DELIVERABLE 2.2

Privacy by Design

Version 1.1

Elena Malakhatka, Chalmers

Marwa Maghnie, RWTH

25 February 2025

1. Introduction

The ECom4Future project focuses on fostering sustainable, resilient, and user-centric energy communities through innovative technologies and collaborative frameworks. As energy systems transition toward decentralized models, energy communities emerge as key actors in enabling localized energy generation, distribution, and consumption. These communities not only empower individuals to become prosumers but also facilitate sustainable energy practices at the local level. However, this transformation raises critical concerns regarding data privacy, especially considering the large volumes of sensitive user data generated within these networks. The ECom4Future project aims to address these concerns by integrating Privacy by Design (PbD) principles into the development of digital platforms and operational processes for energy communities.

Privacy plays a pivotal role in the successful deployment and acceptance of energy communities. Local energy markets and smart grids rely heavily on the collection, sharing, and processing of user data, such as energy consumption patterns, user identities, and transactional information. Without robust privacy mechanisms, these data exchanges pose risks related to unauthorized access, data breaches, and potential misuse. Privacy concerns can also become a significant barrier to user participation, as prosumers may be reluctant to share their data without adequate protection measures. Implementing Privacy by Design ensures that privacy is not an afterthought but a fundamental component embedded into the core of systems and processes. This not only enhances user trust but also ensures compliance with regulations such as the General Data Protection Regulation (GDPR) and relevant cybersecurity standards.

The primary objective of this report is to explore the application of Privacy by Design principles within energy communities, focusing on both technical and organizational aspects. The report aims to provide a comprehensive overview of the legislative frameworks, privacy models, and implementation strategies essential for safeguarding user data in local energy markets. Additionally, it will analyze key challenges related to privacy, including identity protection, information security, and the integration of privacy solutions across different market phases. By examining a relevant case study and outlining practical tools and techniques, the report seeks to translate privacy requirements into actionable platform features. Ultimately, this report will offer recommendations for policymakers, developers, and energy community stakeholders on how to balance data utilization with robust privacy protections, thereby fostering greater prosumer participation and trust in decentralized energy systems.

2. Core Principles of Privacy by Design

Privacy by Design (PbD), initially conceptualized by Dr. Ann Cavoukian (2011), is a proactive approach that ensures privacy is embedded into the design and operation of technologies, systems, and business practices. The framework rests on seven foundational principles:

- **Proactive not Reactive**: Preventative not Remedial: Anticipates and mitigates privacy risks before they materialize. In energy communities (ECs), this means identifying potential privacy risks related to energy consumption data and deploying early safeguards
- **Privacy as the Default Setting:** Ensures that user data is protected by default without additional user actions. For example, default configurations in smart meters should anonymize user data unless explicit consent is provided.

- **Privacy Embedded into Design:** Privacy measures are integrated into the architecture of EC platforms. Platforms like blockchain-enabled peer-to-peer trading systems are designed to secure transactions without exposing personal data.
- **Full Functionality — Positive-Sum, not Zero-Sum:** Balances privacy with operational performance. In ECs, this means achieving efficient energy distribution while safeguarding user identities.
- **End-to-End Security — Full Lifecycle Protection:** Protects data throughout its lifecycle—from collection, storage, to deletion. For ECs, this includes robust encryption of energy usage data and secure data disposal mechanisms.
- **Visibility and Transparency — Keep it Open:** Systems must be transparent, allowing stakeholders to verify compliance. Energy communities can achieve this through transparent privacy policies and regular audits.
- **Respect for User Privacy — Keep it User-Centric:** User needs and privacy preferences are prioritized. This involves providing easy-to-understand privacy controls and consent mechanisms.

The integration of PbD principles is essential for energy communities to manage sensitive user data effectively. For example:

- **Proactive Privacy:** Risk assessments should be conducted when implementing local energy trading systems to mitigate threats related to data leaks.
- **Default Privacy Settings:** Default configurations in local energy market platforms should limit data visibility to authorized participants only.
- **End-to-End Security:** Encryption protocols and federated learning approaches can ensure data protection throughout the lifecycle.
- **User-Centric Design:** Platforms must offer user-friendly dashboards where prosumers can manage their privacy settings and data-sharing preferences.

