

Industry Brief

Grid Edge Transactions and GDPR's Right to Erasure

June 2022

Prepared by:

FLUX
tailor

Klaar De Schepper, Flux Tailor



LO3 ENERGY

Chris Foster, LO3 Energy





Table of Contents

Executive Summary	1
1. Introduction	2
1.1. Intended Audience	2
1.2. Organization	3
2. Background Facts	3
2.1. GDPR and Personal Data	3
2.2. Relevant Background Information about LO3 Energy	4
2.3. Data Subjects	4
2.4. Processing Environment	4
2.5. Content and Nature of Data Processing: Right to Erasure	5
2.6. Diagram Illustrating Right To Erasure Scenarios	5
2.7. Treatment of Data in Response to a Right to Erasure Request	6
2.8. De-Identification Standards	7
3. Possible Legal Bases and Arguments Post Erasure Request	8
3.1. Legal Obligations	8
3.2. Legitimate Interest	8
3.3. Legitimate Interest Pros and Cons	9
4. Article 17 Right to Erasure Precedent Examples	10
4.1. Dismissal	10
4.2. No Violation	10
4.3. Sanction	11
4.4. Reprimand	11
5. Conclusion	11
Appendices	1
Appendix A: Selection of Relevant Excerpts from GDPR Text	12
Article 4: Definitions	12
Article 6: Lawfulness of processing	13
Art. 17(3)(a) GDPR Right to erasure ('right to be forgotten')	13
Recital 47: Legitimate Interest	14
Appendix B	15
Appendix C: Privacy and Meter Usage Data: A Review of Academic Work	17
Table 1: Potential Risks and Harms vs. Granularity	17
Table 2: References	19

Executive Summary

More residential energy customers participate in grid optimization as both consumers and prosumers. Building and maintaining software is not core to the business models of either distribution operators or retail energy providers. Thus, energy providers typically leverage services that help them aggregate demand, provide services and facilitate transactions, rather than building their own from scratch. As detailed energy data is involved in these transactions, best practices should be followed by service providers that control, store, and process energy data.

Existing data privacy regulation leaves room for interpretation, which leaves companies lacking clarity on what measures to implement and exposing them to risk. This brief is focused on GDPR but the discussion is also relevant for data privacy regulation in place and under way in other parts of the world. As the Right to Erasure is the top issue for which GDPR cases are brought to Data Protection Authorities,¹ and in many respects is a superset of other data subject rights, it is the lens through which we examine the matters considered.

To accelerate development and unlock full market potential, industry and government collaboration will be needed to resolve open questions through best practice guidance.

The original energy usage data involved in energy transactions are part of the evidence that helps validate billing records of the transactions after the fact. In the case of transactions based on sets of customer data, such as aggregated demand flexibility transactions, data from one end user is used to (re)calculate transaction values for all others in the group. If data would be erased, for example following a data subject request, energy transactions that use that data as input can no longer be re-calculated using the exact methodology underpinning the transaction. As B2B2C providers of energy service software function as data processors calculating transactions as part of the service they provide to their clients, they may be asked to provide records and validated re-calculations of transactions upon requests from their customers.

Key Preliminary Findings From our review of available government, academic, and industry resources:

Question 1: Is energy usage data considered “Personal Data” under GDPR?

Answer: Yes, unless re-identification is not “Reasonably Likely”

Energy usage data is considered “Personal Data” under GDPR, and there is disagreement about the point at which data is sufficiently “irreversibly” de-identified to no longer be considered “Personal Data”

Question 2: Can energy data be retained if de-identified?

Answer: Yes, it may be possible to do so as long as conditions for a legal basis are met. “Performance of a Contract” or “Legitimate Interest” are two potential GDPR legal bases.

Both “Performance of a Contract” and “Legitimate Interest” may be legal bases for processing data post-erasure request, where to use “Legitimate Interest” a “Legitimate Interest Assessment” needs to be on record establishing the Legitimate Interest and describing the considerations taken in a “balancing test”. The Legitimate Interest Assessment will be up for scrutiny if the legal basis for processing post erasure-request is contested.

Key Recommendations:

Standard specifications should be developed for energy data de-identification to accompany energy data exchange standards and data access mandates.

These specifications can be followed by organizations both as part of complying with government regulation and as guidance in places where data privacy regulation doesn't yet exist.

¹ Source: Irish Council for Civil Liberties. 2021. “Europe’s Enforcement Paralysis.” <https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf>.

1. Introduction

In our increasingly connected world data has become the lifeblood of industry - and the energy industry is no exception. Energy meters and connected devices produce, consume, and exchange energy data at staggering volumes. As energy is consumed as part of many activities, and behaviors and devices leave unique footprints that can be derived from detailed energy usage data, energy data can tell us very personal things about someone's life. The level of detail of the information that can be derived depends on the resolution of the data, and whether any methods are in place to affect its usability for re-identification.

To enable the rapid market growth needed to accelerate greenhouse gas emission reduction, consumers need to be able to trust that industry standards are in place to secure their data. Standards exist for data exchange and efforts have been made to standardize general data privacy practices. However, there isn't a standard for data processing methods that takes into account the risk of a data breach, nor the risk of customer-re-identification. This depends on the data architecture, the availability of auxiliary data, and data resolution.

Under data privacy regulation, notably the EU General Data Privacy Regulation (GDPR), data subjects have rights in relation to their personal data. An increasing number of U.S. States and nations have followed the E.U.'s example in drafting or adopting regulation to formalize the rights of data subjects in their respective jurisdictions. One of these rights is the "Right to Erasure;" which is the right of a data subject to request that their personal data is deleted from a data processor's systems. But how exactly "personal data" is defined, and at what point of de-identification and data privacy measure implementation the data either is no longer considered "personal data" or its use and treatment methods are supported by regulation isn't entirely clear. Energy companies and their software vendors must understand how the data so critical to their business should be processed, and where the boundaries of data subject rights lie for their customers.

As a company on the forefront of the intersection of technology and data in the energy sector, LO3 Energy wants to ensure that the rights of customers are respected. LO3 Energy has engaged Flux Tailor as experts to perform research and work towards establishing best practices followed throughout the energy industry and beyond. To not get lost in the complex differences between data privacy regulations, we focus on GDPR as the "Gold Standard" that most stringently enforces regulation to design for as a globally oriented company. While we focus on the "Right to Erasure" the questions we raise about the definition of personal data, and measures needed to de-identify, are more broadly applicable to data privacy considerations. In absence of clear industry standards and established best practices, we contemplate two specific issues of interest to data subjects.

