Privacy Operating Procedure – TOOL **Aquafil CSR Data** Regulation (EU) No 679/2016

Summary

1. Definitions

LCE:	**LIFE CYCLE ENGINEERING SPA**
CUSTOMER:	**Aquafil**
PROVIDER:	**Aruba Business**
TOOL:	**WEB-TOOL Aquafil CSR**
EMAIL_CLIENTE:	Lucija Aleksic <lucija.aleksic@aquafil.com>; Nika Cuk <nika.cuk@aquafil.com>

2. Purpose

The purpose of this Procedure is to define the ways in which LCE manages the personal data included in the TOOL in compliance with the current regulations on Privacy GDPR - Regulation (EU) no. 679/2016 and Legislative Decree 101 of 10/08/2018 and subsequent amendments.

As part of the specific project of the CUSTOMER, LCE has developed a calculation TOOL useful for processing plant data for the generation of environmental indicators to be used for internal monitoring and external communication.

3. TOOL Data Management and Processing

3.1 Data Classification

In relation to the provisions of the GDPR - Regulation (EU) no. 679/2016 and subsequent amendments and additions. The following are definitions and regulatory references for a clearer understanding of data in terms of privacy:

- **PERSONAL DATA:** any information relating to a natural person, identified or identifiable, even indirectly, by reference to any other information, including a personal identification number;
- **SENSITIVE DATA:** personal data revealing racial and ethnic origin, religious, philosophical or other beliefs, political opinions, membership of political parties, trade unions, associations or organisations of a religious, philosophical, political or trade union nature, as well as personal data revealing health and sex life (Article 9 GDPR).
- **JUDICIAL DATA**: these are considered, by letter e) of paragraph 1 of Article 4 of the Code, as personal data suitable for revealing measures in the field of criminal records, the registry of administrative sanctions dependent on crimes and related pending charges, or the status of defendant or suspect pursuant to Articles 60 and 61 of the Code of Criminal Procedure;
- **DATA PRESENTING SPECIFIC RISKS**: These are data that, although not as sensitive as sensitive and judicial data, present specific risks for fundamental rights and freedoms, as well as for the dignity of the data subject, in relation to the nature of the data, or the methods of processing or the effects that it may have: in view of this fact, their processing is permitted in compliance with the measures and precautions prescribed by the Guarantor to guarantee the data subjects.

For the purposes of the Management and Control of the TOOL , the reference data that may be processed are EXCLUSIVELY PERSONAL DATA consisting of:

- Users' name, surname, e-mail;
- Name, surname, e-mail address of the Tool Administrators.

In line with the risk-based approach defined by the GDPR, the impacts on the rights and freedoms of data subjects in the event of a breach of their personal data have been classified, in order to identify the appropriate security measures to protect the data itself.

The RISK can be classified as LOW considering the activities carried out on the TOOL and the types of Personal Data processed.

Categories of Personal Data	Categories of data subjects	Level of Impact
Common data	*CUSTOMER* *Employees*	*Low impact*

3.2 Description of the Treatment

For the purposes of the Management and Control of the TOOL, LCE, as External Data Processor, develops the processing operations reported in the Table.

Treatment	Description of the Treatment
Logical access control to corporate information systems	*The processing refers to the management by Suppliers of the profiles and accesses of employees and third parties.*

These activities refer to the collection, recording and storage of personal data contained within the TOOL developed in accordance with the purposes and objectives established by the contractual agreements signed with the CUSTOMER.

In particular, the following processing operations are permitted relating to the collection, recording and storage of personal data contained within the TOOLS developed in accordance with the purposes and objectives established by the contractual agreements signed with the CUSTOMER.

Actions related to name, surname, e-mail of USERS and ADMINISTRATORS

- Creation of the User for the purpose of automatic access (name, surname, e-mail)
- Use of Information to Identify You and Enable Automatic Access
- Use of the information to associate the data contained in the TOOL with users

- Use of e-mail to send instructions at the first access and communications related to the operation of the TOOL
- Use of e-mail to send communications related to the operation of the TOOL

Any other processing operation must be carried out within the limits of its duties and in compliance with the legal provisions established in agreement with LCE's Data Processor.

4. Safety Precautions

4.1 Minimum Security Measures

LCE, in the development and management of the TOOL, operates in compliance with the principle of *Privacy by Default* through the adoption of appropriate technical and organizational measures to ensure that:

- only the personal data necessary for each specific purpose of the processing are processed, by default;
- personal data is accessible to a defined number of persons;
- Data subjects should always know for what purposes their data is collected.