3. Legislative and Cybersecurity Frameworks

The General Data Protection Regulation (GDPR), enforced since May 2018, is the primary legal framework governing data protection and privacy within the European Union (EU). GDPR plays a crucial role in local energy markets by ensuring that personal data, such as energy consumption patterns and transaction histories, is processed lawfully, fairly, and transparently. For energy communities (ECs), this means:

- **Data Minimization:** Only essential data should be collected for operational purposes, limiting unnecessary exposure.
- **Explicit User Consent:** Prosumers must provide clear consent for data processing activities, with the ability to withdraw consent at any time.
- **Right to Data Portability:** Users should be able to access and transfer their data across platforms without compromising privacy.
- **Data Protection Impact Assessments (DPIAs):** ECs must conduct DPIAs for high-risk processing activities, such as peer-to-peer energy trading, to identify and mitigate potential privacy risks.

Non-compliance with GDPR can lead to substantial fines, reduced trust among participants, and operational setbacks. Thus, GDPR compliance is not only a legal necessity but also a strategic imperative for the growth of energy communities.

Given the increasing digitization of energy markets, robust cybersecurity frameworks are essential to protect sensitive data. Key frameworks include:

- **NIS Directive (Directive on Security of Network and Information Systems):** Establishes measures to achieve a high level of network and information security across the EU. ECs handling critical energy infrastructure must comply with its requirements, including incident reporting and risk management (European Union Agency for Cybersecurity, ENISA).
- **ISO/IEC 27001:** Provides a framework for an information security management system (ISMS) that helps ECs manage security risks associated with energy data sharing. Implementing ISO/IEC 27001 ensures:
    - Confidentiality and integrity of data.
    - Secure communication protocols for peer-to-peer transactions.
    - Continuous monitoring and improvement of security practices
- **Cybersecurity Act (EU Regulation 2019/881):** Introduces an EU-wide cybersecurity certification framework, enhancing the security of ICT products, services, and processes. For ECs, certification ensures that digital energy trading platforms adhere to high security standards.
- **Smart Grid Interoperability Panel (SGIP) Standards:** Focuses on cybersecurity measures specific to smart grids, including end-to-end encryption, secure authentication, and resilient communication protocols.

Energy community policies at both national and EU levels significantly influence privacy practices. The Clean Energy for All Europeans Package promotes the establishment of ECs, emphasizing consumer rights and data protection. Key policy considerations include:

- **Consumer Empowerment:** Policies ensure that prosumers have full control over their data, with transparent mechanisms for consent and data access.
- **Interoperability and Standardization:** EC policies encourage adopting interoperable systems that comply with GDPR and international cybersecurity standards.
- **Local Energy Market Regulations:** National regulations may specify additional privacy requirements tailored to local energy markets, addressing unique operational contexts and data-sharing practices.

Moreover, ISO 31700-1:2023 aligns with these policies by providing comprehensive guidelines for embedding privacy requirements into system designs, ensuring that privacy remains a core consideration throughout the lifecycle of energy community platforms.

4. Privacy Models in Local Energy Markets

Privacy models play a crucial role in managing user data within local energy markets. The two most prominent models—Peer-to-Peer (P2P) and Hierarchical Privacy Models—offer distinct advantages, challenges, and levels of user control. Understanding these models is essential for designing secure, efficient, and user-centric energy communities.

4.1 Peer-to-Peer (P2P) privacy model

Peer-to-Peer (P2P) privacy models enable direct energy trading between prosumers without the need for intermediaries. This decentralized model fosters autonomy and user engagement, allowing participants to manage their own energy data and transactions. A significant benefit of P2P models is user empowerment, as prosumers retain complete control over their data (Capper et al., 2022). Moreover, P2P frameworks enhance flexibility, supporting dynamic pricing and customized trading agreements. Technologies like blockchain further bolster decentralized trust, providing secure and transparent transaction records without relying on a central authority.

