Zebra Technologies’

AI Acceptable Use Policy

This Zebra Technologies’ AI Acceptable Use Policy (“***AUP***”) governs the use of Zebra’s AI-powered products and solutions (“***Zebra AI***”). Zebra AI may include generative artificial intelligence, agentic elements, or machine learning components (“***AI***”) for use by companies under an agreement with Zebra (each, a “***Customer***”).

This AUP forms part of the contractual relationship between Zebra and the Customer. Customers are responsible for ensuring that end users use Zebra AI in accordance with Customer policies and this AUP. Zebra is committed to offering AI in accordance with its AI Principles of Accountability, Ethical Purpose, and Responsibility.

This AUP may be updated periodically. Customer’s continued use of Zebra AI following any published updates will constitute acceptance of those changes. For any questions, Customers should contact its Zebra sales support representative.

Permitted Uses and Acceptable Use Cases

Customers may permit use of Zebra AI solely for the documented intended purposes specified in its agreement with Zebra. Zebra AI may not be further integrated into third-party systems. If no intended purpose is expressly specified in the Customer’s agreement with Zebra, the permitted uses will be:

- Documented business-related chat, search, and machine/computer vision functionalities.
- Leveraging tools made available to members of Zebra’s PartnerConnect program.
- Internal testing or proof-of-concept usage aligned with Customer’s business and in compliance with this AUP.

Prohibited Content and Behavior

Customers and end users must not facilitate, permit, or enable the use of Zebra AI to generate or effectuate:

- **Fraudulent, Misleading, or Disinformation**, including, but not limited to, spam, scams, phishing, or malware; purposefully false statements or misleading information.
- **Inappropriate Content**, including, but not limited to, sexual innuendo or content; offensive or insensitive language or innuendo; harmful or violent language or depictions.
- **Unauthorized Access**, including, but not limited to, attempting to gain unauthorized access to a system or account; targeting or tracking a person’s location, behavior, or communication.
- **Disclosure of Private Information**, including, but not limited to, sharing a person’s personal data, including healthcare and medical information; sharing images, video, or content depicting another person without their permission.
- **Disruption of Zebra AI**, including, but not limited to, excessive or automated use that disrupts normal operation; intentional load testing or attempted bypass of Zebra-enabled sensitivity controls or restrictions.
- **Violation of Intellectual Property Rights**, including, but not limited to, any misuse of a third party’s intellectual property or confidential information.

Prohibited AI Practices

Customers must not facilitate, permit, or enable use of Zebra AI in ways that violate any applicable law or the EU AI Act's rules on prohibited AI practices. These prohibited uses include, but are not limited to, using Zebra AI to:

- Exploit vulnerable individuals or manipulate behavior through subliminal techniques.
- Implement any form of social scoring system or any use that results in discrimination.
- Conduct or support individual predictive policing based on profiling or behavioral data.
- Perform untargeted scraping of facial images.
- Use emotion recognition in workplaces or educational settings.
- Use biometric categorization to infer race, political views, religion, sexual orientation or any other protected class or segment.
- Enable real-time remote biometric identification in public spaces on behalf of law enforcement.
- Enable use cases that result in unlawful, unfair or discriminatory algorithmic bias or differential treatment.

Collectively, referred to as "***Prohibited AI***."

Restricted (High-Risk) Use Cases

The use cases below are considered high-risk under the EU AI Act and similar laws and regulations. Zebra AI is not designed or intended for any high-risk use cases described in this AUP. Customer assumes all responsibility for compliance with applicable laws and regulations. Zebra AI may not be used for any of the following purposes:

- Safety components of products which require any form of third-party conformity assessment.
- Enable remote biometric identification systems.
- Support or enable critical infrastructure projects, such as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.
- Education or vocational training.
- Independently determine employment, workforce management, or access to self-employment/gig work.
- Qualify access to essential private or public services / benefits.
- Perform functions of law enforcement, migration, asylum, border control, administration of justice or systems impacting democratic processes.
- Direct political campaigns or election-related activities.
- Perform legal interpretation or decision-making.
- Determine healthcare provision or diagnostics.
- Make direct automated financial decisions, eligibility assessments, credit scoring or automated decisions that produce legal or similarly significant effects.
- Determine employment or housing eligibility assessments.

Collectively, referred to as "***High-Risk AI***."

ANY USE OF ZEBRA AI FOR PROHIBITED AI OR HIGH-RISK AI PURPOSES IS AT CUSTOMER'S SOLE RISK. ZEBRA HEREBY DISCLAIMS ALL LIABILITY FOR SUCH USES BY CUSTOMER.

ZEBRA'S CUSTOMER ASSUMES FULL RESPONSIBILITY FOR ANY SUCH USE OF ZEBRA AI IN VIOLATION OF THIS AUP OR CUSTOMER'S AGREEMENT WITH ZEBRA. ZEBRA DOES NOT AUTHORIZE SUCH USES AND MAY TERMINATE AGREEMENTS OR REPORT VIOLATIONS TO AUTHORITIES IF MISUSE IS DETECTED.

Customer Responsibilities

Customers are solely responsible for:

- Providing appropriate notices and training to end users on the responsible use of AI.
- Ensuring compliance with all applicable laws and regulations.
- Ensuring that any training materials or input data used with Zebra AI are lawfully obtained and appropriately vetted.
- Using Zebra AI only for documented intended purposes in a manner that supports the legitimate business objectives of Customer in a responsible manner.
- Verifying the accuracy and appropriateness of Zebra AI outputs.
- Implementing human oversight where appropriate or mandated.
- Conducting a risk assessment or undertaking a Data Privacy Impact Assessment, as appropriate, if Zebra AI is processing sensitive data.
- Use of Zebra AI in any way that constitutes unfair or deceptive acts or practices under Section 5 of the U.S. Federal Trade Commission Act.
- Use of Zebra AI in any context involving children under 13 years of age.
- Disclosing where AI-generated content is generated and obtaining any necessary end user consent.
- Reporting any use cases or misuse of Zebra AI, including violations of this AUP and any Zebra AI-related incidents or breaches.
- Creating and enforcing internal policies to ensure end user's compliance with this AUP.
- Maintaining documentation of Zebra AI usage where required by applicable law.

Violations of this AUP

Zebra may suspend or terminate access to Zebra AI for violations of this AUP. Zebra may, at its discretion, provide notice and an opportunity to remedy the violation. Zebra reserves the right to act immediately in cases of misuse or uses that violate any law, regulation, or Zebra's agreement with Customer.

Version: 1.0

Effective Date: August 4, 2025