In compliance with the legislation on the protection of personal data and the protection of data subjects, established by the main international standards on the management of Information Security, LCE also provides:

- communicate to the Data Controller the name of an "Information Security Representative", who has the task of liaising with the Data Controller regarding the application of security measures and taking care of the solution of any problems;
- not to replicate or use the Data Controller's data in its own development/test environments, unless explicitly approved by the Data Controller;
- comply, where applicable, with the instructions provided in the procedure "Rules for the use of company IT resources by third parties";
- implement the measures prescribed by the Data Controller for the processing carried out by electronic means with regard to the attribution of the functions of System Administrator"
- implement all the security measures provided in relation to the characteristics of the TOOL Implementation and Management Service and the level of Impact for Data Subjects.

4.2 Security measures related to the impact on the rights and freedoms of data subjects

As mentioned in Chapter 2.1, the Level of Impact on the rights and freedoms of data subjects associated with Data Processing in the TOOL is LOW; the related specific Security Measures adopted by LCE as Data Processor are shown in the Table below.

Measure Code (Risk Level)	Measure	Description	How to manage it
1(B)	Security policy and procedures for the protection of personal data	The organization must document its rules regarding the processing of personal data as part of the cybersecurity rules; Such safety documentation shall be reviewed and revised, if necessary, annually	- The Web-Tool is hosted on a dedicated server with exclusive access to authorized operators, subject to specific appointment, within LCE and the Sub-processor in charge - All data uploaded and available in the Web-Tool are recorded exclusively in a dedicated database and installed on the same server, and are not processed for internal use in any other form. - The TOOL reference domain is assigned the HTTPS protocol and the SSL encrypted security certificate with annual renewal. - Access to the Web-Tool is protected by a 2-parameter authentication system (username, password) which also makes use of the Google Recaptcha human verification tool. - Users' passwords are recorded in the database in encrypted form using SHA-256 algorithm
d	Roles and Responsibilities	Roles and responsibilities related to the processing of personal data must be clearly defined and assigned in accordance with security rules.	The roles and responsibilities related to the processing of personal data are clearly defined by the LCE Data Processor and assigned in accordance with the security rules through dedicated appointments for the Processors, Sub-Processors and System Administrators.

Measure Code (Risk Level)	Measure	Description	How to manage it
		During internal re-organizations or terminations of employment relationships or even temporary changes to the job, the revocation of rights and responsibilities and the respective authorizations must be clearly defined.	In the Web-Tool area, the responsibility for the processing of personal data recorded in the corresponding Database is the responsibility of the System Administrator identified through a specific appointment, who is assigned the role of supervisor.
7(B)	Access Control Policy	Specific permissions for access control must be assigned to each role (involved in the processing of personal data) following the need to comply with the "need to know" principle.	- Accesses to the Web-Tool are recorded in a specific log archive in the corresponding database, supervised by the System Administrator. - Access control permission is assigned exclusively by the System Administrator in charge.
10(B)	Resource/Asset Management	The organization must have a record of the computing resources used for the processing of personal data (hardware, software, and network). The log must include at least the following information: IT resource, type	The System Administrator at company level has a digital register of IT resources, used for the processing of personal data, periodically managed and updated.

Measure Code (Risk Level)	Measure	Description	How to manage it
🟩		(e.g. server, workstation), location (physical or electronic). IT resources should be reviewed and updated regularly (specify), and a specific person should be assigned the task of maintaining and updating the register (e.g., IT manager).	
13(B)	Change Management	The organization must ensure that all changes made to the information system are recorded and monitored by a specific person (e.g., IT or Security Officer). This monitoring should be carried out on a regular and periodic basis. Software development must be carried out in a special environment that is not	The process of managing the software implementations of the Web-Tool, whether corrective, adaptive, evolutionary, involves the following steps: - Analysis of the activities to be carried out in collaboration with the LCE Data Processor - Definition of the work plan and delivery dates and recording of the activities to be carried out on the ticketing platform - Development in an independent local environment connected to a database with fictitious data and first internal testing. - Transition to an online testing environment, detached from the official system and connected to databases with fictitious data - Execution of the tests carried out by the LCE Processors