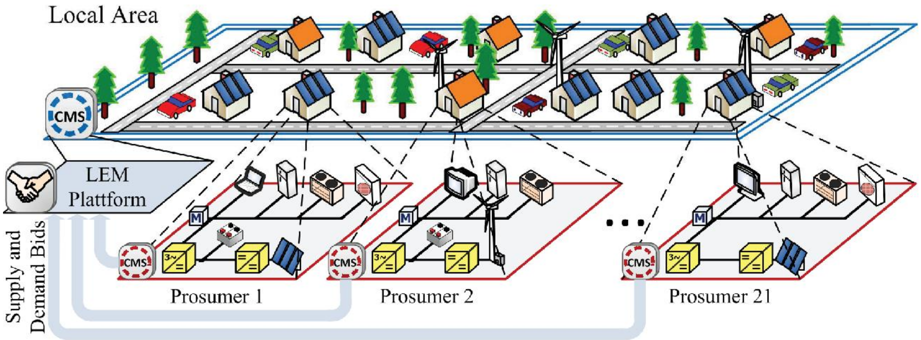

Figure 1. Peer-to-Peer (P2P) privacy model

However, P2P models come with notable challenges. The absence of intermediaries can expose user data to security risks. Complex security requirements also arise, as securing data across decentralized networks necessitates advanced encryption and authentication mechanisms (Zhang et al., 2021). Additionally, scalability can be a concern, as managing numerous transactions in a decentralized system is resource-intensive. Despite these challenges, P2P models are highly suitable for community microgrids where real-time, localized energy exchanges are prioritized (Kazmi et al., 2021).

4.2 Hierarchical Privacy Models: Benefits in Structured Energy Markets

In contrast, Hierarchical Privacy Models follow a tiered approach where a central entity, such as a utility provider or community manager, oversees data processing and energy trading. This centralized structure offers improved scalability, simplifying transaction management and enabling broader market participation (Faia et al., 2024). A key advantage is consistent data governance, ensuring uniform compliance with privacy standards such as GDPR and ISO 31700-1:2023 (Alqahtani & Mustafa, 2023). Hierarchical models also reduce operational complexity by delegating security management to central authorities, easing the technical burden on individual prosumers.

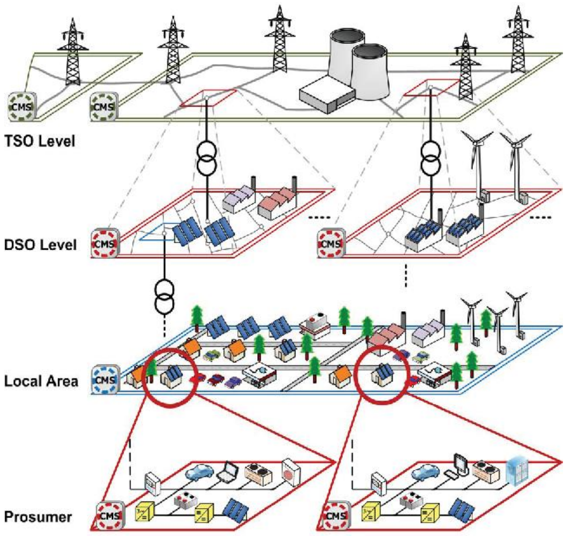

Figure 2. Hierarchical Privacy Models: Benefits in Structured Energy Markets

Nonetheless, these models are not without drawbacks. Reduced user control is a primary concern, as central management can limit prosumers' ability to govern their data. Furthermore, the single point of failure inherent in centralized systems increases vulnerability to data breaches and operational disruptions. Use cases for hierarchical models include virtual power plants and regional energy cooperatives, where a central entity aggregates resources and ensures regulatory compliance.

5. Key Privacy Constraints and Open Challenges

In the evolving landscape of local energy markets, privacy constraints and challenges significantly impact the adoption and effectiveness of energy community (EC) models. As ECs increasingly rely on data-driven technologies, understanding the categories of privacy constraints and addressing the associated challenges becomes essential for safeguarding user trust, ensuring regulatory compliance, and maintaining operational efficiency.

Privacy constraints in energy communities can be broadly categorized into user-centric, legislative, technologically feasible, and algorithmic factors.

- **User-Centric Constraints:** These constraints arise from user concerns regarding the collection, storage, and sharing of personal data. Prosumers are often hesitant to participate in local energy markets if they believe their energy consumption patterns or personal information could be exposed or misused. Building trust through user education, transparent data policies, and robust consent management systems is critical for overcoming these constraints.
- **Legislative Constraints:** Compliance with privacy regulations such as GDPR and adherence to international standards like ISO 31700-1:2023 impose specific requirements on ECs. These include data minimization, explicit consent collection, and ensuring data portability. Legislative constraints often present challenges when national and regional regulations differ, requiring tailored approaches for cross-border ECs.
- **Technologically Feasible Constraints:** Technical limitations in existing energy platforms can restrict the implementation of advanced privacy-preserving mechanisms. For instance, integrating encryption techniques, federated learning models, and secure access control can be costly and complex. Ensuring that these solutions are scalable and interoperable across various energy systems is essential for widespread adoption.
- **Algorithmic Constraints:** Algorithm-driven energy markets, particularly those employing dynamic pricing or demand-response strategies, can inadvertently expose user data. Algorithms must balance operational efficiency with privacy preservation, necessitating the development of privacy-aware computation techniques. For example, differential privacy and homomorphic encryption can enable secure computations without compromising sensitive user information.

