DESCRIPTION OF PERSONAL DATA FILE
Section 10 of Finnish Personal Data Act (523/99)

1. Controller	Name Wärtsilä Corporation
	Contact information P.O. BOX 196 FIN-00531 Helsinki
2. The person in charge and/or contact person	Tuomo Iivonen
	Contact information Tel. +358 10 709 0000 P.O. BOX 252 FIN-65101 Vaasa
3. Name of the register	**login.wartsila.com** Individual User Data Register
4. The purpose for processing the personal data / the purpose for the use of a register	**login.wartsila.com** is a business-to-business extranet channel used to complement conventional customer service offerings. Depending on business relationship between customer company and Wärtsilä online services like documentation delivery, spare parts ordering, shipping information handling and others can be activated for customer users based on separate agreements. User data is collected and processed to: - Grant access and access rights to login.wartsila.com and its service offerings. - Tailor the login.wartsila.com site and information to individual User's or groups of Users. - Administer access and use of services available in login.wartsila.com. - Respond to queries, requests and concerns of the User. - Inform Users of new services and other login.wartsila.com related issues.
5. Content of the register	**Data subjects ("Users"):** a. Employees of Wärtsilä's existing customers who have registered with login.wartsila.com. b. Employees of Wärtsilä's suppliers, subcontractors, partners, value-added resellers and service partners who have registered with login.wartsila.com. c. Employees of subcontractors of Wärtsilä's customers who have registered with login.wartsila.com. d. Other user groups who have registered with login.wartsila.com. e. Employees of Wärtsilä, who contribute to online application workflows on Wärtsilä's behalf f. Employees of Wärtsilä, who use login.wartsila.com to access applications dedicated for Wärtsilä internal use only. **Two components of the File:** 1. Concepts (with concept owner to supervise/control working methods, data types and fields)

	2. Fields **<u>1. Concepts</u>** a) Access right management b) Document and information bulletin management c) Supplier management services d) Shipment information handling e) Spare part ordering f) Engine service planning tasks **<u>2. Fields</u>** **The following personal information is collected from customer Users (* = required):** - User's first name*, last name* - Company* - Main Business category - Work e-mail* - Company street address - Town/city - Postal code - Country* - Work phone Information stored in login.wartsila.com user database contains additional fields as compared to the information gathered for registration purposes. These fields are required because of the technical implementation of the system: - Username & password - Date of user ID creation/termination - SAP ID - For other back-end applications in login.wartsila.com: Application-specific codes that controls users' access to application data For Wärtsilä internal employees only their internal username is stored. login.wartsila.com collects and stores only information that is related to User's role as a registered login.wartsila.com user.
6. Regular sources of information *	The data is provided by the users (data subjects) themselves, their Wärtsilä representative, ssuperior or company representatives. User saves the data in the login.wartsila.com user administration system via a user profile view.
7. Regular destinations of disclosed data and whether the data is transferred to countries outside the European Union or the European Economic Area	Data may be transferred within Wärtsilä Group and both within the EU and outside it to the US, China and elsewhere in Asia. Wärtsilä may also use subcontractors to provide some products or services. It may need to share personal data with these subcontractors so that they can provide those services. Subcontractors are not allowed to use such personal data for any other purposes. Strict confidentiality requirements are imposed on the services provided by subcontractors. In order to ensure and fulfill administrative and development needs, this site uses technology that lets us collect and report certain technical information like User's http identification, Internet protocol address, computer's operating system, browser type, traffic patterns and the address of any referring Web sites. Aggregated usage reports (personally identifying information excluded) are made available to: a) login.wartsila.com service-specific business owners b) customer account team management c) login.wartsila.com administration and maintenance personnel.

8. The principles how the data file/register is secured.	**Common Information Security and Information Technology Security** The value of relevant and correct information is based on the following quality characteristics: **Integrity:** accuracy, consistency and completeness of information. **Availability:** access of authorized users to information when required. **Confidentiality:** prevention of non-authorized access to information. **Non-repudiation**: obstacles to credible claims of information forging. The Information Security function aims at preservation of information quality. Every form of information media is subject to information security. The information technology security function (IT security) is a subset of information security, focused on technological information processing solutions; such as hardware, software and system services, and directed especially towards the prevention of intentional misuse and damage of information or processing systems. **Common Rules of Access and Usage Rights** Only known and identified individuals may receive access and usage rights to Wärtsilä information and systems. In the absence of clear contrary evidence, all actions taken during an access session are the responsibility of identified user. The identity of the user must be unique and kept separate from the attached usage rights. Wärtsilä has the right to access the information in the user's domain for technical maintenance tasks, as permitted by the **legislation** of the country in question. This right will not be exploited for unreasonable invasions into the privacy of users. **Authorization Policy of the login.wartsila.com Register** Persons requesting access rights to the system cannot grant their own user rights. All data in the system has a data owner(s) responsible for granting access rights to the data. User rights have two main components: the user role and the organisational extent. The user role defines the activities that the User is allowed to perform. The organisational extent tells who does the User work for and what are her/his responsibility areas. These two components give clear rules for what a User can do (the user role) and what information a User can see (the organisational extent). Both components must be specified in a user rights request. The user rights request will be approved according to the authorisation process. **Backup of the data:** Data is copied and stored for backup and restore purposes in Finland.