PRIVACY POLICY FOR INSTALLER / USER (EU)

■ General

LG Energy Solution (hereinafter referred to as "The Company") cares about your privacy. The Company provides many products and services. This privacy policy applies specifically to LG Energy Solution RESU Monitor service website(https://res.lgensol.com) and Mobile Application(RESU Monitor). This privacy policy does not apply to any other LG Energy Solution branded products or services. The purpose of this privacy policy is to explain how we collect information, what we collect, how we use it, how we share it, and what controls and rights you have. Personal information is only used for the battery quality of LG Energy Solution. By using the Services, you consent to the terms of this privacy policy. The Company may amend this Privacy Policy as required by relevant laws or Company's internal regulation.

■ Purpose and legal grounds of processing personal data

<Installer's Personal Data>

1. Information to be collected (Information collected when creating an account)

    1) Required

    Email

    2) LG ESS Battery web site ID

    Optional

    Mobile Phone Number

2. Purpose

    Member registration / Product Registration / Product Monitoring / Owner Page Activation /

    Contact for Battery Maintenance

3. Method of Collection

    Web-page(provided by installers) /

    Mobile Application- RESU Monitor (provided by installers)

4. Legal grounds of processing personal data

1) The Company processes personal data for purposes related to the negotiations and performance of a contract, i.e. for the purposes necessary to perform the contract – this concerns customers who are natural persons and are parties to the contract with the Company.

2) Personal data is also processed in order to comply with obligations resulting from legal provisions, e.g. tax regulations and other provisions that apply to the Company

3) The Company may process personal data for administrative purposes, conducting internal policies, financial planning, debt collection, processing inquiries and complaints, pursuing claims and defending against claims, verification of compliance with internal procedures, marketing of Company's products and services i.e. for purposes of the legitimate interest of the Company.

4) In other cases, the Company may process personal data based on a voluntary consent to the processing of data and for the purposes indicated in such consent. Then a legal basis for processing is the customer's consent.

If you don't provide personal data to the Company, you may be restricted from entry into the contract, performance of the contract including remittance of payment, which means that collection of data is necessary for this purpose, results from the provisions of law and is a condition of concluding a contract. The provision of personal data in order to fulfil the legitimate interest of the Company is voluntary, but necessary for the achievement of the above objectives. In the case of consent, providing personal data by the customer is voluntary, and not giving such consent has no negative consequences.

<User's Personal Data>

1. Information to be collected (Information collected when creating an account)
   Email (Information collected during the installation phase only)

   1) Required
      Address (Detailed/City/Country/Continent Information)
      Time zone (Installation information)
      Photo of installed product
      Photo of product serial number
      Email
      Zip Code

   2) Optional
      BMS Data of installed product (Voltage, Current, Temperature, SOC, SOH, Serial Number, System Status, Version, Type)
      RMD Info. (RMD : Remote Monitoring Device)
      Periodic Data of Product
      Mobile Phone Number
      State
      Name

2. Purpose
   Product Status monitoring (Company / Installer)
   Product Event Collection
   Product usage Pattern analysis
   Display the Web page (Installer / User)
   Contact for Battery Maintenance
   FOTA (*Firmware Over-the-air)

3. Method of Collection
   Webpage (provided by users)
   Mobile Application (provided by users)
   RESU Device – Remote Monitoring Device (RMD)

4. Legal grounds of processing personal data
   The Company may process personal data based on a voluntary consent to the processing of data and for the purposes indicated in such consent. Then a legal basis for processing is the customer's consent.

■ Retention period

The Company retains the personal data for the period as required by the law. The Company may retain the data which may be used for proving the existence of the contract and the performance of such contract for the period of the contract and by the time all the rights or obligations under the contract are terminated or may retain data until the expiration of the claim limitation period, whichever is longer. - in accordance with the data retention policies applied by the Company. And the Company will destruct personal information without delay when the customer requests or Purpose has been completed. You may obtain the data retention policies by contacting the Company.

■ Recipients (Where Do We Send Your Data?)

Except for the following cases, the Company will not disclose personal information with a third party.

Scope	Regions (of data subjects)	Recipient	Purpose
User's Personal data	EU	Certified Installers*	Product Installation, Monitoring, Maintenance
Installer's Personal data User's Personal data	Global	LG CNS (Buildings E13 and E14, LG Science Park, 71, Magokjungang 8-ro, Gangseo-gu, Seoul, Republic of Korea) The third party company contracted by the company such as service providers and auxiliary agents for RMA(Return Material Authorization) and truck roll reimbursement.	Maintenance of system

Certified installers are those who can directly or indirectly sell you the energy products that you have requested, and those who may perform financing, permitting, inspections and installations. Locations of certified installers : The countries of sale listed in our Warranty Document (Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, United Kingdom)

Furthermore, depending on the circumstances, the personal data may be transferred to other entities, e.g. entities providing services to the Company, such as IT service providers, advisers, auditors, and to the extent that it is necessary to fulfill obligations resulting from legal regulations, e.g. to the government authorities.

■ Deletion of personal data

1. The Company will delete the personal data without delay, when the purpose of personal data processing is achieved or the retention period is expired unless the personal data is necessary or mandatory by the laws or the contract with the third party.

2. In case of the personal data in the form of the paper, the Company uses the paper shredder to dispose of such data or incinerate the paper, and in case of the personal data in the form of the electronic files, the Company deletes the data by using the means which preclude any restoration of such data.