Despite advancements in privacy-preserving technologies, several open challenges continue to affect local energy markets:

- **Identity and Data Protection:** Protecting user identities and sensitive data remains a central challenge. Prosumers' participation in P2P transactions and smart grid operations generates identifiable data that could reveal behavioural patterns if not adequately protected. Implementing decentralized identity management systems and anonymization techniques can mitigate these risks. However, striking a balance between data utility and privacy remains an ongoing concern.

- **Information Security Gaps:** Ensuring information security across distributed networks is complex, especially in P2P energy trading systems where multiple nodes interact. The absence of centralized oversight increases the risk of cyberattacks, data breaches, and unauthorized access. Addressing these gaps requires deploying end-to-end encryption, multi-factor authentication, and real-time threat detection systems. Furthermore, continuous security audits and compliance checks are essential for maintaining robust information security protocols.
- **Physical Constraints in Implementation:** Physical infrastructure limitations, such as outdated smart meters, inadequate communication networks, and energy storage inefficiencies, can impede the deployment of privacy-preserving solutions. For example, legacy systems may not support advanced encryption or federated learning models, limiting the ability to implement end-to-end privacy controls. Upgrading infrastructure, adopting standardized communication protocols, and integrating edge computing technologies can address these physical constraints, enhancing the overall privacy and security posture of ECs.

Addressing these constraints and challenges requires a multi-disciplinary approach that combines technological innovation, regulatory compliance, and user-centered design. Future research should focus on developing cost-effective, scalable, and interoperable privacy solutions that align with evolving market demands and user expectations.

6. Tools and Techniques for Privacy Implementation

Implementing effective privacy measures in local energy markets requires a combination of technical solutions and organizational strategies. These tools and techniques ensure that sensitive user data is protected while maintaining operational efficiency and user trust.

6.1 Technical Solutions

- **Data Anonymization and Pseudonymization:** Data anonymization removes personally identifiable information (PII) from datasets, ensuring that individuals cannot be re-identified. This technique is essential in energy communities where energy consumption patterns could reveal sensitive personal details. Pseudonymization, on the other hand, replaces private identifiers with artificial identifiers or pseudonyms. Although pseudonymized data can still be re-linked with additional information, it reduces risks during data processing and sharing (Alqahtani & Mustafa, 2023). For example, in peer-to-peer (P2P) energy trading platforms, pseudonymization allows secure energy exchanges while protecting user identities. Anonymized consumption data can be aggregated for analytical purposes without compromising individual privacy.
- **Encryption:** Encryption ensures that data is unreadable to unauthorized users by converting it into coded formats. End-to-end encryption protects data throughout its lifecycle, from collection at smart meters to transmission and storage. Advanced encryption standards (AES) and public key infrastructure (PKI) are widely used in securing energy data, particularly during transactions in P2P systems (Zhang et al., 2021).
- **Data Aggregation:** Aggregating data from multiple users into broader datasets masks individual contributions, providing valuable insights without revealing specific user details. Aggregation techniques are particularly useful in hierarchical energy market models, where centralized entities manage large volumes of data. For instance, aggregated load

profiles can inform grid management decisions without exposing individual consumption patterns (Kazmi et al., 2021).

- **Federated Learning:** Federated learning allows machine learning models to be trained across multiple decentralized devices without sharing raw data. Instead of moving data to a central server, only model updates are shared. This approach significantly reduces privacy risks associated with centralized data storage. Federated learning is particularly relevant for energy communities employing demand-response optimization algorithms (Zhang et al., 2021).
- **Access Control Mechanisms:** Access control mechanisms regulate who can access specific data and systems. Role-Based Access Control (RBAC) assigns permissions based on user roles within the energy community, ensuring that only authorized personnel can view sensitive data. Combining RBAC with Multi-Factor Authentication (MFA) further strengthens security by requiring multiple forms of verification (Dynge et al., 2023).