Flux Tailor reviewed GDPR text, erasure request ("Article 17") precedents, and academic literature to consider data privacy regulation implications as it relates to the energy usage data processed by the company. Our goal is to present this topic and background information to invite others to this conversation and jointly work towards solutions. The two core questions with which we started were outlined as follows:

1. **Is 15 minute interval energy consumption data considered "personal data"? Is that answer affected by:**

 - a) Whether or not it is associated with a service address or other Personally Identifiable Information (PII)?
 - b) If it is separately stored from customer-identifiable data through links to pseudonymised data?

2. **If a deletion request is submitted under GDPR Section 3 Article 17 Right to Erasure ("Right to be Forgotten"), what data needs to be deleted, and what data may be retained?**

 - a) Is having de-linked data and deleting the PII customer data and links enough to be able to retain energy consumption data for record keeping purposes to support LO3 Energy's B2C clients in case of a dispute?
 - b) What exactly are the constraints around data retention?
 - c) If raw de-identified and de-linked energy usage data can not be retained, are there any other forms of data retention besides that of raw data allowed that would suffice for dispute resolution purposes, for example aggregation or other processing?

1.1. Intended Audience

This industry brief is intended for use by energy service companies, government officials, data privacy policy experts, advocacy groups, researchers, academics, investors, and others who are interested in establishing best practices for managing personal data such as energy data. It is also designed to provide researchers and academics with a limited overview of GDPR regulation. Although this document presents research from around the world and is written for a world-wide audience, it is narrowly focused on policy and legal issues in the European Union. Neither of the authors have law degrees, and findings of the review of legal text may lack clarity and will certainly lack insights that would be brought by legal experts.

1.2. Organization

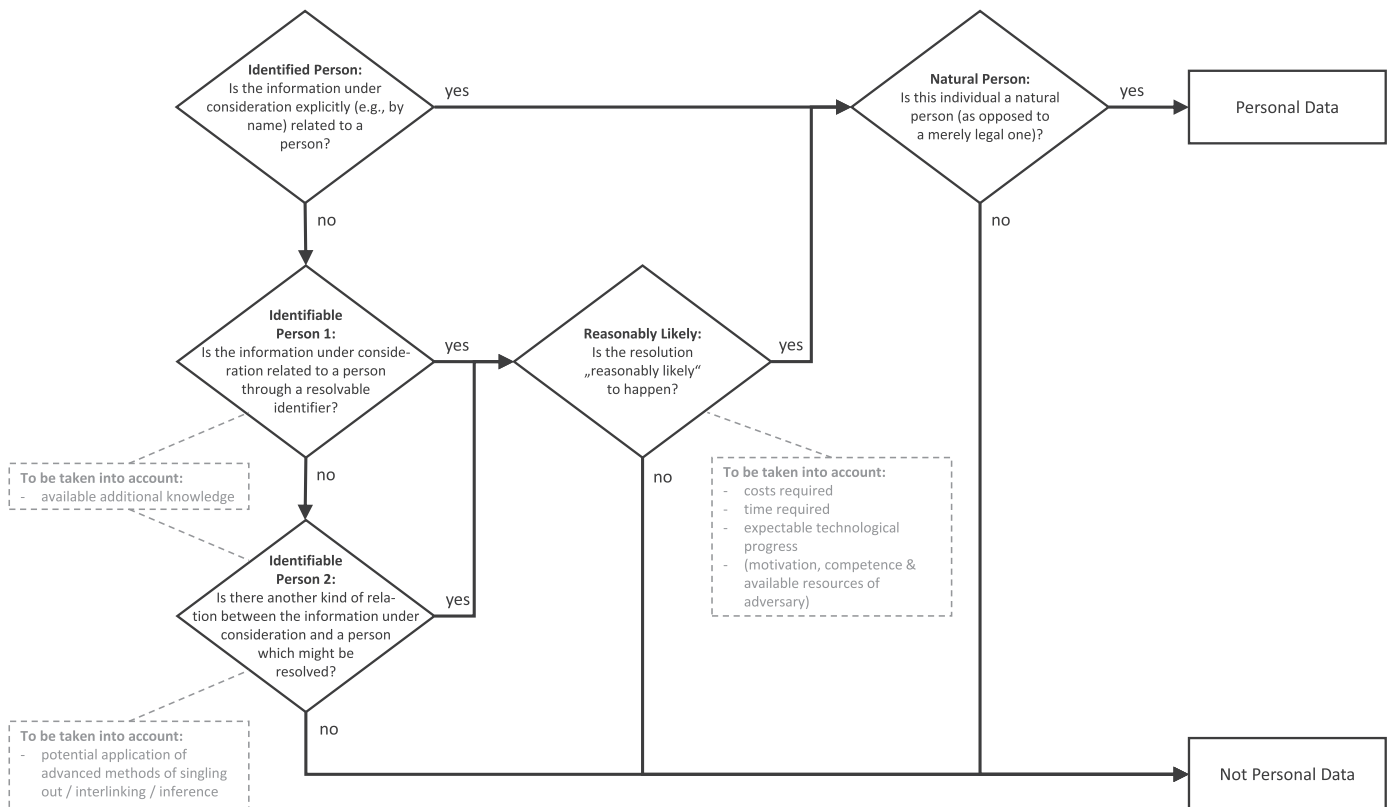
We first introduce background information about GDPR, LO3 Energy, its use of data from energy customers and producers. We then introduce an example scenario under which the erasure of energy usage data can lead to issues. What follows is a review of possible legal bases for data processing post-erasure request, and example precedents for data erasure cases that have been brought to European Data Protection Authorities (DPAs). The brief concludes with recommendations for industry and government collaboration to ensure data subject interests while enabling business activity. Relevant text and further references discussing this text can be found in Appendices A–C.

2. Background Facts

The summary below was derived from information made available to Flux Tailor by LO3 Energy. Publicly available sources of information are referenced in footnotes used throughout this brief and in Appendices A–C. LO3 Energy provided non-public materials as input for the brief through virtual meetings, e-mail, chat conversations, and internally and externally used company materials that serve as a record of processing activities required under GDPR Article 30 such as privacy policies and Data Book materials.

2.1. GDPR and Personal Data

Energy usage data is considered “Personal Data” under GDPR, even if it’s been stored separately from personal data through pseudonymized links: “Thus, it is critical to understand that when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data. Only if the data controller would aggregate the data to a level where the individual events are no longer identifiable, the resulting dataset can be qualified as anonymous.” However, GDPR does not specifically define “anonymization”.² As Finck et al. state in the academic paper from which we show the below diagram: “To the French Commission Nationale de l’Informatique et des Libertés (CNIL), anonymization consists in making ‘identification practically impossible’.”³ Anonymization ‘seeks to be irreversible’ so as to no longer permit the processing of personal data, but based on precedents for erasure cases it seems complete irreversibility is not required. The process by which data is rendered anonymous is left up to the companies handling that data. The below diagram illustrates how it is established whether or not data should be deemed “Personal Data” under GDPR.



