

PDF Sample Data Protection SUPPLIER SECURITY POLICY

Purpose, scope and users

The purpose of this document is to define the rules for relationship with suppliers. This document is applied to all suppliers who can influence confidentiality, integrity and availability ofLtd sensitive information including personal data. Users of this document are top management and persons responsible for suppliers inLtd

Commented [dk1]: The Scope helps guide why and by who the Supplier and or Partner's involvement must be treated.

Abbreviated definitions against relevant clauses inform the owner/user how to apply this Policy

1. Reference documents

- EU GDPR
- Risk Assessment/Treatment Plan
- Confidentiality (NDA) Policy

2. Relationship with suppliers and partners

2.1. Identifying the risks

Security risks related to suppliers and partners are identified during the risk assessment process, as defined in the Risk Assessment. Special care must be taken to identify risks related to information in communication technology with the product supply chain.

Commented [dk2]: As with all positions noted on all templates, the Managing Director can appoint, if required, a Senior Manager in any appropriate position/role in any policy or process.

Commented [dk3]: As with all risk assessments its important to evaluate the value to the business and in the case of failure how that is likely to effect its performance, long and short term.

Managing Director and or Senior Management decide whether it is necessary to additionally assess risks related to the business suppliers.

2.2. Screening

Managing Director and or Senior Management decide if it is necessary to perform background verification checks for suppliers, and if yes – which methods to be used.

In cases where personal data is being processed, **Managing Director** and or Senior Management are responsible for potential or existing suppliers to fill out the GDPR Compliance Questionnaire and information harvested through the questionnaires will be used to decide whether to start working with potential supplier, and the improvements to be made by existing suppliers.

2.3. Contracts

For suppliers providing data processing services for personal data, **Managing Director** and or Senior Management are responsible for signing an agreement that is based on Supplier Agreement.

For other suppliers **Managing Director** and or Senior Management are responsible for deciding which security clauses will be included in the contract with suppliers. Such decision(s) must be based on the results of risk assessment; however, the clauses which stipulate confidentiality and return of assets after the termination of the agreement are mandatory. Further, the contracts must ensure reliable delivery of the products/services and is particularly important with cloud service providers.

Managing Director and or Senior Management will decide whether the individual employees of the supplier/partner will have to sign a Confidentiality Statement when working for [organization name].

Managing Director and or Senior Management decides who will be the contract owner for each contract – i.e. Procurement Manager will be responsible for a supplier.

2.4. Training and awareness

Contract owner decides which employees of suppliers need security awareness training. **The Supplier** is responsible to provide all the training and raising of awareness of the GDPR systems of their employees.

2.5. Monitoring and review

Contract owner must regularly check/monitor the level of service and fulfilment of security clauses by suppliers, reports and records created by the supplier, as well as audit the supplier at least once a year. Security incidents related to the supplier's job must be forwarded immediately to the business.

2.6. Changes or termination of supplier services

Contract owner proposes changes or termination of the contract, and **[job title]** makes the final decision. **Managing Director** will perform a new risk assessment before the changes are accepted.

Commented [dk4]: Most likely jointly with the Procurement Manager and the Sales Team.

2.7. Removal of access rights / return of assets

When the contract is changed or terminated, the access rights for employees of suppliers must be removed. When a contract is changed/terminated, the contract owner must make sure all the equipment, software or information in electronic or paper form is returned.

3. Managing records kept based on this document

Commented [dk5]: Probably as with all records do not over complicate records

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Processor of GDPR Compliance Questionnaires	Managing Director computer	Managing Director	Only Managing Director can access those records	5 years after termination of the contract or the company law that prevails
Hard copy contracts with suppliers/partners or interested parties	Cabinet, safe, or similar that must be secure	Managing Director	Only Managing Director & or the Procurement Manager has access to the cabinet, or safe	5 years after termination of the contract or the company law that prevails
Records of monitoring and review	Contract owner's computer	Managing Director & Contract owner	Only Managing Director can access those records	5 years after termination of the contract or the company law that prevails

Procurement management to lead the monitoring of these relationships and performance of all contracts

This should also involve senior management if the event is of a serious nature that may possibly damage the business and its reputation