Measure Code (Risk Level)	Measure	Description	How to manage it
		connected to the computer system used for the processing of personal data. When testing is needed, dummy data (not real data) should be used. In cases where this is not possible, specific procedures must be in place to protect the personal data used in the tests.	- Registration of the backup structure and database of the official environment and upgrade of the Web-Tool in the official environment.
15(B)	Data Processors	Formal guidelines and procedures regarding the processing of personal data by data processors (contractors/outsourcing) must be defined, documented and agreed between the Data Controller and the Data Processor prior to the commencement of the processing. These guidelines and procedures must mandatorily establish the same level of security of personal data as required by the Data Controller's security rules.	The LCE Data Processor, in collaboration with the System Administrator, has formalized this Data Privacy Operating Procedure , focused on the security measures adopted for the processing of personal data of the Web-Tool.

Measure Code (Risk Level)	Measure	Description	How to manage it
		Upon discovery of a personal data breach, the Processor shall inform the Controller without undue delay. Formal requirements and obligations shall be formally agreed between the Data Controller and the Data Processor. The Data Processor must provide sufficient documented evidence of the compliance of his/her organization and the processing carried out with the safety requirements.	
18(B)	Incidents, manipulation/breaches of personal data	An incident response plan with detailed procedures must be established to ensure an effective and orderly response to incidents related to personal data. Personal data breaches must be immediately reported to the Management and notification procedures for reporting breaches to	The Incident Response Plan relating to personal data is managed in accordance with the procedures provided by the CLOUD PROVIDER where the Web-Tool resides. In particular, in compliance with the provisions of the European Regulation 2016/679 ("GDPR"), the CLOUD PROVIDER • has verified and adapted the technical and organizational measures to ensure the security of the personal data processed by it in the provision of services.

Measure Code (Risk Level)	Measure	Description	How to manage it
		the competent authorities and data subjects must be in place, in accordance with Articles 33 and 34 of the GDPR.	- It provides its services through means and tools suitable for effectively protecting the security of information (physical, logical, IT and organizational). In particular, in the event of events that may lead to the breach of the data processed by the CLOUD PROVIDER, the System Administrator and the Data Processor are immediately notified in accordance with the procedures and within the time limits set out in the applicable legislation in force (with Articles 33 and 34 of the GDPR). Main reference regarding the measures adopted by the CLOUD PROVIDER - General Terms and Conditions: https://business.aruba.it/documents/term_conditions/condizioni-generali-aruba-business.pdf
21(B)	Business Continuity	The organization must establish the main rules and checks to be performed to ensure the level of continuity and availability of the IT system that processes personal data (in the event of a personal data breach/incident).	In order to ensure the business continuity of the Web-Tool, the System Administrator uses: - Warranties and certifications provided by the Cloud Provider - Internal data backup and recovery service management system - Periodic (daily) monitoring of the correct functioning of the IT system

Measure Code (Risk Level)	Measure	Description	How to manage it
24(B)	Confidentiality of staff	The organization must ensure that all employees understand their responsibilities and obligations regarding the processing of personal data. Roles and responsibilities must be clearly communicated during the selection or assignment process.	During the engagement phases, employees sign up to the roles and responsibilities that are assigned to them, including obligations related to the processing of personal data. The subjects in charge of the Processing of Personal Data contained in the Web Tool to which this procedure refers.
27(B)	Formation	The organisation must ensure that all employees are adequately informed (including through awareness-raising campaigns): - about the security measures in place on the systems on which they operate;- about the relevant data protection requirements and legal obligations.	LCE employees in charge of software development, and the processing of personal data contained therein, are constantly updated on new provisions on IT security, data protection and related legal obligations. Training activities are planned periodically on the basis of the indications of the LCE Privacy Manager.

Measure Code (Risk Level)	Measure	Description	How to manage it
30(B)	Access Control & Authentication	An access control system that is applicable to all users accessing the IT system must be implemented. The system must allow you to create, approve, review, and delete user accounts. The use of common user accounts (so-called group accounts) is not allowed and, in cases where this is necessary, it must be ensured that all users with access to the same user have the same roles and responsibilities. An authentication mechanism must be in place that allows access to the IT system (based on the access control policy), which at least provides for the recognition of users by means of a username/password combination. Passwords must adhere to a certain level of complexity (configurable), which the access control system must have the ability to verify to avoid the use of simple passwords.	Access to the server where the web tool resides is accessed exclusively by authorized operators within the IT department of LCE (as System Administrator) Access is allowed only to registered and active users and is protected by a 2-parameter authentication system (username, password) which also makes use of the Google Recaptcha human verification tool. In order to use the Software, you must also give your consent to the use of the cookie for the inclusion of the Google security control, which is explicitly required in the conditions of first access, change of device, change of browser, access to the browser in incognito mode.

