ATTACHMENT B

Community Choice Aggregation Program

Data Protection Plan

Good Energy, L.P.

I. Introduction

Good Energy, L.P. ("Good Energy") has developed a Community Choice Aggregation Program to help municipalities facilitate market-based deployment of clean energy resources, increase retail competition for residential and small commercial customers, and provide individuals and businesses with greater ability to manage their energy usage and bills (the "Program"). The Program will also allow local municipalities, in cooperation with Good Energy, to promote the New York State Public Service Commission's (the "Commission") goals in its Reforming the Energy Vision proceeding for an energy system that is cleaner and more dynamic.

Before being implemented, the Program must be reviewed and approved by the Commission to ensure that the Program complies with the requirements of the Commission's *Order Authorizing Framework for Community Choice Aggregation Opt-out Program* issued on April 21, 2016 (the "CCA Order").[1] Consistent with the CCA Order, Good Energy has developed this Data Protection Plan to ensure that customers' confidential information obtained as part of operation of the Program will be protected from disclosure and/or inappropriate use.

II. Elements of the Plan

1. Access to Customer Data

As part of the Program, Good Energy, local designees of participating municipalities, and energy service companies ("ESCOs") selected to provide power and natural gas for the Program (collectively, "Data Administrators") will receive access to certain information on file with a customer's local distribution company ("LDC"), including, among other things, the customer's name, mailing address, and energy usage history ("Customer Data"). In particular, depending on the status of implementation of the Program, LDC's will provide three types of Customer Data to Data Administrators: aggregated customer and consumption data, customer contact information, and detailed customer information. Each type of Customer Data is described more fully below.

a. **Aggregated Customer Data** – contains general usage information for all residents within a municipality that are eligible to participate in the Program, including the number of customers by service class, the aggregated peak demand (kW) (for electricity) by month for the past 12 months, by service class to the extent possible, and the aggregated energy (kWh) for electricity or volumetric consumption for gas by month for the past 12 months by service class.

b. **Customer Contact Information** – comprises certain contact information for the provision of opt-out notices, including the customer of record's name, mailing address, telephone number, account number, and primary language (if available), and any customer-specific alternate billing name, address, and phone number.

c. **Detailed Customer Data** – contains specific consumption information and/or gas profiles for all individual customers who elected not to opt-out of the Program during the

[1] Case 14-M-0224: *Proceeding on Motion of the Commission to Enable Community Choice Aggregation Programs*, Order Authorizing Framework for Community Choice Aggregation Opt-out Program (Issued Apr. 21, 2016).

opt-out period, including usage data and low-income status. To the extent available, the following information will be provided by the LDC according to the general standards for transfers of data to ESCOs through the electronic data interchange ("EDI"):

i. Consumption history for an electric or gas account shall include:

1. Customer's service address;
2. Electric or gas account indicator;
3. Sales tax district used by the LDC and whether the LDC identifies the customer as tax exempt;
4. Rate service class and subclass or rider by account and by meter, where applicable;
5. Electric load profile reference category or code, if not based on service class, whether the customer's account is settled with the ISO utilizing an actual hourly or a class shape methodology, or Installed Cpacity tag, which indicates the customer's peak electricity demand;
6. Customer's number of meters and meter numbers;
7. Whether the customer receives any special delivery or commodity "first through the meter" incentives, or incentives from the New York Power Authority;
8. The customer's Standard Industrial Classification code;
9. Usage type (kW or therm), reporting period, and type of consumption (actual, estimated, or billed);
10. 12 months, or the life of the account, whichever is less, of customer data via EDI and , upon separate request, an additional 12 months, or the life of the account, whichever is less, of customer data via EDI or an alternative system at the discretion of the LDC, and, where applicable, demand information; if the customer has more than one meter associated with an account, the LDC shall provide the applicable information, if available, for each meter; and
11. Electronic interval data in summary form via EDI, and if requested in detail, via an acceptable alternative electronic format.

ii. A gas profile for a gas account shall include:

1. Customer's service address;
2. Gas account indicator;
3. Customer's number of meters and meter numbers;
4. Sales tax district used by the LDC and whether the LDC identifies the customer as tax exempt;
5. The customer's Standard Industrial Classification code;
6. Rate service class and subclass or rider, by account and by meter, where applicable;
7. Date of gas profile; and

8. Weather normalization forecast of the customer's gas consumption for the most recent 12 months or life of the account, whichever is less, and the factors used to develop the forecast.

2. Data Security

Data Administrators will utilize industry standard physical, technical, and administrative controls and procedures to safeguard Customer Data collected as part of the Program and to prevent unauthorized or accidental access, destruction, loss, alteration, or disclosure of, to protect against anticipated threats or hazards to the security, confidentiality, or integrity of, and to permit only the appropriate use of, such customer information.

