



PERSONAL DATA PROTECTION POLICY

Public Power Corporation S.A. is a Société Anonyme with the distinctive title “PPC S.A.” (hereinafter called PPC), having its registered seat in Athens, 30 Chalkokondyli st., GR-104 32, legally represented, with TRN:090000045, Tax Office: Athens Tax Office for Commercial Companies and G.E.MI No 786301000, website: <https://www.dei.gr>.

PPC respects the privacy and ensures the protection of personal data. The personal data of its customers are protected using high standards and safety procedures so as to prevent accidental loss and unauthorized disclosure or access, in the context of the applicable legal framework.

By May 25th, 2018, the General Data Protection Regulation 2016/679 (hereinafter called “GDPR”) has entered into force. PPC, as Data Controller, informs its customers that the company or/and third parties acting on its behalf will process their personal data, in the context of their transactions related to PPC products or services.

1. Which personal data is processed by PPC?

PPC collects and processes:

- a) Personal data, in the context of the contractual relationship of the company with its customers, business partners, and in general persons involved in transactions with PPC, which you have provided to the Company’s Services or voluntarily entered in electronic form and in particular,
 - ✓ Identification data: name, surname, father’s name, date of birth, ID No or Passport No, TRN No, or other identification elements).

- ✓ Contact data: postal address, e-mail address, mobile number or other telephone numbers, social media, etc.
- ✓ Data concerning the relation with the supplied property or other facility/equipment to which power or services is/are supplied: owner, tenant, user etc.
- ✓ Data concerning the health of the customer or/and his dependent family members: category of vulnerable customers, Social Residential Tariff.

b) Personal data that are automatically collected upon your approval when you browse, IP address, type of device, web browser, web page redirection, web pages visited by you, date and time of visit. For further information, you may see the [Cookie Policy](#).

c) Personal data that you provide on a voluntary basis when participating in surveys and contests or when entering your data to a contact form or chatbox of PPC (software interactive robot).

d) Personal data that you provide on a voluntary basis to third-party sources (e.g. social media, internet search engines) by consenting to their transfer to companies interested in advertising and promoting products, such as PPC, in accordance with the terms provided for each time.

It is noted that customers are obliged to promptly inform PPC about any change in their above personal details.

2. Legal grounds on processing personal data

Unless otherwise stipulated at the time of personal data collection, the legal grounds on processing are the following:

- a)** your consent for the processing of personal data (Article 6 (1) (a) of the GDPR), as provided for/requested each time.

PPC collects and processes your personal data with your consent and provided that you have been previously informed through the present policy about the type of data, the purpose, the extent of processing, and the recipients of the data. Your consent may be withdrawn at any time.

- b)** processing is necessary for the fulfillment of our contractual relationship with you (Article 6 (1) (b) of the GDPR),
PPC processes your personal data in the context of the performance of your contract or when entering a new contract with you, as well as to take action to respond to your requests. This processing enables us to call you and send you text messages aimed at informing you, resolving problems, and improving our services always for your own benefit.
- c)** processing is necessary for compliance reasons with the legal obligation of the company (tax, insurance, accounting requirements under the law, etc. (Article 6 (1))
PPC may process your personal data in order to comply with its mandatory legal obligations, including, for example, accounting and tax requirements, which are implemented on the basis of its internal policies and procedures.
- d)** processing is necessary for the purposes of the legitimate interests pursued by the company (Article 6 (1) or (f) of the GDPR).

In the context of supporting PPC's legitimate business interests, we process personal data to prevent fraud, maintain the security of our network and services, and improve them.

Finally, when you visit PPC's facilities and Stores, we collect CCTV data for the safety of **persons and goods** in line with the provisions of the GDPR and the Guidelines issued by the Data Protection Authority.

3. Purposes of Processing

PPC collects and processes personal data for the following purposes:

- ❖ **Conclusion and performance of Contract between PPC-Customer or PPC-Partner** for products and services offered
- ❖ **Processing and handling of requests** concerning available products and services
- ❖ **Electronic payment option**, via the company's website or payment service providers, and electronic management of your bill

- ❖ **Updates on new PPC products and services**, the conduct of customer satisfaction surveys, advertising campaigns, energy analysis, and market layering, or other promotional activities or events
- ❖ **Participation of customers in contests and other activities organized by PPC**
- ❖ **Compliance of the company with the obligations deriving from the law** (tax, insurance, accounting obligations, etc.)
- ❖ **Establishment, exercise, or defense of any kind of legal claims of the company**, directly or through its external legal associates
- ❖ **Performance of a task carried out in the public interest**
- ❖ **Profiling** for optimal response to your needs and personalization of our updates and proposals based on your preferences, as well as for the provision of energy-saving pieces of advice, etc. Your profile is created by analyzing information on your browsing, search patterns, and interactions with our company. You interact with our company when you apply for our products or services, you visit one of our websites, you subscribe to our publications, you participate in a contest, promotion or survey, or you send us an email.

4. To whom do we share your data?

Access to the personal data of PPC customers is granted to PPC employees, who are responsible for the management of contracts, as well as for the handling of requests, comments, complaints, submitted either in hard copy or digital format.