Measure Code (Risk Level)	Measure	Description	How to manage it
33(B)	Logging & Monitoring	Log files must be generated for each system/application used for the processing of personal data. They must include all types of data access (view, edit, delete). Log files must contain a timestamp and must be adequately protected from tampering and unauthorized access. Clocks must be synchronised with a single reference time source (e.g. NTP server)	Each activity carried out within the web-tool is recorded in the database in a dedicated log archive; in particular, details such as user, machine IP, date and time, archive, type and description of the activity are stored for each operation. The time reference is synchronized with the server's internal clock. Access to the log archive is exclusive to operators formally appointed and authorized by the System Administrator.
35(B)	Server/Database Protection	Databases and applications must be configured to operate using an account other than the one used by the operating system and with least privileges to function properly. Databases and applications must only process the personal data that is actually necessary for the pursuit of the purposes envisaged from time to time.	- Access to the database is configured by a dedicated user and different from the administrator user used to access the server. This user is exclusive and has the executing, reading and writing permissions necessary to carry out the functions available to the web-tool, provided for in the design phase - In the web-tool field, the "calls" to the database are specific and targeted to involve only the archives and data necessary to carry out the single activity in progress.

Measure Code (Risk Level)	Measure	Description	How to manage it
38(B)	Workstation Security	Users should not be able to turn off or bypass security settings. Anti-virus applications and detection signatures should be updated on a weekly basis. Users should not have privileges to install or disable unauthorized software applications. The system must have a session time-out when the user is inactive for a certain period of time. Critical security updates released by the operating system developer should be installed regularly.	- Access to the server where the web tool resides is exclusively accessible to operators formally appointed and authorized by the System Administrator. - The reference server is a cloud hosting platform, based on the Linux Operating System, which provides both an automatic update system and the presence of anti-virus and anti-malware software, managed directly by providers. - The web tool also has a session timeout scheduled in 30 minutes
41(B)	Network/Communication Security	Whenever access is made via the Internet, communication must be encrypted via cryptographic protocols (TLS/SSL).	In order to ensure a high degree of network/communication security, the Web-Tool is equipped with an HTTPS protocol with SSL security certificate.

Measure Code (Risk Level)	Measure	Description	How to manage it
44(B)	Back-Up	Data backup and recovery procedures must be defined, documented, and clearly identify roles and responsibilities. Backups must be assigned an adequate level of physical and environmental protection consistent with the standards applied to the original data, and their execution must be monitored to ensure completeness. Full backups should be performed regularly.	- The Cloud Provider providing the server where the Web-Tool is located provides a dedicated system for the backup and recovery of the operating system and the default configuration. In the event that a data restoration is necessary, the System Administrator shall promptly inform the LCE contact person in order to forward notice of extraordinary maintenance of the Web-Tool starting from the agreed time. Then we proceed to identify the last available backup copy in chronological order, then activate the remote connection to the hosted server and perform the "restore" function of the database and, if necessary, reload the Structure of the source files of the tool. Roles and responsibilities of authorized operators as System Administrator: - Backup Configuration; - Monitoring of backup procedures; - Manage recovery operations.

Measure Code (Risk Level)	Measure	Description	How to manage it
47(B)	Mobile	Mobile device management rules must be defined and documented to establish clear measures for their proper use. In order to access the information system, mobile devices must be pre-registered and pre-authorized. They must be subject to the same levels of access control as fixed workstations.	- There is no use of mobile devices to access the server system where the application resides - In the web-tool field, since it is an application that can be used via the internet, access is allowed from any device, with protection guaranteed by the authentication system and the HTTPS security protocol with SSL security certificate
50(B)	Application Lifecycle Security	During the software lifecycle, and particularly in the design and development phase, known best practices, frameworks, or standards for software security must be executed. Specific security requirements must be defined during the early stages of the development cycle. Specific solutions and techniques must also be provided to support the security of data protection systems (privacy enhancing technology). Standards and best practices must also be followed for secure development and	The web-tool is technically designed in order to guarantee the appropriate security standards in relation to the level of sensitivity of the data processed; Here are the main features: • A leading provider with the highest certified standards of reliability, safety and attention to the environment (https://www.datacenter.it/certificazioni-aruba.aspx); • Dedicated servers and databases with exclusive access; HTTPS protocol and security SSL certificate; • Login system with double level of protection; • Secure development process: Implementation in an on-premises environment, testing and validation in a test environment, and moving to production.