Source: Figure 1 Assessment scheme for person-relatedness of data under the GDPR. Finck, Michèle, and Pallas, Frank. 2020. “They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR.” *International Data Privacy Law*, Volume 10, Issue 1, February 2020, Pages 11–36, <https://doi.org/10.1093/idpl/ipz026>

2 Piltz, Carlo. 2019. “Austrian Data Protection Authority: The Erasure of Personal Data Is Also Possible through Anonymization.” <https://medium.com/golden-data/austrian-data-protection-authority-the-erasure-of-personal-data-is-also-possible-through-4e61b882e4ad>.

3 Finck, Michèle, and Pallas, Frank. 2020. “They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR.” *International Data Privacy Law* 10 (1): 11–36. <https://doi.org/10.1093/idpl/ipz026>.

2.2. Relevant Background Information about LO3 Energy

LO3 Energy's platform, Pando, serves as a foundational accounting layer and transactive engine at the grid edge. The platform links DER activity with new financial incentives and compensation models. Energy service providers can efficiently track, allocate, and account for an increasingly complex set of transactions. This detailed accounting creates transparency and flexibility for organizations to provide value to end customers in new ways. Importantly, the new incentives for local resources and support for communities can be offered cost effectively through streamlined, efficient backend processes.

Pando is a software-as-a-service (SaaS) product built using a high-technology software stack capable of scaling to global markets. Leveraging best-in-class cloud infrastructure allows LO3 Energy to deploy Pando in a variety of configurations with logical data boundaries LO3 Energy calls Privacy Zones. Pseudonymised data flows between micro-services over encrypted protocols with authenticated requests. Some activities within the platform result in anonymized transactions being written to a public blockchain technology to serve as an immutable record of outcomes. Data encryption, role-based access, layered networks and firewalls, and monitoring work to ensure private data remains private. User interfaces in the form of browser-based web applications, web APIs, and a brandable mobile application provide the means to interact with the platform.

When a service provider engages LO3 Energy to furnish the Pando platform to their customers (the end customers), the service provider acts as the "controller" and LO3 Energy the "processor" in accordance with duties defined within GDPR. Typically, the controller provides the needed energy data to Pando, either directly from their own internal sources, such as a meter data management system (MDMS), or indirectly through a mechanism the controller provides to the end customer, such as a smart home device. This data is provided through either a file-based data exchange hosted by LO3 Energy or via a web API. LO3 Energy processes the energy data received, applying their proprietary technology to determine market outcomes, and provides those results back to the controller via web application or file exchange, and to the end customer using the Pando mobile application.

LO3 Energy operates as a B2B2C company in the U.S., the EU, Japan, and Australia.

2.3. Data Subjects

- Residential and commercial energy consumers
- Participant users who are both consumers and producers of energy (a.k.a. prosumers); they sell energy from batteries, solar panels, or other distributed energy resources.

2.4. Processing Environment

LO3 Energy utilizes a micro-service architecture to segment the data within the Pando platform. Each purpose-built subsystem has access to only the data within the scope of its function. Within the overall system are services whose sole responsibility is to store and retrieve a particular type of data, and other services rely on those services to complete a business process objective. Services interact with each other over encrypted and authenticated network connections, using a set of pseudonymous internal identifiers to correlate data across services. Practically this means that differing types of data (energy data, user PII, marketplace transactions, etc.) are isolated from each other, and knowledge of how the varied internal identifiers on the data is required to connect a user to energy data to marketplace transactions.

2.5. Content and Nature of Data Processing: Right to Erasure

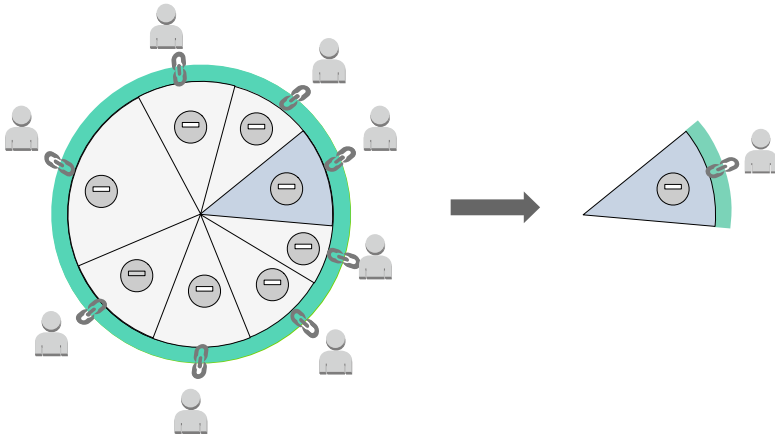
The below table lists the data processed by LO3 Energy, their processing purposes, and the manner in which data is treated upon an erasure request.

Process	Description	Purpose	Processing Erasure Request Treatment
Energy Data	Energy data could originate from LO3 Energy provided hardware, API services provided by third parties for use with their device, or a meter data management system (MDMS) provided by a utility or retailer.	Platform relies on the regular intake of energy data in order to determine what transactions need to be recorded.	Not erased: Connected to financial transaction.
User Onboarding	Being a B2B2C product, users do not register directly with LO3 Energy and cannot join themselves to a marketplace. Rather, LO3 Energy relies on a client (utility, retailer, etc.) to provide a list of user accounts to register.	Users need to be registered in identity service to login.	Data is deleted or automatically expunged; e-mail address is deleted; no location data is stored.
Marketplace Settlement	Convert energy data to orders, and fulfill market orders based on configured algorithm	To execute the orders on the marketplace.	Not erased: Connected to financial transaction; blockchain transactions, where used, consist of a verification hash of data which is deemed by LO3 Energy to not be personal data; blockchain transactions cannot be deleted
App Market Preferences	Once login is complete, user will be able to set marketplace bids and daily budget, as well as manage their energy preferences and participation. If the user is a prosumer, they will also be able to see their marketplace earnings. Other marketplace information, such as aggregated marketplace performance or informative data, are not personal data and are therefore excluded here.	To provide users access to their marketplace data and settings	Data is deleted
Report Generation	Extracting marketplace data from systems, and compiling that data into a report.	Reports are used to resolve billing and inform customers of activity.	Transaction reports for financial settlement are not subject to erasure requests; other reports are expunged after a period.

