Technical and Organizational Measures

Overview

This document describes the technical and organizational measures implemented by Zebra Technologies Corporation and its affiliates' (referred herein as "***Zebra***") for information security, privacy, and data sharing practices ("***TOMs***"). Zebra's TOMs are designed to provide an appropriate level of data protection across Zebra's organization, products, services, and solutions, including data provided to Zebra by its customers ("***Customer Data***").

Zebra has considered information security practices and privacy laws and regulations from around the world in developing its information security compliance programs. These practices, laws, and regulations include International Organization for Standardization ("***ISO***") controls and numerous U.S. and global privacy laws, such as the European Union's ("***EU***") General Data Protection Regulation ("***GDPR***"), the United Kingdom's ("***UK***") Data Protection Act 2018 and the UK GDPR, the California Consumer Privacy Act ("***CCPA***"), Canada's Personal Information Protection and Electronics Documents Act ("***PIPEDA***"), and the Brazilian General Data Protection Law ("***LGPD***"). Zebra's TOMs are shared to demonstrate the steps Zebra has taken to develop a comprehensive information security program. These steps include:

- Monitoring, assessing, and improving security and privacy controls across the organization on an ongoing basis
- Assessing the privacy impact of new technologies developed or implemented by Zebra
- Ensuring that in all Zebra processing activities, the rights of data subjects are able to be respected
- Implementation of information security controls and privacy policies, standards, and standard operating procedures
- Ensuring that Zebra's products, services, and solutions are compliant with applicable information security and privacy laws and regulations

A. Global Data Transfer Strategy

Zebra applies a focused and consistent approach to the management of how Customer Data is used and stored globally.

Transfer Risk Assessments

In consideration of the Court of Justice of the European Union's decision in Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems ("***Schrems II***") and the European Data Protection Board's ("***EDPB***") *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, Zebra has developed a six-step international data sharing compliance framework by:

1. Mapping its intra-group and extra-group international transfers
2. Identifying the transfer mechanisms covering those transfers
3. Assessing the protective effectiveness of the transfer mechanisms

The information contained herein, and the statements expressed, are of a general nature and are not intended to address the circumstances of any particular individual or entity. There can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

4. Applying supplementary measures to ensure a level of protection essentially equivalent to the protection offered within the European Economic Area ("***EEA***") and UK
5. Ensuring any formal requirements are met
6. Reviewing its transfer mechanisms periodically (the "***Data Framework***")

The above Steps 3 and 4 of Zebra's Data Framework require Zebra to assess, on a case-by-case basis, the laws of the data recipient's country against the European Essential Guarantees set out in the EDPB's *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*. The European Essential Guarantees are that:

- Processing should be based on clear, precise, and accessible rules
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
- An independent oversight mechanism should exist
- Effective remedies need to be available to the data subject

Where it is assessed that a transfer mechanism is unable to be complied with by the data recipient (for example, because the national security surveillance laws of the data recipient's country are fundamentally inconsistent with the European Essential Guarantees), Zebra implements supplementary contractual, technical and organizational measures to strengthen the transfer mechanism. The nature and volume of data being transferred is also taken into account in this assessment.

Where there are no suitable supplementary measures which can ensure a level of protection essentially equivalent to the protection offered within the EEA or UK, Zebra suspends or terminates such data transfers.

Transfers within Zebra's Organization

All affiliates and subsidiaries of Zebra are members of an intragroup data sharing agreement incorporating lawful transfer mechanisms which have been assessed in light of the Schrems II decision and EDPB guidance. The intragroup data sharing agreement imposes responsibilities on Zebra group members to only share Customer Data when necessary and, when in receipt of Customer Data, to use it in accordance with established privacy practices.

Transfers outside of Zebra's Organization

Zebra implements appropriate data processing agreements which incorporate contractual clauses where appropriate to legitimize the processing of Customer Data undertaken by Zebra. Where a supplier agreement involves the transfer of Customer Data outside of the EEA or UK to a country not deemed adequate by the European Commission, Zebra implements lawful transfer mechanisms which are assessed in accordance with the requirements of the Schrems II decision and EDPB guidance.

B. Information Security Policies and a Commitment to Confidentiality

- Zebra ensures that any employee, contractor, agent, or Zebra supplier who is authorized to access Customer Data is subject to contractual duties of confidentiality. Those personnel or suppliers authorized by Zebra to handle Customer Data are contractually

The information contained herein, and the statements expressed, are of a general nature and are not intended to address the circumstances of any particular individual or entity. There can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

prohibited from disclosing Customer Data without authorization, and Zebra is able to, and will, enforce those obligations where appropriate to do so.

- Zebra maintains and follows information security policies and practices that are integral to Zebra's business and mandatory for all Zebra employees, including contractors, agents, and suppliers. Zebra reviews its information security program regularly and amends policies thereunder as Zebra deems reasonable to maintain protection of Customer Data.
- The underlying principle behind Zebra's information security policies are that all business departments shall meet or exceed the ISO 27001:2013 control requirements unless regulatory requirements or regional laws stipulate otherwise.
- Zebra maintains and follows its standard mandatory employment verification requirements for all new hires. In accordance with Zebra internal processes and procedures, these requirements are periodically reviewed and include proof of identity validation and additional checks as deemed reasonably necessary by Zebra.
- Zebra employees complete regular security and privacy education as set forth by Zebra.