Measure Code (Risk Level)	Measure	Description	How to manage it
		for the definition of security requirements at the design stage, which must then be validated and tested before release into production.	
52(B)	Deletion/deletion of data	Media must be erased by overwriting before it can be deleted. In cases where this is not possible (CDs, DVDs, etc.) physical destruction must be carried out. Information on paper and removable storage devices used to store personal data must be physically destroyed prior to disposal.	- All data managed via the Web-Tool are exclusively recorded in the database dedicated to the application - In the event of a decommissioning of the Web-Tool or a change of infrastructure, the Cloud Provider provides for an automatic formatting of the server where the Tool resides.
55(B)	Physical Security	The physical perimeter of the IT system infrastructure must not be accessed by unauthorized personnel.	The physical perimeter of the IT system infrastructure of the Cloud Provider where the Web-Tool resides provides for Supervision and control through:

Measure Code (Risk Level)	Measure	Description	How to manage it
🟩			- Anti-intrusion sensors, video surveillance, mantraps with dual authentication mechanisms and anti-tailgating technological systems - 24/365 monitoring: Network Operation Center (NOC) on-site, redundant and manned 24 hours a day, 365 days a year - Data security: data management and protection in highly secure ISO 27001 certified infrastructures - Redundant systems: Fully redundant power centers and cooling systems - Energy backup: fully redundant backup areas that ensure reliable power and cooling - Fire prevention: separation of all systems and environments and self-extinguishing detection systems ensure maximum safety against the risk of fire

4.3 Instructions for Data Management Agents TOOL

Below are the main instructions that must be followed by the Persons in Charge involved in the development and management of TOOL projects in accordance with the provisions of the Data Controller and the Data Processor.

- Always use your personal access/authentication code USERNAME + PASSWORD;
- Do not disclose your authentication credentials, which must always be for strictly personal use;
- Avoid working on other people's terminals and/or leaving the TOOL open with your password entered in the event of even temporary removal from the workplace, in order to avoid unauthorized processing;
- Process only the data whose knowledge is necessary and sufficient to carry out the operations envisaged by the TOOL to be carried out in strict compliance with your authorization profile;
- To store its computer media in such a way as to avoid access by persons who are not authorised to process the data contained therein;
- Make copies of data subject to privacy on removable media only if part of the processing or data security (backup) defined by agreements with the CUSTOMER data controller;
- Provide immediate notice of unauthorised access to the Data Processor or the Data Controller;
- Report to the Data Processor or to the Data Controller any circumstances that make it necessary or appropriate to update the security measures provided for by the TOOL in order to minimize the risks of destruction or loss, even accidental, of data, unauthorized access or processing that is not permitted or does not comply with the purposes of the collection;
- Carry out the communication and dissemination of data exclusively to the subjects indicated by the Data Controller or the Data Processor and according to the procedures established during the design phase of the TOOL.
- Maintain, without prejudice to what is specified in the previous point, the utmost confidentiality on the data subject to privacy of which it becomes aware in the performance of the assignment, for the entire duration of the same and even after the end of it;
- provide the Data Controller or Data Processor with information relating to the activity carried out, in order to allow them to effectively carry out their control activities;
- Provide ample and complete collaboration to the Data Controller and the Data Processor in order to carry out everything necessary and appropriate for the correct performance of the assignment in compliance with current legislation.

4.4 Personal Data Breach

In the event of Personal Data Breaches, the System Administrator shall immediately notify the Data Processor (LCE) who shall inform the Data Controller within 48 hours of becoming aware of them by sending a communication by email to the addresses **Email_cliente**.

In particular, we are notified of any breach of security that accidentally or unlawfully results in the destruction, loss, modification, unauthorized disclosure or access to Personal Data transmitted, stored or otherwise processed within the TOOL.

Taking into account the nature of the processing and the information available, the Data Processor cooperates with the Data Controller in relation to the development of investigation and remediation activities as well as for any notifications to the competent authorities.

In the case of Data Breaches, LCE, in collaboration with the System Administrators, guarantees the CUSTOMER or the figures hired by him, access to its systems and to the premises that host them for the verification and/or verification of any violations, guaranteeing the necessary support throughout the analysis phase of the incident.

