Information Security Requirements for Suppliers

ITS-0015-Appendix-A

Functional Team: Security	Category: Supplier Relationships	
Author: Sylke Hauptmann	Approvals: Approved by Sylke Hauptmann 10/10/2019 Bjorn Svard 10/11/2019 Klaus Niebur 10/14/2019 Jesus Gamazo 10/15/2019 Maryann Perttunen 10/16/2019	
Version: 1.0	Release date: 10/16/2019	Pages: 2
Initial release		

1 Introduction

Information Security and Data Privacy controls are essential obligations of the SUPPLIER relationship with AUTOLIV. Such controls encompass all types of DATA in all forms that may be shared or used as part of the business relationship. For purposes of this Information Security Requirements

- DATA includes all electronic, digital, visual, audio, printed, and prototype or other physical information
- SUPPLIER encompasses all supplier, vendor, 3rd-party contractor or other non-customer business partner relationships with AUTOLIV

2 Requirements

AUTOLIV requires compliance and evidence to support such compliance with the following high-level requirements for any SUPPLIER to AUTOLIV, regardless of the type of relationship (e.g. information-only, services, indirect materials, direct materials).

Area	Description
Information Security & Data Privacy	• Information Security and Data Privacy are managed according to international information security, cyber security and data privacy standards (e.g. ISO/IEC 27000 family; GDPR) throughout the entire supply-chain
Information Security Risk Management	• A Risk Management methodology, with regular risk assessments,that provides for the identification, proper treatment and documentation of substantive risks and vulnerabilities that may impact AUTOLIV DATA must be maintained
Data Classification	• AUTOLIV data classification definitions and related requirements must be understood and controls must be implemented accordingly (AS265 Data Classification Policy)

Area	Description
Access to CONFIDENTIAL or SECRET Information	• Every SUPPLIER requiring access to Autoliv CONFIDENTIAL and/or SECRET data needs to be evaluated under information classification aspects before access will be granted (risk-based approach) • If the SUPPLIER has access to CONFIDENTIAL and/or SECRET information, access shall be limited based on need to know for the transaction at issue and the SUPPLIER must maintain an explicit list of individuals that are authorized to access such information, or ensure procedures or conditions for access are defined and enforced
Record Retention	• AUTOLIV record retention definitions and related requirements for retention length for AUTOLIV-related DATA must be understood and controls must be implemented accordingly (AS303 Records and Information Management)
Data Protection Compliance	• SUPPLIER is required to sign the AUTOLIV Data Processing Addendum in the case where personal data is processed (AS263 Data Privacy Policy)
Communication of Incidents, Risks, or Changes	• AUTOLIV must be informed without undue delay ▪ regarding any security breaches that might have impact on AUTOLIV DATA or the provided services stated in the underlying contract ▪ of any changes to the SUPPLIER's policies, procedures or environment that may impact AUTOLIV's business or the security of its DATA, as a result of regular risk assessments or otherwise
Physical Security	• Physical Security controls adequate for the type of data involved must be implemented at any SUPPLIER location where AUTOLIV's DATA is stored or processed (AS323 Physical Security – Policy & Guideline)
Right to audit	• AUTOLIV or an external third-party authorized by AUTOLIV has the right to audit and test the Information Security and Data Protection implementation at the SUPPLIER location upon reasonable advance notice. ▪ Alternatively, SUPPLIER may provide proof of compliance by presenting an applicable certificate (e.g. ISO/IEC 27001 "Information technology – IT Security process") or certification according to the VDA Model "TISAX" (Trusted Information Security Assessment Exchange)

3 Compliance and Clarifications

SUPPLIER shall ensure that the Information Security and Data Privacy controls, requirements and obligations in this policy are required of its suppliers that have access to, manage, or control AUTOLIV Data. These controls, requirements and obligations are required within SUPPLIER's entire supply chain. SUPPLIER shall identify a single point of contact for reviewing compliance with the Information Security Requirements; the single point of contact shall be identified in the ALV Supplier Board under "Contact / Function: "Information Security Contact"."

In the case of questions or required clarifications, the SUPPLIER shall contact the related lead buyer for assistance.

4 Modification Index

Version	Date	Modification
1.0	*10/16/2019*	Initial Release