2.6. Diagram Illustrating Right To Erasure Scenarios

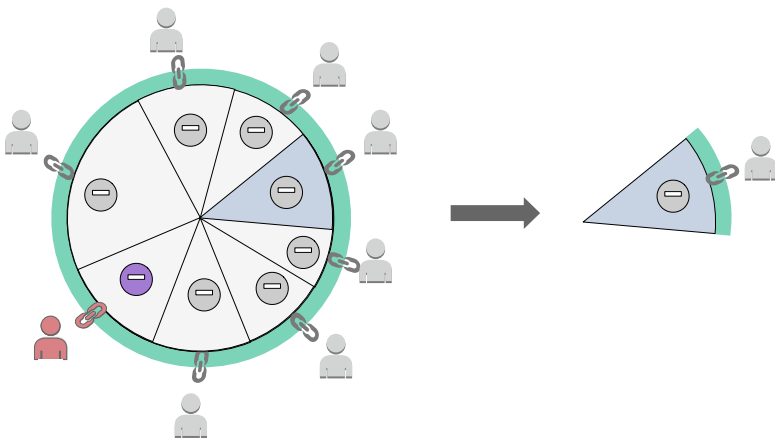
The diagram below illustrates an example remuneration calculation for a demand flexibility event transaction for a group of participants. It illustrates the following scenarios:

A: Baseline Scenario: Meter Usage Data Linked via Pseudonymous Identifier



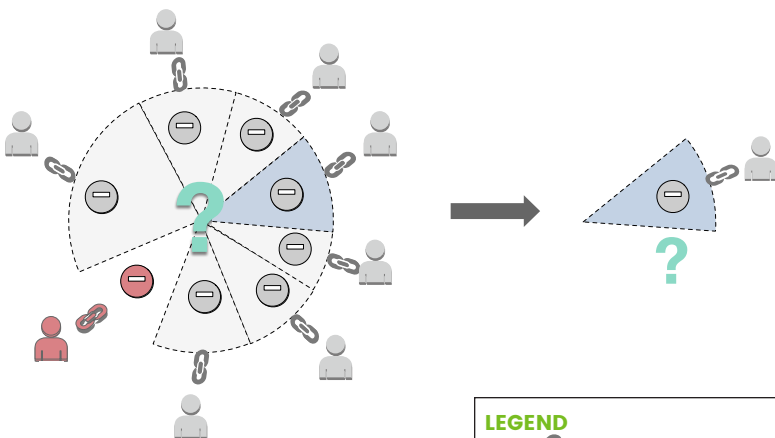
Event remuneration value for a single customer is calculated based on an aggregate of usage from participants in an event. Customer PII is stored separately from meter usage data. Meters are referenced using a unique ID that can not be directly resolved to the natural person, physical meter, or the location of the meter. The total remuneration for a group of users participating in the event is calculated based on the combined (“aggregated”) meter usage data and market values. The remuneration for a given participant is calculated based on the proportion for the participant per the values reported by the participant’s energy meter.

B: Current Post-Erasure Scenario: PII Deleted, Meter Usage Data Maintained

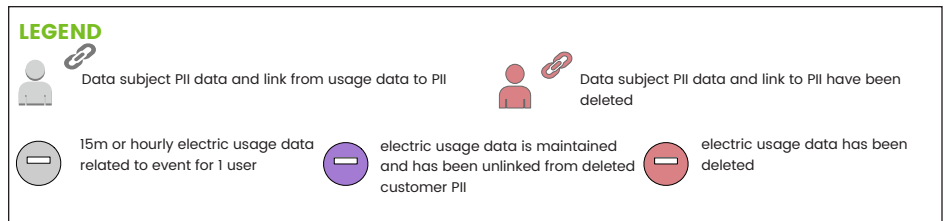


The currently proposed deletion scenario would allow LO3 Energy to still calculate remuneration if an erasure request has been submitted. Customer PII such as e-mail address are removed, and the link from meter data to PII is deleted, but the meter usage data is not deleted. Total remuneration for a group of users participating in the event can still be calculated as all meter usage data is present. Remuneration for a given user can still be (re) calculated as all meter usage data is present and the proportion for each user can be calculated.

C: Meter Usage Data Post-Erasure Scenario: Both PII And Meter Usage Data are Deleted



If meter usage data would be deleted, it would no longer be possible to recalculate the remuneration for a given user in the exact same manner as was done originally, as part of the original source data is missing. Customer PII, energy usage data, and the link from meter data to PII are deleted. Total remuneration for a group of users participating in the event can not be recalculated as underlying data is missing. Remuneration for a given user can no longer be (re)calculated as the deleted meter usage data is missing and proportions can not be calculated.



2.7. Treatment of Data in Response to a Right to Erasure Request

LO3 Energy has designed their solution to support erasure requests. When the erasure flow is complete, the energy data necessary for remuneration are intact, but are only referenced by a LO3 Energy generated internal meter identifier, not the actual meter identifier. The erasure process removes data identifying the user and also the tie between the user and the meter. Where data is written to a blockchain, only anonymous hashes⁴ of the original data is recorded on-chain, which is not erasable. The LO3 Energy data retention policy, privacy policy, and contracts indicate the personal data involved, and what of that data can or cannot be erased.

The following personal data will be erased:

Data
User Account (email address, permissions granted within the system)
Device Configuration (information about the source device for energy information)
Mobile App Preferences
System-generated Emails or Push Notifications
User Identifiable Analytics

The following data will automatically expunge after a set period of time:

Data	Expunge Period
Account Registration	14 days
Application Logs	90 days
Platform Logs	90 days
Database Backups (systems with erased data)	30 days

Some of the personal data is not erased as continued retention and/or processing is necessary:

Data	Reason to Retain
Energy Readings	Connected to financial transaction
Energy Marketplace Transactions	Connected to financial transaction
Billing Reports	Records of billing output sent to Controller
Blockchain Transactions	<ul style="list-style-type: none"> Cannot be deleted Data is verification hash Connection of blockchain record to user record has been deleted

Also retained are records related to the data erasure request, including any submitted identity verification information and a copy of the erasure notification letter.

4

For more information on hashes see the NIST glossary available at: <https://src.nist.gov/glossary/term/hash>

2.8. De-Identification Standards

In the U.S., guidance on de-identification of health information exchanged between medical practitioners and insurers serves as a precedent for rulemaking on standards for de-identification at the federal level.⁵ Researchers have shown that the “safe harbor” option under those rules still leaves room for re-identification — demonstrating the importance of continuous re-evaluation of such guidance.⁶ For energy data, there is a body of work on the level at which energy data needs to be aggregated to be both useful and ensure data privacy, informing rulemaking around aggregated whole building data.⁷ This work is relevant here not just for the data utility vs. privacy considerations and statistical methods discussed, but also because of the fact that final rules for aggregated whole building data differ between U.S. territories. Figuring out rules for all 50 states plus territories results in a lot of redundant work for service providers producing and receiving aggregated whole building data. What is needed is guidance at a national or — even better — international level.

3. Possible Legal Bases and Arguments Post Erasure Request

Under GDPR, there are legal bases other than data subject consent that can be used as legal basis for data processing. Once a data subject has submitted a request to delete their data under the Right to Erase, these other legal bases can be used under certain circumstances. From our review of GDPR itself and other research inputs, the following could be possible legal bases that LO3 Energy could use.

3.1. Legal Obligations

Performance of a Contract: It may not be possible to use this as the data subject requesting the erasure has rescinded the contract.