To protect the confidentiality, integrity, and availability of customers' data, Data Administrators will utilize a variety of industry standard physical and logical access controls, firewalls, password protections, intrusion detection/prevention systems, network and database monitoring, and backup systems. These systems will be designed to cover all networks, servers, computers, notebooks, laptops, PDAs, mobile phones, or other devices that contain Customer Data, or through which Customer Data is made available.

Data Administrators will limit access to customers' data to those persons and entities having a specific business purpose for maintaining and processing such information. Those granted access to a customer's data will be trained on their responsibilities to protect the confidentiality, integrity, and availability of such information.

Data Administrators will work cooperatively with the LDC(s) to implement this Data Protection Plan, and will at a minimum, implement the following actions:

a. Conduct a risk assessment to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of electronic, paper, and other records containing Customer Data and evaluate and improve, where necessary, the effectiveness of their safeguards for limiting those internal and external risks;

b. Timely notify the LDC(s) of any important modifications of this Data Protection Plan within a reasonable amount of time;

c. Review and, as appropriate, revise this Data Protection Plan: (i) at least annually or whenever there is a material change in their business practices that may reasonably affect the security or integrity of Customer Data; (ii) in accordance with prevailing industry practices and applicable law; and (iii) as reasonably requested by the LDC(s). If the Data Administrators modify this Data Protection Plan following such a review, the Data Administrators will promptly notify the LDC(s) of such modifications and will provide the modifications to the LDC(s) in writing upon a LDC's request. The Data Administrators will at no time alter or modify this Data Protection Plan in such a way that will weaken or compromise the confidentiality, security, or integrity of Customer Data;

d. Maintain and enforce this Data Protection Plan in all locations where Customer Data is processed by the Data Administrators;
e. Conduct security testing using a third party to provide monitoring penetration and intrusion testing with respect to Data Administrators systems and promptly provide a copy of the results to the LDC(s), provided that the third party may redact IP addresses and other client names and information;
f. Provide annual security awareness training to all individuals having access to Customer Data and maintain a record of such training; and
g. Implement a standard process for identifying, assessing, and mitigating security risks.

3. Confidentiality

Data Administrators will not sell, disclose, or provide Customer Data to others, including their affiliates, unless such sale, disclosure, or provision is required to operate the Program, is specifically authorized by the customer, or is required by law or court order. If Data Administrators request customer authorization to disclose Customer Data, Data Administrators will first describe to the customer the information they intend to release and provide details concerning the recipient of such information.

Data Administrators will hold all Customer Data in strict confidence and except as otherwise needed for provision of the Program, required by law, or permitted as below, (a) not disclose Customer Data to any other person or entity (including but not limited to ESCOs, subcontractors, and affiliates or members of Good Energy); (b) not process Customer Data outside of the United States; (c) not process Customer Data other than in connection with the Program; (d) not process Customer Data for any marketing purposes other than in connection with the Program; (e) limit reproduction of Customer Data to the extent required for the Program; (f) store Customer Data in a secure fashion at a secure location in the United States that is not accessible to any person or entity not authorized to receive the Customer Data; and (g) otherwise use at least the same degree of care to avoid publication or dissemination of the Customer Data as Data Administrators employ (or would employ) with respect to their own confidential information that they do not (or would not) desire to have published or disseminated, but in no event less than reasonable care. At all times, the Data Administrators will comply with the requirements of the Uniform Business Practices with respect to confidential treatment of Customer Data.

4. Disclosure of Customer Data

Notwithstanding the provisions of Section 3 above, the Data Administrators may disclose Customer Data to those representatives who have a legitimate need to know or use such Customer Data for the sole and limited purposes of administering and/or conducting the Program. Such representatives will first be advised of the sensitive and confidential nature of such Customer Data and agree to comply with the provisions of this Data Protection Plan.

In the event that Data Administrators or any of their representatives receive notice that they have, will, or may become compelled, pursuant to applicable law or regulation or legal

process, to disclose any Customer Data (whether by receipt of oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands, other similar processes or otherwise), Data Administrators will, except to the extent prohibited by law, immediately notify the LDC(s), orally and in writing, of the pending or threatened compulsion. To the extent lawfully allowable, the LDC(s) will have the right to consult with the Data Administrators and the parties will cooperate, in advance of any disclosure, to undertake any lawfully permissible steps to reduce and/or minimize the extent of Customer Data that must be disclosed. The LDC(s) will also have the right to seek an appropriate protective order or other remedy reducing and/or minimizing the extent of Customer Data that must be disclosed.