C. Information Security Incidents

Zebra maintains and follows a documented incident response protocol for information security incident handling. This security incident protocol enables Zebra to:

- Quickly identify and escalate security incidents to the appropriate team
- Assess the incident
- Contain the incident to limit or eliminate further loss or damage
- Make any required notifications to regulators, customers, and data subjects
- Log the incident and implement any remedial action to avoid the security incident occurring again in the future

D. Physical Security and Entry Control

- Zebra maintains appropriate physical entry controls, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into Zebra facilities.
- Use of an access badge to enter a Zebra facility is logged. Zebra revokes access to Zebra facilities upon the authorized employee, contractor, agent, or supplier personnel no longer having a valid business need for access. Zebra follows formal documented separation procedures that include prompt removal from access control lists and surrender of physical access badges.
- Any person duly granted temporary permission to enter a Zebra facility is registered upon entering the premises and is escorted by authorized personnel.
- Zebra takes reasonable precautions to protect its physical infrastructure against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

E. Access, Intervention, Transfer and Separation Control

- Zebra maintains documented architecture of networks managed by Zebra. Zebra separately reviews such network architecture for compliance with its standards.
- Zebra maintains measures to prevent Customer Data from being accessed by unauthorized persons.
- Zebra secures Customer Data not intended for public or unauthenticated viewing when transferring Customer Data over public networks.
- If Zebra requires access to Customer Data, Zebra provides such access only to authorized personnel.
- Zebra maintains technical measures including lockout of accounts after multiple sequential failed login attempts and strong password or passphrase authentication.
- Logs in which access and activity are recorded are retained in compliance with Zebra's records retention policy.

F. Service Integrity, Resilience, and Availability Control

To achieve these standards, Zebra:

- Performs penetration testing and vulnerability assessments
- Enlists an independent third party to perform penetration testing
- Performs automated management and verification of underlying components' compliance with security configuration requirements
- Remediates identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact
- Takes reasonable steps to avoid disruption to its business when performing its tests, assessments, scans, and execution of remediation activities
- Maintains policies and procedures designed to manage security risks associated with the application of changes to its organization.
- Maintains an inventory of information technology assets used in the operation of Zebra's business.
- Maintains measures designed to assess, test, and apply security advisory patches to Zebra systems, networks, applications, and underlying components.

G. Information Systems Audit Controls

- Zebra performs audit activities on operational information systems.
- Zebra's audit requirements and activities involving verification of operational systems are planned and agreed to minimize disruptions to business processes.
- Audit requirements for access to systems and data are approved and agreed to by appropriate management.
- The scope of technical audit tests is agreed and controlled.
- Audit tests are limited to read-only access to software and data.

- Access, other than read-only, is only allowed for isolated copies of system files. These files are to be erased when the audit is completed. If there is an obligation to retain these files under audit documentation requirements, they are given appropriate protection and securely stored.
- Requirements for special or additional processing are identified and agreed upon.
- Audit tests that could affect system availability are performed outside standard, regional business hours.
- All access is monitored and logged to produce a reference trail.

H. Protection of information

- Zebra uses cryptography, as appropriate, to protect the confidentiality, authenticity, and/or integrity of information.
- Documentation is established to ensure the proper and effective utilization of cryptography controls.
- Owners and users of cryptographic keys are made aware of their responsibilities for using and protecting keys (and where necessary disclosing keys) assigned to them.
- The purpose of backups is to ensure that data and information can be recreated, consistent with the requirements of the business, should a failure or disaster event occur. An effective backup and recovery strategy is important to ensure overall availability and integrity of data.
- Data from all information technology (IT) platforms and technologies used in production, for these platforms, must be backed up at regular intervals, in accordance with the agreed backup and recovery requirements.
- Data from development and test systems are fully backed up, in line with business requirements. Backups typically take account of the data affected, its sensitivity, and the timeframes required for the recovery to meet the business requirements.
- Data is archived, consistent with the criticality of the data, the nature of the business processes supported, and legal or regulatory requirements.

I. User identification and authorization

- A user registration process enables the managing of access privileges on the information systems. Each user has a unique user identification (ID) or account identifier.
- A formal de-registration of user accounts enables the termination or adjustment of access privileges.
- Access to applications is removed on termination by Zebra.
- The allocation of secret authentication information is controlled through a formal process.
- Access re-certification requires asset owners to review users’ access rights at regular intervals.

J. Events logging

- Event logs, user activities, exceptions, faults, and information security events are produced, kept, and regularly reviewed.

- Monitoring and logging are implemented in systems to generate alerts when events or faults occur, and to facilitate subsequent log analysis following fault detection.
- Roles and responsibilities for detection of potential information security incidents from security monitoring activities must be defined to ensure accountability.

K. System configuration

- Procedures are implemented to control the installation of software on operational systems.
- Development, testing, and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.
- Any amended, newly created, or purchased version of software must always be subjected to a formal testing and release procedure, in accordance with the control requirements before it is introduced into a production environment.

L. Data Processing

- Zebra limits its collection, transfer, access, storage, and processing of Customer Data only to the data necessary for the purpose for which it is collected.
- Customer Data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- The Customer is responsible for ensuring that any Customer Data that is provided to Zebra is complete and accurate and for obtaining consents where required for Zebra’s use of Customer Data.
- Reasonable steps are taken to ensure that inaccurate Customer Data, regarding the purpose for which they are processed, are erased, or rectified without delay.
- Creation of processing records occurs through regular review of processing activities as part of Zebra’s privacy program. Records of processing document details on how, where, and why information is processed by Zebra.
- Data record sets at Zebra are retained in accordance with Zebra’s record and retention policy, absent the application of specific laws or an agreement governing retention.
- It is acknowledged that privacy implications may exist when Customer Data is collected, used, disclosed, or retained in a country that is different from the country of origin of such Customer Data. When permitted, Zebra takes the necessary actions to ensure the protection of Customer Data during cross-border transfers and/or access.

This version was last updated on 17 June 2024

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corp., registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2024 Zebra Technologies Corp. and/or its affiliates.

The information contained herein, and the statements expressed, are of a general nature and are not intended to address the circumstances of any particular individual or entity. There can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.