Manage litigation: LO3 Energy wants to retain energy usage data in order to respond to inquiries on the validity of a marketplace result. LO3 Energy would need to be able to analyze energy data at all of its points of processing in case something went wrong as data made it through the platform. Prior inquiries have proved that depth of data valuable for satisfactorily resolving those matters. LO3 Energy strives for accuracy and integrity improvements throughout the product, yet still there remains a desire to retain the data to ensure veracity. The input data needs for auditing in case of litigation include the original energy data, processed energy data, marketplace orders, and settlement records.

3.2. Legitimate Interest

There is a “Legitimate Interest” in keeping the data, and a “Legitimate Interest Assessment” has been conducted to establish and document this legitimate interest. A documented Legitimate Interest Assessment (LIA) is a GDPR requirement whenever you rely on legitimate interest as a legal basis for processing activities. GDPR article 6(1)(f) states:

“Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

Working Party 29, the precursor of the European Data Protection Board (EDPB) issued an “Opinion 12/2011 on smart metering,” states “Including practical measures such as Privacy Enhancing Technologies and Privacy Impact Assessments to enhance the security and privacy of the data processed by smart meters will make it more likely that this condition for processing could be available to a data controller.”⁸

Based on direct knowledge from LO3 Energy, and the publicly available material reviewed by Flux Tailor, potential answers to the prompts testing conditions for data processing of data that is maintained post Right to Erasure requests based on “legitimate interest” are as follows:

3.2.1. What is the purpose?

In a complete erasure scenario, LO3 Energy would not be able to re-calculate remuneration for a past event in the case another user that participated in the same marketplace settlement event contests the amount remunerated. The purpose of retaining just the de-identified, unlinked energy usage data after an erasure request is to perform data processor services with the highest possible level of certainty that all data necessary to verify transactions is available, and client data processors have similar assurance that they will be able to verify documentation in case of audits requested by their end user customers.

5 The Office for Civil Rights (OCR), and Bradley Malin. 2012. “Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.” Health Information Privacy, 1–32. <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>.

6 Sweeney, Latanya, Ji Su Yoo, Laura Perovich, Katherine E Boronow, Phil Brown, and Julia Green Brody. 2017. “Re-Identification Risks in HIPAA Safe Harbor Data: A Study of Data from One Environmental Health Study HHS Public Access.” Technol Sci. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6344041>

7 Ruddell, Benjamin L, Dan Cheng, Eric Daniel Fournier, and Stephanie Pincett. 2020. Guidance on the Usability-Privacy Tradeoff for Utility Customer Data Aggregation. <https://www.sciencedirect.com/science/article/pii/S0957178720301004>.

8 Article 29 Data Protection Working Party Opinion 12/2011 on smart metering Adopted on 4 April 2011. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wpi183_en.pdf

3.2.2. Is the processing necessary? Are there alternatives?

- As the data controller for whom LO3 Energy is performing data processing may ask for complete documentation of the calculation, the company wishes to maintain all “raw” usage data, including that of users whose other personal data has been deleted.
- The means by which energy data is delivered to LO3 Energy may not provide another source of the data in the necessary quantity or form. There may not be a copy of the data anywhere else, or it may not be accessible to LO3 Energy. For example, a home energy smart device configured to send data directly to LO3 Energy may not have sufficient local storage to maintain data covering the entire remuneration period.
- There are some alternatives to using raw meter usage data. References to a variety of privacy-preserving techniques are listed in Appendix B: Index of Curated Research References.

3.2.3. Balancing Test

Demonstrate that the rights and freedoms of the data subject do not override your (the Controller’s) Legitimate Interest. Summary of arguments:

- **Risks:** An internal or external intruder can break through LO3 Energy’s protections, can access meter usage data, and has auxiliary data that can help re-identify a data subject from a set of de-identified data.
- **Harms:** The historical data obtained is used for consumer profiling, profile based discrimination, burglary, stalking, kidnapping, targeted advertising, or other data subject harms resulting from re-identification.
- **Usage:**
 - Data collected is never sold or licensed to any third party for any reason. Data may only be used by LO3 Energy for the express purpose for participation, and for LO3 Energy internal analysis for purposes of improving the capabilities of the product LO3 Energy provides.
 - LO3 Energy’s product may be utilized in programs designed to fulfill energy equity and/or decarbonization goals established by private enterprises which engage LO3 Energy’s services, or by governmental regulation.
- **Mitigating Measures Taken:**
 - No customer location data is stored in the system.
 - Meter data is de-identified and links from de-identified meter data to customer PII are removed.
 - Systems containing meter data are blocked by access from both internal and external intruders using a variety of protections, including, but not limited to: at-rest and in-transit encryption, encrypted interfaces with authentication, role-based access controls, firewalls, network isolation, intrusion detection, and security monitoring
 - The maximum resolution of the energy usage data retained is 15 minutes which limits re-identification risk.
 - Geographically distinct operating regions with logical data boundaries.
 - Data is stored co-mingled with generated data to obscure personal data in the data set.
 - LO3 Energy has implemented measures to ensure data privacy including:
 - An established data lifecycle to govern the retention age of data collected and produced
 - Mandatory annual and on-going security training for all employees and contractors, which includes a specialized module for GDPR
 - A designated Data Protection Officer

3.2.4. Legitimate Interest Pros and Cons

Advantages:

- Legitimate interest is flexible and can be used as long as a Legitimate Interests Assessment (LIA) is in place prior to data processing.
- Companies perform LIAs as a service, and although a true standard for how to conduct them or who should conduct them doesn’t exist, templates on how to conduct them do exist.

Disadvantages:

- Requires documentation and introduces some level of risk as the assessment could be contested. “If they disagree with your justification for legitimate interest, the burden is on you to prove otherwise. Given the risks associated with collecting data unlawfully under the GDPR – including the potential for a large fine – it’s risky to put your documentation up for scrutiny in this way.”⁹

⁹ Luke Irwin (2020) “The GDPR: Legitimate interest – what is it and when does it apply? -”, IT Governance. Available at: <https://www.itgovernance.eu/blog/en/the-gdpr-legitimate-interest-what-is-it-and-when-does-it-apply>.

4. Article 17 Right to Erasure Precedent Examples

The below example precedents were found in a variety of online sources, and confirmed by searching the European Data Protection Board's (EDPB) website by keyword "Article 17", and filtering results by "Decisions". No existing instances of erasure request use cases were found pertaining to organizations in the energy industry. The examples below were chosen to illustrate the types of considerations made by Data Protection Authorities (DPA's) in different countries, and to display the variety of opinions. This is not an exhaustive list of relevant precedents.