6.2 Organizational Strategies

- **User Education:** Educating prosumers about data privacy, security risks, and their rights is vital for building trust. Training programs, workshops, and clear privacy policies enable users to understand how their data is collected, processed, and protected. User education also ensures that individuals can make informed decisions about data sharing, enhancing participation in local energy markets (Heuninckx et al., 2023).
- **Transparency:** Transparency involves openly communicating data processing practices, privacy policies, and security measures to stakeholders. Energy communities should provide accessible privacy notices, regular updates on privacy-related changes, and clear explanations of user rights. Transparent operations not only foster trust but also ensure compliance with GDPR and ISO 31700-1:2023 standards (Capper et al., 2022).
- **Governance Frameworks:** Robust governance frameworks outline policies, procedures, and accountability structures for data privacy management. These frameworks should include:
    - Data Governance Committees responsible for overseeing privacy policies and ensuring regulatory compliance.
    - Regular Privacy Audits to assess and address potential vulnerabilities.
    - Incident Response Plans to mitigate the impact of data breaches and restore normal operations promptly (Faia et al., 2024).

  Governance frameworks also play a critical role in aligning technological solutions with user-centric privacy principles, ensuring that privacy remains a foundational aspect of energy community operations.

Implementing privacy in local energy markets requires a nuanced approach that combines robust technical measures with thoughtful organizational strategies. While technical tools such as data anonymization, pseudonymization, encryption, data aggregation, federated learning, and access control mechanisms provide the necessary infrastructure for safeguarding sensitive data, their effectiveness ultimately depends on how well they are integrated into broader governance frameworks. For instance, encryption and federated learning may offer high levels of security, but without proper user education and transparent communication, prosumers may still feel hesitant about participating in energy markets. Similarly, governance frameworks and transparency efforts ensure regulatory compliance and foster user trust, but these must be adaptable to evolving technological capabilities and user expectations. The interplay between these technical and organizational solutions highlights the need for a holistic approach—one that not only protects data but also empowers users through knowledge, control, and trust. This balance is essential for building resilient and user-centric energy communities that can thrive in a data-driven landscape while maintaining privacy as a fundamental value.

7. Translating privacy requirements into platform features

Translating privacy requirements into practical platform features is essential for aligning energy trading systems with regulatory standards, such as the General Data Protection Regulation (GDPR), while maintaining user trust and operational efficiency. This sub-chapter discusses how GDPR principles are reflected in platform functionalities, ensuring that privacy remains a core aspect of system design and operation.

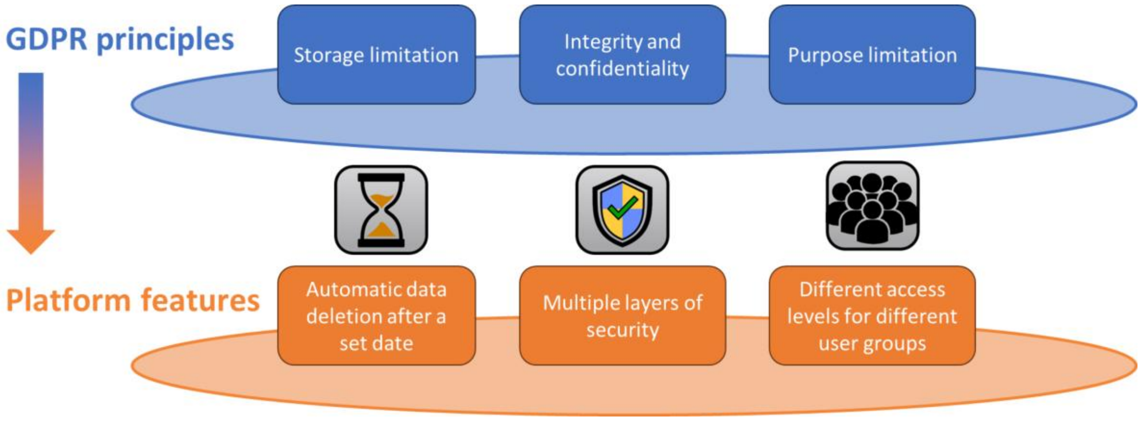
GDPR principles
Storage limitation
Integrity and confidentiality
Purpose limitation
Platform features
Automatic data deletion after a set date
Multiple layers of security
Different access levels for different user groups

