Confidential
2018-04-01

Technical and organisational privacy and security measures

The following minimum requirements are applicable when Supplier is Processing Personal Data on behalf of Tieto. These requirements are addition of the requirements already placed on in the agreements between the Parties. The requirements set out herein shall however in no way be interpreted to limit the Supplier's obligation as defined under the Laws.

Privacy requirements

1 The Supplier agrees, in the Processing of Personal Data under the Services, to comply strictly with the Laws, including without limitation, to observe the requirements derived therefrom in all its such activities, such as 'privacy by design' and 'privacy by default'.

2 Supplier's top management shall set direction for and show commitment to privacy. At a minimum, there shall be a high-level privacy policy that applies enterprise-wide and assignment of overall responsibility for privacy to a top-level executive or equivalent.

3 Personnel with access to Personal Data shall be required to take appropriate data protection training on a regular basis.

4 Supplier shall maintain the Personal Data in a form and format that enables access with the greatest convenience to the Data Controller that is reasonably feasible and consistent with the efficient provision of the Services and protection of Personal Data.

5 Insofar as this is possible and taking into account the nature of the Processing, if requested by the Data Controller in order to comply with the Laws, the Provider shall at no additional cost:

   1 provide the Data Controller with a copy of and/or access to data subjects' Personal Data in tangible and/or electronic form

   2 modify, correct, block or securely delete data subjects' Personal Data

   3 limit the Processing of Personal Data to storage only

   4 deliver to the Data Controller personal data concerning data subject in a structured, commonly used and machine-readable format

6 Personal Data shall be retained for only as long as necessary to fulfill the stated purposes in contractual agreements with Data Controller, or as required by the Laws, and shall thereafter be appropriately returned or disposed at the choice of Data Controller.

7 Reasonable steps shall be taken to ensure Personal Data is correct and accurate.

8 Personal Data records processed under the DPA must always be kept isolated and processed separately from other personal data records.

9 Supplier shall have a documented process to verify and regularly ensure that Sub-Processors and any other third parties that are used are compliant with requirements of Tieto (as stated herein and under the agreements) and the Laws.

Security requirements

Supplier shall:

1 maintain and monitor an information security governance framework, which enables the organisation's governing body to set clear direction for, and demonstrate their commitment to, information security and risk management.

2 conduct regular information risk assessments for target environments.

3 maintain a specialist information security function, led by a sufficiently senior manager, who is assigned with adequate authority and resources to run information security-related projects; promote information security throughout the organization; and to manage the implications of relevant laws, regulations and contracts.

4 develop a comprehensive, approved information security policy and communicate it to all individuals with access to the organisation's information and systems.

5 embed information security into each stage of the employment life cycle and maintain a comprehensive security awareness program.

6 maintain an information classification scheme, which applies to information of all types, to help protect information against corruption, loss and unauthorized disclosure.

7 protect physical assets throughout their life cycle, addressing the information security requirements for their acquisition, maintenance and disposal.

8 maintain a structured system development methodology that: applies to all types of business application; is supported by segregated development environments; and involves a quality assurance process. Develop business applications in accordance with an approved system development life cycle, which includes incorporating information security during each stage of the life cycle.

9 incorporate security controls into business applications to protect the confidentiality and integrity of information when it is input to, processed by and output from these applications.

10 restrict access to business applications, mobile devices, systems and networks to authorized individuals for specific business purposes.

11 design systems to cope with current and predicted workloads and configure them in a consistent, accurate manner to protect them, and the information they process and store, against: malfunction; cyber attack; unauthorised disclosure; corruption; and loss. Manage the security of systems by performing backups of essential information and software, applying a rigorous change management process and monitoring performance against agreed service level agreements.

12 design physical, wireless and voice networks to be secure, reliable and resilient.

13 identify and manage information risk throughout each stage of relationships with external suppliers, by embedding information security requirements in formal contracts and obtaining assurance that they are met.

14 maintain a sound technical security infrastructure and integrating technical security solutions, which include: malware protection; identity and access management; intrusion detection; and information leakage protection. Deploy approved cryptographic and pseudonymization solutions in a consistent manner across the organization to help: protect the confidentiality of information; determine if critical information has been altered; provide strong authentication; and support non-repudiation.

15 manage threats and vulnerabilities associated with business applications, systems and networks by: scanning for technical vulnerabilities; maintaining up-to-date patch levels; performing continuous security event monitoring; acting on threat intelligence and protecting information against targeted cyber attacks. Establish a comprehensive information security incident management framework.

16 protect critical facilities and services against: targeted cyber attacks; unauthorised physical access; accidental damage; loss of power; fire; and other environmental or natural hazards.

17 develop, maintain and regularly test business continuity plans and arrangements for critical business processes and applications throughout the organisation.

18 conduct thorough, independent and regular audits of the security status of target environments.

Data breach notification

The following requirements are applicable in case of Personal Data Breach.

The Data Processor shall without undue delay notify the Data Controller if it or one of its Sub-Processors becomes aware of a Personal Data Breach. Information shall be provided to the contact person named by Tieto, if not otherwise agreed between the Parties.

Information provided to the Data Controller shall include, at minimum:

1 a description of the nature of the Personal Data Breach including the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;

2 a description of the likely consequences of the Personal Data Breach;

3 a description of the measures taken or proposed to be taken by the Data Processor to address the Personal Data Breach, including measures to mitigate its possible adverse effects; and

4 the circumstances giving rise to the Personal Data Breach, and any other related information requested by the Data Controller. The Parties may agree on a more detailed breach notification process separately.

In addition, in case of a Personal Data Breach the Data Processor will be responsible for:

1 taking all the necessary steps to protect the Personal Data after having become aware of the Personal Data Breach, including appropriate measures to secure the Personal Data and limit any possible detrimental effect to the data subjects. The objective of the Personal Data Breach response will be to restore the confidentiality, integrity, and availability of the Services, to establish root causes and remediation steps, and to mitigate any damage caused to data subjects, the Customer and Tieto; and

2 reasonably cooperating with the Customer or Tieto in responding to such Personal Data Breach.

If a Personal Data Breach is attributable to the Data Processor, the Data Processor shall perform all above actions at its own cost and expense.

If a Personal Data Breach is not attributable to the Data Processor, such costs and expenses for the Data Processor and arising out of the above actions shall be borne by Tieto provided that such costs and expenses have been agreed in advance in writing.