4.1. Dismissal

2020-06-02 Slovenia: summary: Slovenian Administrative Court upholds the decision of the Slovenian SA: the right of erasure does not enable an individual to have his personal data erased from Baptismal Register. Decision: Dismissal of the complaint because the register is an archive document necessary for archiving purposes in the public interest and the deletion of the data would hamper the objective. Note that although GDPR applies to Slovenia as an EU member state, the country is just now working on an implementation law.

4.2. No Violation

2018-12-05 Austria

4.2.1. From summary by Austrian Lawyer Nino Tlapak at the firm Dorda:¹⁰

- 4.2.1.1 "The key finding of the decision is that anonymisation instead of full deletion is permitted, because neither processing nor any other further use are possible as there is no personal reference left"
- 4.2.1.2 "The DSB held that even if future technologies could make reconstruction possible, a complete irreversibility is not necessary"
- 4.2.1.3 "The most important impact in practice is that data controllers may (i) amend its data retention and erasure concepts, (ii) implement consistent anonymisation tools and processes as well as (iii) develop anonymised statistic models instead of having to fully delete prospects' or customers' data"

4.2.2. Relevant quotes from translation from German of the DPA's findings:¹¹

- 4.2.2.1 "The respondent then initiated further steps and – depending on the system – either deleted the data that could be clearly assigned to the complainant immediately or "anonymized it in accordance with the GDPR". A traceability to his person is therefore irrevocably excluded. This procedure is also clearly permissible within the meaning of Art. 17 GDPR and equates to deletion."
- 4.2.2.2 "By implementing all of these described steps, the original customer connection was effectively anonymized by overwriting it with a "dummy customer connection". There would now be no personal data and therefore no identifying features that could be associated with the customer's original online request. Rather, there would only be an empty customer connection to Max Mustermann and therefore no further information would be available that would point to the complainant. From a legal point of view, the anonymization of personal data carried out in this way corresponds to permanent deletion, as the data would no longer be personal and would therefore be outside the scope of the GDPR."
- 4.2.2.3 "All master data would be taken over from the sample customer, which means that it is no longer possible to successfully search for the person concerned in the systems." *In addition, there are no referenced objects that contain data that would enable identification.*" highlighting key sentence that may make this precedent not apply: here there are referenced objects that could enable identification in the case the attacker has knowledge of a user's usage patterns."

4.3. Sanction

2021-04-20 Denmark (EDPBI:DK:OSS:D:2021:210): "The Danish Data Protection Agency considers that it is not necessary for the complainant to have access to his customer account for at least two years after the purchase, in order for him to exercise his right of complaint under the Purchase Act. It is therefore not necessary for Coolshop to comply with a legal obligation that the customer account should not be deleted until at least two years after the complainant's last purchase. On this basis, the Danish Data Protection Agency considers that Coolshop cannot refuse to delete the complainant's customer account on the basis of Article 17(3)(b) of the Data Protection Regulation."

¹⁰ Austria: anonymisation accepted as valid data deletion method - Lexology (no date). Available at: <https://www.lexology.com/library/detail.aspx?g=b7d087a4-acc3-4cfc-af89-0b51417e9ed8>
¹¹ Austrian DPA: (auto translated) DSB-DI23.270 / 0009-DSB / 2018'. Abbreviated URL: <https://bit.ly/3H0DAaT>

4.4. Reprimand

2021-03-24 Sweden:

"The complainant has requested deletion of his credit or debit card information. However, Spotify does not process card data when a user pays via PayPal, such as the complainant, but instead treats unique identifiers for the payment cards or "instruments" ("unique payment instrument identifiers") used by a customer when registering free trial periods. The legal basis for the processing is legitimate interests. That the complainant has written that he withdraws his consent may be interpreted as an objection to the processing. The continued processing is not subject to the right to erasure because Spotify has a strong, legitimate interest in continuing the processing that outweighs the rights and freedoms of the complainant. Among other things, the company has stated that the company's legitimate interest with the processing is to counteract fraud regarding free trial periods.

Recital 47 of the GDPR states that processing of personal data that is absolutely necessary to prevent fraud constitutes a legitimate interest in the controller concerned. IMY therefore considers that the company has a legitimate interest. Furthermore, IMY believes that processing is absolutely necessary for purposes relating to legitimate interest. The investigation shows that the data has been minimised insofar as it is possible for the company to achieve the purpose of the legitimate interest. In the weighing of interests to be made between the Company's legitimate interest and the interests, rights and freedoms of the complainant, IMY notes that the company's legitimate interest weighs heavily. The processing appears as something that the complainant can reasonably expect when registering a free trial and not particularly privacy invasive. The personal data in question can neither be considered as sensitive from a privacy perspective.

In a summarized assessment, IMY finds that the company has demonstrated compelling legitimate grounds that outweigh the complainant's interest in the reuse of his card information to register new free trial periods on the company's services and that his personal data shall not be processed. In light of the reasons the company has presented, IMY finds that the company has demonstrated compelling legitimate grounds that outweigh the complainant's interests, freedoms and rights. The Company has thus had the right to continue processing the data after the complaint has objected to the processing and the complaint has therefore not been entitled to erasure under Article 17(1)(c) GDPR." However: Spotify did not notify the complainant sufficiently, so "Against this background, IMY finds that the company's response of 8 June 2018 has not been sufficiently justified pursuant to Article 12(4) because the company has not clearly stated what personal data is being processed, that the data is processed on the basis of a legitimate interest and what the legitimate interest is and that the answer has not contained information about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. Spotify has thus processed personal data in violation of Article 12(4) GDPR."

5. Conclusion

Energy service companies and their investors want assurance that their practices comply with data privacy regulation. Specific guidance on de-identifying energy data is one example of what is needed for organizations to safely store and exchange information. GDPR language leaves too much room for interpretation and exposes energy service companies to too much risk. These questions are relevant for aggregators in Europe, but also in the U.S., where a growing number of states already have data privacy regulation with a right to erasure, and with federal regulation is now in the works. Those working on rules for FERC 2222 should be contributing to the guidelines we propose. A key factor in the success of that endeavor will be availability of data, but the privacy implications of the exchange of the data must be considered.

Industry specific guidance should be created, as the harms and risks of re-identification and the measures to prevent it depend on the type of data at hand. As safe-harbor rules that are fixed in legislation may be out of date by the time they are enacted, we propose an international industry-led standard managed by a body of experts that evaluates and updates guidance on risk and privacy-preserving methods continuously.

LO3 Energy and Flux Tailor invite feedback on the information and questions presented in this brief. Those interested can reach out to us at dataprivacy@fluxtailor.com and privacy@lo3energy.com or follow us on social media at [@fluxtailor](https://twitter.com/fluxtailor) and [@LO3Energy](https://twitter.com/LO3Energy).

Appendix A: Selection of Relevant Excerpts from GDPR Text

This appendix contains a (non-exhaustive) review of relevant excerpts from GDPR text. This is not an exhaustive list of applicable GDPR sections.

