. In addition, Customers & their visitors may request Evolv to delete their Personal Data at any time. This includes Customer User Information which, unless requested, will be retained.

Images on Product's Computer ("Scanner"):

Based on the retention setting option selected by Customer, if images are selected to be retained, they are retained for no more than 30 days.

Images on Product's Tablet(s):

The latest 100 alert images are available on the tablet; all images are automatically deleted when the power to the tablet is turned off.

Images on MyEvolv Portal & MyEvolv Mobile App:

Subject to the Customer opting-in, images are retained on the MyEvolv Portal and/or mobile app for 1-14 days, at Customer's discretion.

Privacy Protective Features and Privacy Compliance

The Product employs the following privacy-protective and compliance-related features:

- The Product by default only collects the personal data set forth above. Customers may opt to store less information through the Data Retention options.
- Images of individuals are not identified by name and the Product does not know (or seek to discover) the name or any other identification information of any individual.
- The Product does not process or analyze individuals' physical characteristics such as race, hair color, height, or weight.
- Customers have sole control over whether images from the Product are transferred to the Customer's own video management system ("VMS"), or other security application, or downloaded from the Evolv Applications. Any further processing of personal data after such a transfer is at Customer's sole election. Evolv does not take part in any such further VMS data processing.
- Evolv complies with international cross-border data transfer protections as set forth in the DPA.

Access Controls

Provisioning and deprovisioning of new users can be managed exclusively either by Evolv or by customer's federated identity mechanisms. Evolv applies access controls to restrict which Evolv personnel can access Personal Data. Customers have permission settings to limit the level of access their users have to and in the Evolv Applications and to the Product.

Encryption and Other Security Measures

- The Product is co-located in AWS tier-1 datacenters with industry standard certifications. Further detail is available at the following links:
    - AWS Security Website
    - AWS overview of security processes

- AWS employs state-of-the-art security measures as required by ISO 27001 and SOC 2 Type II standards.
- Evolv uses industry-standard encryption technologies to secure Personal Data for both the on-premises data and data stored on AWS.
- Evolv maintains a written information security program designed to protect the security and confidentiality of Personal Data, including to protect against any anticipated threats or hazards to the security and integrity of Personal Data and ensure the proper disposal of PII.
- Security awareness training is provided to all Evolv personnel.
- While AI and machine learning are the core of Evolv's automated threat detection capabilities, Evolv does not source or train its models on Customer data inputs. Evolv's machine learning models are independently developed,, proprietary to Evolv, and tested for accuracy.. Evolv's use of AI and machine learning does not involve Generative AI, nor automated decisions about human subjects.
- Evolv has a formal training program for all employees on the responsible use of AI.
- Evolv maintains a written incident response plan that includes procedures to be followed in the event of any incident that results in a breach of Personal Data.
- Post deletion and decommissioning, Evolv applies industry strength data destruction practices to Express storage media.

Subprocessors

The Product software is hosted at AWS's industry-standard data centers in the US.

For a list of our Subprocessors, please visit the Resources section below or visit www.evolvtechnology.com/privacy.

Evolv requires Subprocessors to agree to data protection terms to protect personal data they process on Evolv's behalf.

Resources

- Evolv Privacy Policy
- Evolv Data Processing Addendum
- Evolv Subprocessor List (available to Customers only)

This document is provided for informational purposes only, does not constitute an agreement between Evolv and any third party, and does not create any warranties or obligations on behalf of Evolv or its suppliers or customers. This document represents Evolv products as of the effective date referenced above and is subject to modification, revision, or withdrawal at any time.