Figure 3. Translating privacy requirements into platform features

Three key GDPR principles—storage limitation, integrity and confidentiality, and purpose limitation—form the foundation for designing privacy-compliant energy trading platforms. Each principle corresponds to specific platform features that ensure data protection and regulatory adherence:

1. **Storage Limitation → Automatic Data Deletion After a Set Date:** The GDPR requires that personal data not be stored longer than necessary. To comply with this principle, the platform includes an automatic data deletion feature, which ensures that user data is deleted after a predefined retention period. This minimizes the risk of unauthorized data access and reduces storage costs, while reassuring users that their information will not be kept indefinitely.
2. **Integrity and Confidentiality → Multiple Layers of Security:** Data security is vital for maintaining the confidentiality and integrity of user information. The platform incorporates multiple layers of security, including encryption, secure authentication methods, and real-time threat detection systems. By using these security layers, the platform protects data during transmission and storage, preventing unauthorized access and data breaches. Advanced encryption protocols, such as end-to-end encryption and homomorphic encryption, ensure that data remains secure throughout its lifecycle.
3. **Purpose Limitation → Different Access Levels for Different User Groups:** GDPR stipulates that personal data should only be processed for specified, explicit purposes. To support this principle, the platform implements role-based access control (RBAC), ensuring that different user groups have access only to the data necessary for their role. For example, system administrators may have access to aggregated market data, while

individual users retain control over their specific energy usage information. This approach reduces the risk of data misuse and fosters user trust by limiting unnecessary data exposure.

These platform features not only ensure regulatory compliance but also enhance user experience and participation. For instance, automatic data deletion assures users that their privacy is respected, while multiple security layers protect sensitive transactions, increasing confidence in the platform's reliability. Differentiated access levels also promote a clear governance structure, where users understand who can access their data and for what purposes.

Moreover, these privacy-centric features support scalability and interoperability. As energy communities grow and interact with broader energy markets, maintaining consistent privacy protections across all user groups and data processes becomes critical. The modular design of these features allows seamless integration with existing systems while ensuring continuous compliance with evolving privacy regulations.

Future developments in privacy-preserving energy trading platforms can build upon these foundational features by incorporating adaptive privacy controls based on user preferences. For example, providing users with customizable privacy settings would further enhance user-centric design. Additionally, integrating artificial intelligence (AI) for real-time risk assessments can proactively identify and mitigate emerging privacy threats.

The incorporation of privacy requirements into platform features, as illustrated by the alignment with GDPR principles, ensures that privacy is not an afterthought but a fundamental aspect of system architecture. This approach not only meets regulatory obligations but also builds trust, supporting the sustainable growth of decentralized energy trading systems.

8. Case Study Analysis

Case Study: Privacy-Preserving Renewable Energy Trading System for Residential Communities

This case study focuses on a privacy-preserving renewable energy trading system for residential communities, as detailed in Deng et al. (2022). The system facilitates energy trading among community members by integrating smart home energy management systems (HEMS), community energy management systems (CEMS), and local renewable energy sources (RES). The central market operator oversees market clearing processes, ensuring fair and efficient energy distribution. Privacy preservation is central to this system’s design, incorporating multiple technical and organizational strategies to protect user data while supporting sustainable energy practices.

The trading framework relies on bidirectional communication between smart meters, HEMS, and the market operator. Users' preferences, appliance schedules, and operational constraints are processed locally within the HEMS to generate optimized bidding information. Secure data communication channels link CEMS across different communities with the market operator and local RES, minimizing exposure of sensitive data.