4.5 Audits and inspections

LCE guarantees the CLIENT or the subjects hired by him, the possibility of carrying out inspections and audit activities, with at least five working days' notice, in order to verify the effective and correct adoption of the security measures provided for the Processing of data in the TOOL.

LCE, in collaboration with the System Administrators, at the request of the CUSTOMER, makes available the documentation relating to the physical, logical and organizational security measures of its responsibility adopted to protect data for the purpose of providing the Management and Maintenance Services of the TOOL

4.6 Return and deletion of personal data

Following the expiry of the Contract and/or the Services or, in any case, in the event of termination (for any reason) of the Management/Maintenance/Assistance contract of the TOOL, LCE interrupts any processing of the same on the basis of the CUSTOMER's indications and provides:

- the immediate return of Personal Data;
- the complete deletion of Personal Data from their systems/workstations and from any storage medium .

In both cases, a written statement is issued at the same time that there are no copies of the personal data at LCE and, in the event of a written request from the Data Controller, the technical methods and procedures used for cancellation/destruction are indicated.

5. Persons Authorised to Process Data

5.1 Persons in charge of the Processing

LCE, in its capacity as Data Processor, guarantees that access to the Personal Data contained within the TOOL is limited exclusively to its employees and collaborators whose access is necessary for the management and maintenance of the TOOL itself; the qualified personnel is formally appointed as DATA PROCESSOR in written form.

As part of the appointments in question, the Data Processor provides its employees and collaborators responsible for processing TOOL Personal Data with the necessary instructions to:

- ensure that they are used correctly, lawfully and safely
- bind the confidentiality of all information acquired in the course of their activity, including for the period following the termination of the employment relationship.

LCE also provides the CUSTOMER with (upon specific request) the updated list of persons authorised to process Personal Data managed through the TOOL.

5.2 System Administrator

LCE formally appoints the System Administrator, selecting professional figures dedicated to the management and maintenance of IT systems or their components, with which Personal Data is processed.

LCE also communicates to the CUSTOMER (upon specific request) the names of the System Administrator of reference for the TOOL as well as provides information regarding the evaluations developed for the purpose of their designation.

As External Data Processor for the Management of the Data contained in the TOOL, LCE is responsible for:

- indicate in the Appointments of System Administrators the areas of operation allowed based on the relative authorization profile assigned
- prepare and maintain the list containing the identification details of the natural persons qualified as System Administrators and the functions assigned to them.
- periodically communicate to the Data Controller the updated list of names of system administrators, specifying their area of responsibility (systems, databases, networks, applications, etc.), in cases where the management of these areas is the direct responsibility of the Data Processor;
- verify at least annually the work of the system administrators through internal audits and inform the Data Controller about the results of such verification;
- verify the correct maintenance and management of the log files provided by the TOOL;
- guarantee a strict separation between those who authorize and/or assign access privileges to the TOOL (CUSTOMER as Data Controller) and those who carry out the technical-system activities of System Administration (Segregation of Duty).

5.3 Sub-Processors

In the event that LCE intends to use additional data processors (hereinafter, "Sub-processors") for the execution of the Data processing activities present in the TOOL, it shall notify the CUSTOMER Data Controller in advance (for the purpose of requesting the necessary written authorization) indicating:

- Name and registered office of the Sub-processors it intends to use;
- Place where they carry out their business if different from the registered office;
- Detailed information about the processing activities entrusted to the

As part of the specific appointments of Sub-Processors, LCE shall indicate the same obligations regarding the protection of Personal Data to which the Processor is subject, with particular reference to security obligations.

Upon request by the Data Controller, LCE provides a copy of the agreements entered into with its Sub-processors and, if necessary, audits them in order to demonstrate their compliance with the legislation on the protection of personal data, as well as with the obligations undertaken.

In the event that there are changes regarding the addition or replacement of additional Sub-processors, LCE informs the CUSTOMER (Data Controller) for the purpose of requesting the necessary authorization to operate on the TOOL.

6. Distribution

This operating procedure is shared and distributed during the training of Sub-Processors, System Administrators and Data Processors contained in the TOOL designed by LCE (in accordance with the provisions of the GDPR – EU Regulation No. 679/2016 on Privacy).

The various parties involved in the management of the TOOL in signing their Appointments undertake to comply with the obligations described above and are liable to LCE (as External Data Processor) in the event of non-compliance, also for the purpose of compensation for any damage caused by the processing of data.