January 2022 – Georgian Water and Power Ltd

Privacy Policy

This document outlines the terms and conditions governing the processing and protection of your personal information by Georgian Water and Power LLC.

1. Data Processor Details:

Our Information: Georgian Water and Power Ltd

Address: Medea (Mzia) Jugeli Street N10, 0179, Tbilisi, Georgia

Phone: +995 32 293 1111

Data Protection Officer: dpo@gwp.ge

Information Services: info@gwp.ge

Website: www.gwp.ge

2. Collection of Personal Data

We collect your personal data through various methods to fulfill the purposes and guidelines outlined in this Policy. The methods for obtaining this data include:

2.1. Personal Data of Subscribers: This encompasses personal data recorded at all stages of interaction with us, including recruitment, application submission, service provision, and any other interaction.

2.2. Suppliers/Partners: Personal data provided to us in cases of cooperation.

2.3. Applicants: Personal data provided in any form as part of an application submitted by you.

2.4. Visitor Individuals: Personal data provided during the admission process.

2.5. Visitors/Users of Digital Channels: Personal data and/or records of actions performed by them on our telephone hotline, internet communication chat, or website.

2.6. Personal data collected by the video surveillance system and access systems.

2.7. Personal data provided by temporary participants, contractors, sub-contractors, and various forms within the project.

2.8. Personal data provided for the continuous service of the Tenant and the Lessor.

2.9. Personal data submitted by employees.

2.10. Any personal data recorded by you as part of receiving our public services.

3. Purpose and Basis of Collection:

- To fulfill of the requirements and duties established by the current legislation of Georgia and the Georgian National Energy Regulatory Commission.
- To perform the obligations inherent in bilateral relations, supported by the will and written consent of the data subject.
- To ensure the safety of our assets, employees, and service personnel, safeguarding territory and buildings, and protecting movable equipment and supplies.

4. Transfer of Data to Third Parties: Data is transferred to third parties solely for the purpose of serving subscribers, accounting, and settling debts, including:
- Subscriber's internal and identification number, subscriber initials, debt, and balance data.
- Law enforcement agencies, in accordance with the requirements provided for by law.

5. Protecting Privacy:
   For us, the safety of individuals associated with us is so important, whether it's during a one-time visit or long-term cooperation or receipt of our services.
   Therefore, we take responsibility to:
- Treat any personal information provided by you as confidential, unless otherwise specified during the initial contact.
- Ensure the security and protection of the personal data you provide.
- Provide you with information regarding the processing of personal data upon request, with a relevant response within 10 business days.
- Contact us about any updates, changes, deletions, additions, or related issues regarding your personal data through official channels (Service Center, Call Center, Online Forms).

6. Data Storage:

Data is stored in specially protected spaces tailored to each process, where only authorized individuals have access. Access is logged and controlled in accordance with recognized "Information Security" protocols.

Printed materials, including application forms, attachment files, contracts, various valuable printed materials, signed documents, partnership agreements, etc., are kept under the supervision of the process owner in secure areas such as closed rooms, cabinets, or safes. These materials are transferred to the archive no later than one year after the request is fulfilled. The archive is maintained for a minimum of 5 years and subsequently destroyed using appropriate procedures.

The duration and terms of digital data storage vary and are processed according to the following norms:

Subscribers' Personal Data:

- In a digital form, data is stored in a specialized database protected by licensed and recognized ERP software compliant with international requirements.
- Access to data entered into the ERP program is restricted to authorized personnel only.
- Digitally, after one year, the data is transferred to the archive where it remains until destruction.
- Additionally, a portion of the data may be processed on the personal computers of authorized individuals within specific projects or business tasks. After completing the project or task, the personal information is deleted from personal computers, and a copy is stored on the file server for one year before being transferred to the archive for destruction.

Information about Suppliers/Partners:

- In digital form, data is stored for at least 3 years after the expiration of the legal relationship period, unless otherwise specified in another agreement.
- Data is stored both in the ERP program and on the file server.
- Data destruction is conducted according to the terms of the contract; if not specified, data will be destroyed after 5 years through the data destruction process.

Applicants:

- An individual who provides their own information in an application. Their data is stored according to the contents of the application.
- Any person may request access to, correction, update, addition, blocking, deletion, and destruction of information regarding the processing of their personal data, unless it contradicts other applicable rights.