Excerpts from: European Parliament (2016) GDPR: REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ E. Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>

Available in other formats at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Article 4: Definitions

For the purposes of this Regulation:

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

[...]

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

[...]

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

[...]

(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

[...]

(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

[...]

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

[...]

(23) 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Article 6: Lawfulness of processing

1. "Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Art. 17(3)(a) GDPR Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
 - (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
 - (d) the personal data have been unlawfully processed;
 - (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which

the controller is subject;

- (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- (e) for the establishment, exercise or defence of legal claims.

Recital 47: Legitimate Interest

Whereas:

“(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.”

Appendix B: Index of Curated Research References

EU Documents

Year	Contributors/Authors	Title	URL
2019	ENISA	Pseudonymisation techniques and best practices	View »
	European Parliament	Directive 2019/944 on Common Rules for the Internal Market for Electricity	View »
	European Parliamentary Research Service Scientific Foresight Unit (STOA)	Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?	View »
	Technology Policy Unit for the Europea Data Protection Supervisor	EU Tech Dispatch: Smart Meters in Smart Homes	View »
	The European Data Protection Board	Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects	
2016	European Parliament	GDPR: REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ E	View »
2014	ARTICLE 29 DATA PROTECTION WORKING PARTY	Opinion 05/2014 on Anonymisation Techniques	View »
		Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC	View »
2011	ARTICLE 29 DATA PROTECTION WORKING PARTY	Opinion 12/2011 on smart metering Adopted on 4 April 2011 THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA	View »

Legal-Academic

Year	Contributors/Authors	Title	URL
2020	Finck, Michèle	They who must not be identified-distinguishing personal from non-personal data under the GDPR	View »
2019	Rifaut, Andre	Guidance on Anonymisation and Pseudonymisation	View »
2018	Politou, Eugenia	Backups and the right to be forgotten in the GDPR: An uneasy relationship	View »
		Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions	

Legal-Online

Year	Contributors/Authors	Title	URL
2021	GDPRHub	GDPR Hub: Article 6 GDPR	View »
	Raul, Alan Charles	The Privacy, Data Protection and Cybersecurity Law Review: EU Overview	View »
2020	Luke Irwin	The GDPR: Legitimate interest – what is it and when does it apply? -	View »
2019	Prinsley, Mark A	Using Performance of a Contract as a Legal Basis for Processing in the context of Online Services	
2019	Tlapak, Nino	Austria: anonymisation accepted as valid data deletion method - Lexology	View »

Precedents

Year	Contributors/Authors	Title	URL
2020	The European Data Protection Board	Summary Final Decision Art 60	
2019	Piltz, Carlo	Austrian Data Protection Authority : the erasure of personal data is also possible through anonymization	View »
2019	Riepan, Iris	Data Protection Authority On Erasure By Way Of Anonymization	
2018	Austrian Data Protection Authority	Austrian DPA: (auto translated) DSB-DI23.270 / 0009-DSB / 2018	View »
2014	Orduña Francisco Javier	Roj : STS 2484 / 2014 - ECLI : ES : TS : 2014 : 2484	

Smart Meter Data Privacy - Academic

Year	Contributors/Authors	Title	URL
2021	Lee, Dasom	Data privacy and residential smart meters: Comparative analysis and harmonization potential	View »
2021	Rahimian, Shadi	Differential Privacy Defenses and Sampling Attacks for Membership Inference; Differential Privacy Defenses and Sampling Attacks for Membership Inference	View »
2021	Yilmaz, Ibrahim	Avoiding Occupancy Detection From Smart Meter Using Adversarial Machine Learning	View »
2020	Kement, Cihan Emre	Load Shaping Based Privacy Protection in Smart Grids: An Overview	View »
2020	Martinez, Jabier	Smart Grid Challenges Through the Lens of the European General Data Protection Regulation	View »
2019	Liu, Kin Sum	Performing Co-Membership Attacks Against Deep Generative Models	View »
2018	Cleemput, S	Secure and privacy-friendly smart electricity metering	View »
2018	Eibl, Günther	Unsupervised Holiday Detection from Low-resolution Smart Metering Data	View »
2017	Asghar, Muhammad Rizwan	Smart Meter Data Privacy: A Survey	View »
2017	Buescher, Niklas	Two Is Not Enough: Privacy Assessment of Aggregation Schemes in Smart Metering	View »
2017	Chen, Dong	Weatherman: Exposing weather-based privacy threats in big energy data	View »
2016	Afrin, Sabrina	An anonymized authentication framework for smart metering data privacy	View »
2016	De, Sourya Joyee	Privacy Harm Analysis: A Case Study on Smart Grids	View »
2016	Lipton, Benjamin	Formalizing anonymity-delay tradeoffs in smart grid networks	View »
2014	Engel Fachhochschule Salzburg, Dominik	Influence of Data Granularity on Smart Meter Privacy	View »
2014	Finster, Soren	SMART-ER: Peer-based privacy for smart metering	View »
2013	Buchmann, Erik	Re-identification of Smart Meter data	View »
2012	Greveler, Ulrich	Multimedia content identification through smart meter power usage profiles	View »
2010	Molina-Markham, Andrés	Private memoirs of a smart meter	View »
1989	Hart, George W	Residential Energy Monitoring and Computerized Surveillance via Utility Power Flows	View »

Data Privacy White Papers

Year	Contributors/Authors	Title	URL
2021	Irish Council for Civil Liberties	Europe's enforcement paralysis	View »
2021	Kurth, Huntan Andrews	How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation	View »
2018	Hurdik, Jan	The Right to be Forgotten in the GDPR	View »
2016	Belfast London New York Palo Alto San Francisco, Dublin	The GDPR: A Guide for Businesses	View »

6. Appendix C: Privacy and Meter Usage Data: A Review of Academic Work

This appendix contains a (non-exhaustive) review of relevant findings from Scholarly Work on Information Revealed by Meter Usage Data.