■ Rights of the data subject

1. The Company has obligation and responsibility to ensure the rights of data subject with regard to personal data in the Company retained in any form such as electronic files, papers.
2. The laws may grant the customer (or its representatives) specific rights in connection with the processing of personal data by the Company. In situations specified in the regulations, the customer has the right to access their data, rectify it, delete, and restrict the processing of personal data, the right to object to the processing of personal data and the right to data portability.
3. The data subject may exercise its rights by contacting the personal data protection department/team as specified information below and upon receiving your fax, phone or email, the Company will promptly respond. The Company may demand to the data subject the copy of identification by which the Company can verify the identity of the data subject.
4. The Company may request the Power of Attorney and the copy of identification by which the Company can verify the existence of legitimate delegation to the representative of the data subject, if the data subject exercises its rights through its representative.
5. If the personal data are processed under the data subject's consent, the data subject may withdraw its consent at any time without prejudice to the lawfulness of personal data processing before data subject's withdrawal of consent.

■ Automated decision making, including profiling

The Company does not adopt any automated decision making including profiling which produces legal effects concerning you or similarly significantly affects you. The Company will give prior notice to you about the logic, necessity, expected results of the automated decision making system, if the Company expects to adopt any automated decision making system.

■ Transfer of personal data

Considering it engages in global businesses, the Company may provide the personal information to the companies located in other countries for the purpose as stated in "Recipients". For the places where the personal information is transmitted, retained or processed, the Company takes reasonable measures for protecting those personal information. Personal data shall be processed to the extent of "Purpose and legal grounds of processing personal data" and, without prior notice, shall not be processed beyond such scope and purpose. Your use of our Platform will involve the transfer, storage, and processing of your personal information within and outside of your country of residence consistent with this policy. In particular, your personal information will be transferred to the Republic of Korea. Please note that the data protection and other laws of countries to which your information may be transferred might not be as comprehensive as those in your country. Therefore, there may be risks due to differences in the level of personal information protection. The personal data are transferred through secured cable or VPN and Company adopts technical and organizational measures necessary to ensure transferred personal data not to be lost, stolen, disclosed, altered or destructed. If you need further information regarding technical and organizational measures to be adopted, contact as below information, then we will promptly respond to your inquiry.

■ Technical and Organizational Measures

The Company shall take the following technical and organizational security measures to protect personal data:

1. Organizational management and dedicated staff responsible for the development, implementation, and maintenance of the Company's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to the the Company organization, monitoring and maintaining compliance with the Company policies and procedures, and reporting the condition of its information security and compliance to senior internal management.

3. Maintain Information security policies and make sure that policies and measures are regularly reviewed and where necessary, improve them.

4. Communication with the Company applications utilizes cryptographic protocols such as TLS to protect information in transit over public networks. At the network edge, stateful firewalls, web application firewalls, and DDoS protection are used to filter attacks.

5. Data security controls which include logical segregation of data, utilization of commercially available and industry-standard encryption technologies.

6. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review manually and revoking/changing access promptly when employment terminates or changes in job functions occur).

7. Password controls designed to manage and control password strength, and usage including prohibiting users from sharing passwords.

8. System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.

9. Physical and environmental security of data center, server room facilities and other areas containing client confidential information designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of the Company facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

10. Operational procedures and controls to provide for configuration, monitoring, and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from the Company possession.

11. Change management procedures and tracking mechanisms to designed to test, approve and monitor all changes to the Company technology and information assets.

12. Incident / problem management procedures design to allow the Company investigate, respond to, mitigate and notify of events related to the Company technology and information assets.

13. Network security controls that provide for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

14. Vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

15. Business resiliency/continuity and disaster recovery procedures, as appropriate, designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

■ Personal Information Protection Management Director

Department Name: LG Energy Solution Information Security Department

■ Personal Information Protection Management Department

① Department Name: LG Energy Solution Security Policy Team

② Tel: +82-2-3773-3340

③ Email: privacy.es@lgensol.com

■ EU Representative

① Name: Jiheon Kim

② Tel: +49-61-965-719-673

③ Email: jiheonkim@lgensol.com

■ Personal Information Handlers

① Department Name: LG Energy Solution EDI Team

② Name: Jaekwang Jeon

③ Tel: +82-2-2206-0795

④ Email: jgjeon@lgensol.com

■ Right to lodge a complaint with a supervisory authority

You may lodge a complaint with a supervisory authority i.e. the President of Data Protection Authority.

※ Supervisory Authority is a separate organization from the Company. If you are not satisfied with Company's response to your complaint regarding your rights on personal data and you need further assistance, then you may lodge a complaint with a supervisory authority.

■ Customer obligation

If the customer provides to the Company personal data of his employees, agents, directors, partners, associates, business partners, suppliers and others, the customer is obliged to inform them that the Company is the data controller of their personal data and that it processes their personal data in accordance with the principles set out above, and if requested by the Company, the customer is obliged to provide the Company with confirmation of the provision of such information.

■ Protection of personal information of children

The Company does not collect any information from the children under 13 or equivalent minimum age as prescribed in the laws in relevant jurisdiction.

■ Selling of personal information

The Company does not and will not sell any personal information.

■ **Enforcement of Privacy Policy**

This Privacy Policy shall enter into force on Dec 1, 2020.

The Installer:

Company Name: _____

Authorized Rep: _____

Product name: _____

Signed: _____

Datum: _____

Customer:

Name of the customer: _____

Installation address: _____

_____

Signed: _____

Date: _____