Visitor Individuals:

Video Surveillance System:

- Processing of biometric personal data by the Video Surveillance System is conducted based on the facility's criticality, with relevant retention periods not exceeding 15 days for a period of one year, special warning stickers are placed on such objects.
- In the event of an incident, fragmented video recordings from the video surveillance system are removed. These recordings are stored for a period of 2 years after the incident's full resolution.

Pass Access Process:

- During the pass access process, the personal data of individuals is recorded in the relevant journal, including name, surname, personal identification data, vehicle identification data, entry and exit times, and reason for a visit. This data is stored for one year before being sent to the shredder for destruction.

Visitors to Digital Channels:

- For individuals using our website and web services, we store their actions and operations to improve service and security.
- When visiting our website, we retain the following information: IP address, visitor's system and software data, protocol, and connection start and end dates.
- Some pages on our website contain forms where you can input personal data such as name, surname, phone number, and email. We take care to protect this data by adhering to the following rules:

- We use the encrypted HTTPS (TLS/SSL) channel between our website and you to prevent third-party access to our correspondence.
- The information you provide is collected on our servers, accessible only to authorized personnel.

External software, such as Jivochat, is utilized on our website:

- Jivochat facilitates fast and flexible communication and stores the data you transmit.
- Data transferred to Jivochat is retained throughout our communication and is not deleted unless relevant instructions are received from your end.

Website Analytics:

- For website analysis, we utilize Google Analytics to track login origins, technical data collected from visitors, and other statistical metrics.
- This information is gathered on the Google platform, and we only utilize summarized accounts.

7. Consent:

- Upon entering our workspace, individuals agree to abide by all internal privacy policies and "information security" requirements.
- By traversing our premises, individuals automatically consent to the provisions outlined by warning signs, including the use of video surveillance systems.
- Utilizing our website and digital channels implies consent to the use of information provided in accordance with this Policy.

8. Delete and Destroy Data:

If you believe your data is inaccurately stored in our database and requires deletion, please contact us in writing at the GWP service center or submit an application through the website. Alternatively, you can reach out to the data protection officer via email at dpo@gwp.ge. Upon request, if we lack a legal basis for retaining your personal data, it will be promptly removed from our databases within 10 working days. Otherwise, we will inform you of the legal purposes of processing and provide avenues for resolution.
Data destruction follows a standardized procedure, including the following:

Destruction of Physically Printed Material:

- Printed material with a shelf life exceeding 5 years is requested for destruction upon expiration.
- Expired printed material (maculature) is annually collected in a designated protected box.
- The quantity of relevant records is documented, and the maculature is transferred to the appropriate box under the supervision of administration and security officers for incineration at the designated location.
- Following destruction, a protocol is prepared where those responsible for the destruction sign and confirm its authenticity.
- Postponement of printed material destruction may occur if an incident or legal issues require re-examination or continued storage within the 5-year period. A decision is made by the relevant commission.

Destruction of Digital Data:

- Archives stored for 10 years or more undergo permanent deletion.
- Deletion is performed on entire archive files.

9. Incident Management:

If you disagree with our Privacy Policy or believe that your personal data has been unlawfully used by us, not in good faith, in violation of privacy, or in any other suspicious manner, please

immediately contact the Data Protection Officer at dpo@gwp.ge or leave a letter for our Data Protection Officer to be forwarded to our service centers.

10. Cookies:

To enhance the functionality of our websites (gwp.ge, mygwp.ge, portal.gwp.ge) and electronic services, we utilize cookies. These cookies aim to streamline website functionality and digitally gather actions recorded on our website for further analysis and development.

A cookie is a file stored on your computer device, enabling our website to remember specific types of information used each time the website is loaded and visited.

If you do not wish to use such cookies or delete them, you must do so yourself through the web browser (web browsing program) to clear and/or disable your cookies. Please note that disabling cookies may affect the comprehensive service provided.

Website: gwp.ge

Name	Provider	Purpose	Duration
PHPSESSID	GWP	Session Control	Session Period
FB Settings	Facebook	Enabling Facebook analytics to monitor visitor behavior and improve service	1 year
Google Analytics	Google	Improving integration and search with Google search engine	1 year
JIVOCHAT Settings	JIVOCHAT	Online communication tool (chat)	1 year

11. Entry into Force of the Policy:

The Privacy Policy comes into effect upon its publication and remains applicable until its next amendment. Changes may be made at any time. Website: www.gwp.ge.