The Company does not transfer or disclose your personal data to third parties unless it concerns:

a) Businesses (within the EU or the European Economic Area) to which PPC has entrusted, in whole or in part, the execution of your personal data processing on its behalf and which provide adequate safeguards based on their published privacy policies and/or explicitly abide by confidentiality either (a) in the context of a contractual relationship which defines the subject matter, purpose, duration of the processing, the type of personal data they process and the rights of the company, or (b) under a regulatory obligation of confidentiality, including, but not limited to:

- Financial Institutions, legally licensed Payment Institutions, and Electronic Money Institutions and Payment Service Providers (e.g. DIAS) for the purposes of electronic payment of electricity bills or other services provided by PPC.
- Companies providing invoice printing and mailing services and in general contract performance support services.
- Advertising, market research, and promotion companies for PPC products and services via phone calls, emails, SMS, and any other legal and appropriate means of multimedia communication
- Companies to which PPC outsources services, such as telephone or electronic customer support, customer satisfaction surveys
- Associated lawyers, law firms, bailiffs, and notaries managing and handling legal claims in case of non-performance of your obligations under the contract
- Debtor notification companies under Law 3758/2009, as in force each time, which are registered with the relevant register, aiming at further informing you, as debtor, and negotiating with you about the time, mode, and other terms of repayment of your overdue debt
- Companies providing physical records' digitalization and management (storage, destruction) services
- Companies providing innovative solutions, development services, maintenance services, IT applications customization, e-mail services, social media or search engines, and web hosting services, including cloud services
- Companies within PPC Group, subsidiaries of PPC, as well as HEDNO.

b) Alternative Suppliers: in accordance with the provisions of the Electricity Supply Code, when switching Supplier, in case of overdue debts with another Supplier.

c) Judicial Authorities and Public Authorities or Bodies: in the context of the exercise of official duty, tax authorities, supervisory bodies, mediation bodies.

d) Companies outside the EU: PPC or its authorized partners may transfer part of the personal data collected and processed to Processors in third countries outside the European Union. In this case, PPC will ensure appropriate guarantees and all safeguards for the processing of personal data outside the European Union, and will fully notify the Hellenic Data Protection

Authority, if required, in full compliance with the relevant regulatory provisions of the GDPR and the applicable legislation in general.

5. How long will we keep your personal data?

PPC will keep all the above data, in accordance with the current institutional framework and in particular pursuant to Law 1040/1980 (National Official Gazette Volume A', issue 76 / 3.4.1980), which is valid and applicable specifically for PPC.

6. How do we protect your personal data?

PPC makes use of technical, physical, and organizational security measures with a view to ensuring the integrity and confidentiality of personal data. Moreover, PPC implements data protection security technologies to prevent unauthorized access, improper use, alteration, unlawful or accidental destruction, accidental loss and continues to strengthen its security procedures, including, inter alia, as per case:

- a) the pseudonymization and encryption of personal data;
- b) the ability to ensure the confidentiality, integrity, availability, and reliability of processing systems and services on a continuous basis;
- c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- d) a procedure for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures that ensure the security of processing.

7. How do we ensure that Processors respect your data?

The Company has lawfully ensured that processors carrying out processing on its behalf meet the requirements and provide sufficient guarantees for the implementation of the appropriate technical and organizational measures, in such a manner that processing will ensure the protection of your rights.

In particular, the Processors provide to part of their personnel access to the personal data subject to processing only to the extent that this is absolutely necessary for the execution, management, and monitoring of the Main Contract. They ensure that access to the data is strictly limited to a number of authorized persons who are absolutely necessary for the purposes and execution of the Main/body of the Contract. They ensure that the persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and in particular that:

- they provide adequate guarantees in terms of technical knowledge and personal integrity to maintain confidentiality,
- they are under the direct supervision of the Processor and comply with the appropriate protection measures,
- they have been informed and have committed themselves in advance to the confidentiality of the data,
- they have been informed of and follow the instructions of the Processor regarding the processing of the data and will be informed of any new instructions that the Controller will address to the Processor,
- they have been informed of and comply with the applicable laws and regulatory provisions for data protection,
- they have been informed that any breach of their obligations may give rise to personal liability (civil and criminal).

8. What are your rights?

We inform you that, according to the current legislation, you have and can exercise the following rights:

- **The right to be informed and access your data:** you have more detailed and clearer information during the collection of your data on their processing and your right to access your data
- **The right to rectification:** you can rectify inaccurate data, as well as fill in incomplete data that concerns you
- **The right to restriction of processing:** PPC guarantees that it restricts processing, under specific conditions

- **The right to object to processing:** you can refuse and object to any further processing of your personal data
- **The right to erasure:** you can request the erasure of your data, provided that it is not held for a specific legitimate and stated purpose
- **The right to data portability:** you can ask PPC to send and/or transfer personal data to another Processor, under specific conditions.

The exercise of one of your above rights shall be carried out upon submission of your relevant request in writing to our company (see the relevant [form for the exercise of data subject's rights](#)) at the e-mail address: customercare@dei.gr, to which we undertake to respond within one (1) month after its receipt. It is noted that this deadline may be extended for two (2) additional months depending on the complexity of your request and the number of requests received in general. Moreover, you may submit your request in any PPC Store.

Furthermore, PPC undertakes to inform you, without undue delay, and in any case within 72 hours, of any breach of your personal data, which is likely to result in a high risk to your rights and freedoms and provided that this breach does not fall within one of the exceptions expressly stipulated by law. In any case, if you become aware of a data breach, you have the right to have recourse to the Hellenic Data Protection Authority (1-3 Kifissias Ave., GR-115 23 Athens, tel. +30 210 6475600, e-mail address: contact@dpa.gr).

PPC fully cooperates with the HDPA on all issues pertaining to personal data, in order to ensure the highest possible level of protection and to assist in suppressing or otherwise addressing cases of data breaches or unauthorized data processing.

9. Who can you contact for any queries/issues?

For any clarifications or information regarding the collection and processing of your personal data by PPC, you may contact the Office of the Data Protection Officer of PPC at: dpo.office@dei.gr

PPC reserves the right to review/update the present document and the general framework for processing personal data, in compliance with any amendments to the applicable

legislation and the applicable regulatory framework, and proceeds to the relevant update notices. For this reason, you are advised to regularly visit this webpage for your information