Table 1: Potential Risks and Harms vs. Granularity

Harms	Information revealed by smart meters	Pattern	Sub Second	Second	Minute	5 Minutes	15 Minutes	Hourly	Daily	Monthly	Ref. #
Burglary	Have you been away from home for some time?	High/ low power usage during the day									1
Burglary, stalking	Are you living alone at home right now?	Single person power usage or simultaneous power usage at distinct areas of the house during the day									1
Burglary, profile based discrimination	When are you usually away from home?	High/ low power usage during the day									1
Consumer profiling	Did you watch the game last night?	Appliance activity matching the game showtime									1
Profile based discrimination	Do you stay at home all day watching TV or in front of the computer?	Appliance activity matching signature of TV, computer									1
Profile based discrimination, targeted advertising	Do you cook often or prefer to eat outside?	High/ low power events around meal times for microwave, cook tops etc.									1
2016	Belfast London New York Palo Alto San Francisco, Dublin	The GDPR: A Guide for Businesses									1
Burglary, stalking, profile based discrimination	"re-identification is possible just by using simple statistics and intuitively selecting adequate consumption features."	Overall consumption;Minimum consumption;Maximum consumption;Standard deviation, Consumption during time interval;Weekend consumption;Wake up hour;Bedtime 0.9-quantile Frequency of mode									2
Burglary, stalking, profile based discrimination	Location by way of blackout event time	Blackout events									3
Burglary, stalking, profile based discrimination	Location by way of weather data	Temperature Changes									4

Table 1: Potential Risks and Harms vs. Granularity (Cont)

Harms	Information revealed by smart meters	Pattern	Sub Second	Second	Minute	5 Minutes	15 Minutes	Hourly	Daily	Monthly	Ref. #
Burglary, stalking, profile based discrimination	Membership Inference	identify single household from aggregate									5
Burglary	Infer holiday periods of residents	Shift in the time of day of usage									6
Profile based discrimination	Infer religious practices	timeshift in daily routines during Ramadan									7
Profile based discrimination, targeted advertising	Detect the use of household appliances such as refrigerators or lighting	Appliance signature									8
Kidnapping, stalking, child abuse	Do you leave a child alone at home? How often and how long?	Single person power usage or simultaneous power usage at distinct areas of the house during the day									9
Burglary, kidnapping, stalking, profile based discrimination	Is your home protected by an electronic alarm system?	Appliance activity matching alarm system									9
Profile based discrimination, Burglary	Do you own a lot of expensive gadgets?	Appliance activity matching signature of expensive gadgets									9
Profile based discrimination, targeted advertising	Bathroom and housework activities										8
Profile based discrimination, targeted advertising	Multimedia content Identification	Detected from known multimedia content									10

Table 2: References

Reference Nr.	Source Citation	URL
1	De, S. J. and Metayer, D. Le (2016) 'Privacy Harm Analysis: A Case Study on Smart Grids', in 2016 IEEE Security and Privacy Workshops (SPW). IEEE, pp. 58–65. doi: 10.1109/SPW.2016.21.	View »
2	Buchmann, E. et al. (2013) 'Re-identification of Smart Meter data', Personal and Ubiquitous Computing, 17(4), pp. 653–662. doi: 10.1007/s00779-012-0513-6.	View »
3	Asghar, M. R. et al. (2017) 'Smart Meter Data Privacy: A Survey', IEEE. Available at: http://www.ceer.eu/portal/page/portal/EER	View »
4	Chen, Dong, and David Irwin. 2017. "Weatherman: Exposing Weather-Based Privacy Threats in Big Energy Data." In 2017 IEEE International Conference on Big Data (Big Data), 1079–86. IEEE. https://doi.org/10.1109/BigData.2017.8258032 .	View »
5	Buescher, N. et al. 'Two Is Not Enough: Privacy Assessment of Aggregation Schemes in Smart Metering', Proceedings on Privacy Enhancing Technologies, 2017(4), pp. 118–134. doi: 10.1515/popets-2017-0030.	View »
6	Eibl, G., Burkhart, S. and Engel, D. (2018) 'Unsupervised Holiday Detection from Low-resolution Smart Metering Data'. doi: 10.5220/0006719704770486.	View »
7	Cleemput, S. (2018) 'Secure and privacy-friendly smart electricity metering', (May). Available at: https://lirias.kuleuven.be/1652298?limo=0%0Ahttps://lirias.kuleuven.be/retrieve/509996 .	View »
8	Engel, D. (2014) 'Influence of Data Granularity on Smart Meter Privacy', (September), pp. 26–27. doi: 10.1109/TSG.2014.2376613.	View »
9	De, S. J. and Metayer, D. Le (2016) 'Privacy Harm Analysis: A Case Study on Smart Grids', in 2016 IEEE Security and Privacy Workshops (SPW). IEEE, pp. 58–65. doi: 10.1109/SPW.2016.21.	View »
10	Greveler, U., Justus, B. and Loehr, D. (2012) 'Multimedia content identification through smart meter power usage profiles', Computers, Privacy and Data Protection, (January), p. 2010.	View »

About LO3 Energy

Founded in 2015, LO3 Energy is a Portland, Oregon-based cleantech company that provides software to enable companies and communities to drive renewable energy use with advanced financial models and tools. The company is committed to working with energy consumers and asset owners to drive adoption of clean energy. LO3 Energy's mission is to accelerate the decarbonization of electric grids worldwide with a software platform that enables partners to implement innovative compensation mechanisms that best support their customers, grid resources, and the networks they operate. The company is best known for its Pando suite of software, which provides utilities, suppliers and asset owners with tools to integrate and leverage new compensation models to support customers making use of renewable assets.

LO3 Energy operates in the U.S., the EU, Japan, and Australia. It operates as a B2B2C company and facilitates participation in local renewable energy and demand flexibility programs for energy service providers. Their energy service provider customers use behind-the-meter distributed resources (DERs) and flexible loads from energy "prosumer" and consumer end users to provide excess generation back to the grid, store it for peak usage, and optimize their consumption. Energy providers are increasingly offering dynamic new customer incentives and programs more frequently while striving to manage cost shifts for ratepayers and maintain a reliable network.

lo3energy.com  

FLUX tailor

About Flux Tailor

Flux Tailor specializes in data-driven customer engagement solutions that support the clean energy transition. We have been working as domain experts with utilities, software developers, and governments on a consulting basis and also develop our own SaaS offerings. Our mission is to bring energy solutions to as many people as possible and help build the clean energy transition workforce. As technical experts, we have provided model design, requirements specification, and quality assurance support for a variety of interactive web-based tools to calculate and estimate cost, savings payback, GHG emission, and grid reliability impact of individual energy users or portfolios of energy users deploying clean energy resources.

To support software development and data management practice, Flux Tailor generates technical documentation that is easy to understand for both software developers and non-technical audiences, and specializes in illustrative and technical diagrams and impactful data visualizations. Flux Tailor is focused on embedding the Voice of the Customer in the design of clean energy solutions. This is implemented through our extensive work with DER solution providers, utilities, regulators, community-based organizations, and consumers.

Since Flux Tailor started in 2016, the company has contributed as utility data domain expert to consulting projects with five major U.S. utility companies, big tech companies, several international governmental organizations, Mission:data (a leading industry coalition promoting consent-based energy data access), and a group of prominent clean tech startups such as Amperon and Zappyride. As part of our data exchange standards work we are currently working with the Green Button Alliance under a NIST grant to update ESPI Req 2.1 ("Green Button") standard to include more comprehensive utility bill information including bill images. We provide customized packages of market intelligence research on data access and data privacy regulation to assist energy companies as they optimize their data processing activities and prioritize the markets they target.

fluxtailor.com  