Data Administrators and their representatives will disclose only such Customer Data which they are advised by legal counsel that they are legally required to disclose in order to comply with such applicable law or regulation or legal process (as such may be affected by any protective order or other remedy obtained by LDC) and Data Administrators and their representatives will use all reasonable efforts to ensure that all Customer Data that is so disclosed will be accorded confidential treatment.

5. Return/Destruction of Customer Data

Upon the expiration of the Program, or as otherwise required by law or Commission order, the Data Administrators will return all Customer Data to the LDC(s), destroy all copies of any Customer Data (including any and all extracts, compilations, studies or other documents based upon, derived from or containing Customer Data) within their or their representatives' possession (including destroying Customer Data from all systems, records, archives and backups), and all subsequent use and processing of the Customer Data by the Data Administrators and their representatives will cease.

Notwithstanding the foregoing, the Data Administrators and their representatives will not erase Customer Data contained in an archived computer system backup maintained in accordance with their respective security or disaster recovery procedures. The Data Administrators will not provide access to or recovery of Customer Data from such computer backup system and will keep all such Customer Data confidential in accordance with this Data Protection Plan.

6. Data Security Incidents

The Data Administrators are responsible for any and all security incidents involving Customer Data that is processed as part of the Program. The Data Administrators will notify the LDC(s) in writing immediately (and in any event within twenty-four (24) hours) whenever the Data Administrators reasonably believe that there has been a data security incident involving Customer Data. After providing such notice, the Data Administrators will investigate the

incident, and immediately take all necessary steps to eliminate or contain any exposure of Customer Data. The Data Administrators will provide the LDC(s) with reasonable assistance and cooperation in the furtherance of any correction, remediation, or investigation of any such data security incidents and/or the mitigation of any damage, including any notification required by law or that LDC(s) may determine appropriate to send to individuals impacted or potentially impacted by such data security incident(s), and/or the provision of any credit reporting service required by law or that LDC(s) deems appropriate to provide to such individuals.

Unless required by law, the Data Administrators will not notify any individual or any third party other than law enforcement of any potential data security incidents involving Customer Data without first consulting with, and obtaining the permission of, the LDC(s). Within 30 days of identifying or being informed of a data security incident, the Data Administrators will develop and execute a plan, with the cooperation of the LDC(s), which reduces the likelihood of a recurrence of such data security incident(s).

7. Ownership of Customer Data

At all times, the LDC(s) will maintain exclusive ownership interest in the Customer Data and the Customer Data will remain the proprietary and confidential information of the LDC(s). Nothing in this Data Protection Plan will be construed as granting or conferring any rights, by license or otherwise, expressly, implicitly or otherwise, under any patents, copyrights, trade secrets or other intellectual property rights of the LDC(s).

8. Additional Protections

The Data Administrators will not create or maintain data which are derivative of Customer Data except for the purpose of performing its obligations under the Program. Customer information collected by the Data Administrators through their websites or other interactions based on those customers' interest in receiving information from or otherwise engaging with the Data Administrators or their partners will not be considered Customer Data or a derivative of Customer Data for the purpose of this Data Protection Plan. The Data Administrators will not collect or retain customer account numbers through such interactions associated with the Program.

The Data Administrators will comply with all applicable privacy and security laws to which it is subject, including this Data Protection Plan.

The Data Administrators will safely secure and/or encrypt all Customer Data during storage and transmission.

The Data Administrators will have in place appropriate and reasonable processes and systems, including this Data Protection Plan, to protect the security of Customer Data and to prevent a data security incident, including, without limitation, a breach resulting from or arising out of the Data Administrators' internal use, processing, or other transmission of Customer Data, whether between or among their representatives, subsidiaries and affiliates, or any other person or entity acting on behalf of the Data Administrators.

The Data Administrators will work cooperatively with the LDC(s) to implement this Data Protection Plan, including: establishing policies and procedures to provide reasonable and prompt assistance to LDC(s) in responding to any and all requests, complaints, or other communications received from any individual who is or may be the subject of a data security incident involving Customer Data to the extent such request, complaint or other communication relates to the Data Administrators' processing of such individual's Customer Data; and establishing policies and procedures to provide all reasonable and prompt assistance to LDC(s) in responding to any and all requests, complaints, or other communications received from any individual, government, government agency, regulatory authority, or other entity that is or may have an interest in the Customer Data, data theft or other unauthorized release of Customer Data, disclosure of Customer Data, or misuse of Customer Data to the extent such request, complaint or other communication relates to Data Administrators' processing of such individual's Customer Data.

II. Conclusion

The Data Protection Plan meets all of the requirements of the CCA Order. Good Energy looks forward to the approval of this plan by the Commission so it may work with interested municipalities to launch the Program and bring the benefits of low cost energy, renewable power, and electricity choice to individuals and communities throughout New York State.