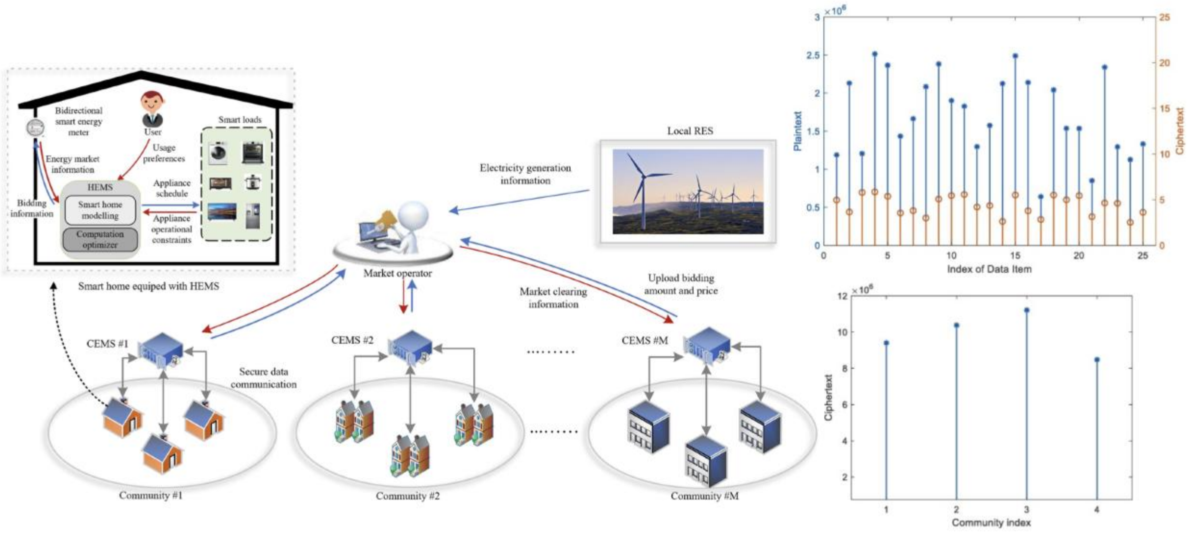

Figure 4. Privacy preserving renewable energy trading system for residential communities (Deng, 2022)

Key privacy strategies applied in this system include:

1. **Secure Data Communication:** The system employs encrypted data transmission between households, CEMS, and the market operator. This ensures that sensitive bidding and energy consumption data are protected from unauthorized access during transmission.
2. **Data Anonymization and Pseudonymization:** User data related to energy consumption and bidding is anonymized at the HEMS level before being transmitted. Pseudonymization is applied to maintain traceability for market clearing without revealing user identities, balancing operational transparency with privacy protection.
3. **Homomorphic Encryption:** This advanced encryption technique allows computations on encrypted data without decrypting it first. By using homomorphic encryption, the market operator can process bids and perform market clearing operations without accessing users' raw data, thereby safeguarding privacy throughout the trading process.
4. **Federated Learning for Demand Forecasting:** Federated learning models are employed to predict community energy demand while keeping raw data decentralized. This approach reduces privacy risks, as only aggregated model updates are shared with the market operator.
5. **Role-Based Access Control (RBAC):** Access to data is restricted based on predefined user roles. For example, only the market operator has access to aggregated bidding information, while individual households retain control over their detailed energy usage data.
6. **Local Data Processing:** By processing data locally at the HEMS level, the system reduces the need to transfer sensitive information to central servers. This decentralization minimizes data exposure risks and enhances user control over personal data.

Lessons Learned and Potential for Replication

1. **Balancing Privacy with Market Efficiency:** The integration of homomorphic encryption and federated learning enables secure data processing without compromising market efficiency. This balance is crucial for ensuring user trust while maintaining operational effectiveness.
2. **Scalability through Modular Design:** The use of CEMS allows the system to scale across multiple residential communities. Each CEMS operates autonomously while interfacing with the central market operator, facilitating expansion without increasing privacy risks.
3. **User-Centric Privacy Controls:** Providing users with intuitive interfaces to manage privacy settings and view data-sharing policies proved essential for fostering trust and participation. Transparent consent management systems further supported user autonomy.
4. **Interoperability and Regulatory Compliance:** The system's design aligns with GDPR requirements by incorporating data minimization principles and ensuring users' rights to data access and deletion. Compliance with ISO 31700-1:2023 standards further enhances interoperability across different energy markets.
5. **Potential for Replication:** The modular architecture and privacy-preserving technologies used in this system are adaptable to various community energy trading scenarios. Future implementations could expand to larger urban networks or integrate additional renewable energy sources, provided that privacy mechanisms are tailored to specific regulatory and user contexts.

This case study demonstrates that privacy-preserving mechanisms are not only feasible but essential for the sustainable operation of residential energy trading systems. The combination of advanced encryption techniques, decentralized data processing, and user-centric privacy controls presents a replicable blueprint for secure, scalable, and user-trusted energy trading platforms.