GDPR compliance

As per the General Data Protection Regulation (GDPR), Hello Energy is entrusted with the responsibility of safeguarding customer data, ensuring its confidentiality, integrity, and availability. Utility data, including consumption patterns and personal details, holds sensitive and confidential information that demands robust security measures. Implementing adequate data security measures ensures compliance with GDPR and fosters customer trust and protects against potential data breaches. Our data security measures are:

1. Data Minimization: Hello Energy collects and processes only the necessary data required to fulfill our services.

2. Access Control: Hello Energy uses 2 factor authentication (2FA) to limit data access to authorized personnel only. We use role-based access controls (RBAC) to ensure that employees only have access to the data necessary for their job functions. And this process is reviewed regularly, to ensure it aligns with the current job roles of the employees.

3. Employee Training and Awareness: Hello Energy provides regular training sessions to employees on data protection best practices, GDPR requirements, and the importance of maintaining data security.

4. Vendor Management: Hello Energy uses a code of conduct for third-party vendors and service providers handling utility data.

5. Data Retention and Disposal: Hello Energy uses clear policies for data retention and disposal, ensuring that personal data is not kept for longer than necessary for the purposes for which it was collected. On request by client we will delete data from our systems.

6. Regular Security Updates and Patch Management: Hello Energy keeps systems, software, and applications up to date with the latest security patches and updates to address known vulnerabilities and mitigate the risk of exploitation by malicious actors.

7. Data storage: Hello Energy software runs on AWS. The servers and databases are located in Frankfuhrt, Germany.

Adhering to these data security measures Hello Energy facilitates compliance with GDPR requirements and demonstrates a commitment to protecting customer data and upholding their privacy rights. By prioritizing data security, utility companies can enhance trust, mitigate risks, and safeguard sensitive information effectively.

Rotterdam. February 2024.