



# Building trust with off-grid solar consumers through better data practices



Consumer Protection Briefing Note: Personal Data Privacy



# Executive Summary

**Internet of Things (IoT) technology and digitalisation are driving innovation across the off-grid solar (OGS) sector<sup>1</sup>. In parallel, there has been growing attention on data-management matters from regulators and industry alike in recent years, given the global shift to data-driven economies and the increased reliance on personal data to fuel business growth. The ability to leverage data has supported the expansion of the OGS industry and provided new opportunities for consumers, yet it also exposes them to a wide range of vulnerabilities that need to be carefully managed. Ensuring data privacy is a challenge that is compounded by the number and nature of partners that OGS companies may work with, and the decentralized nature of their workforce through a reliance on agents. Maintaining data privacy requires the concerted work of many actors: the OGS companies, their partners, their agents, the regulators that are levelling the playing field and the consumers themselves.**

This briefing note aims to improve data privacy – and by extension, Consumer Protection – in the OGS industry by identifying and sharing best practices for companies that directly collect and process data or enable others to do so across the OGS value chain; from financing solar systems to distributing or remotely servicing them through IoT technology.

Good data privacy practices uphold consumers' interests by processing only data for which there is a legitimate purpose and a benefit for consumers. They empower consumers to take charge of their personal data. As consumers are the rightful owners of their personal data, good practice includes encouraging them to decide whether to trade privacy for additional benefits.

There is an increasing amount of evidence showing that consumers value data privacy. OGS companies that uphold high standards of data privacy are poised to benefit from increased consumer trust and long lasting, more profitable relationships.

Data privacy rests on two main pillars:

- Informed and empowered consumers
- Responsible providers who protect consumers' interests

OGS companies can support the first pillar by helping consumers exercise their rights and by using consent as a mechanism to give them choice and power. Consent becomes a way for consumers to assert their preferences rather than a mechanism to get providers 'off the hook'. Companies can support the second pillar as fiduciaries, by ensuring that data is kept private and secure, acting in consumers' best interests and partnering only with organizations that do the same.

<sup>1</sup> See [Pay-As-You-Go and the Internet of Things: Driving a New Wave of Financial Inclusion in the Developing World](#), Mastercard (2018).

# Table of Contents

<b>Introduction</b>	<b>4</b>
<b>Data privacy and consumer protection</b>	<b>6</b>
Data protection regulation	9
What is personal data?	10
Data privacy risks for OGS consumers	11
Understanding and addressing specific business model vulnerabilities	12
Identifying risks through the implementation of a data registry	13
<b>Empowering OGS consumers through better control of personal data</b>	<b>15</b>
Improving data privacy clauses in OGS consumer contracts	17
Improving mechanisms for consent	18
Empowering OGS consumers to exercise their data rights	20
<b>Protecting privacy for OGS consumers by assuming a fiduciary duty</b>	<b>24</b>
Minimizing the consumer data footprint	25
Implementing good practice through effective training for staff and agents	27
Strengthening data security protocols to enhance consumer protection	28
<b>Conclusion</b>	<b>29</b>
<b>Annexes</b>	<b>30</b>
Annex 1 – General Data Protection Regulation (GDPR) key principles	31
Annex 2 – Personal data risk taxonomy for off-grid solar companies	32

## Published: May 2022

This briefing note was written by GOGLA consultant Isabelle Barrès, and reviewed by GOGLA's Rebecca Rhodes and Puck van Basten.

## Acknowledgements

The GOGLA Consumer Protection Toolkit is funded by CDC (through CDC Plus, funded by UKAID), DOEN Foundation, and FMO. Thank you to GOGLA members we spoke with who shared their experiences of implementing the Consumer Protection Code and how they are improving data privacy within their consumer-facing operations, and to experts who shared insights and knowledge..

## Disclaimer

The information in this briefing note is designed to provide helpful information on the topic. GOGLA and the authors are not responsible or liable in any manner for any damages resulting from use of information in this briefing note.

# Introduction

The OGS industry currently serves more than 480 million people and aims to power 1 billion lives by 2030<sup>2</sup>. The sector typically serves low-income customers for whom a solar product is a significant investment, and through this purchase they are exposed to financial, product and service risk. On top of this, the sector is a fast growing, dynamic industry that depends on customer satisfaction for sustainability.

This is why GOGLA, hand-in-hand with members of the industry, developed the Consumer Protection Code (CP Code). The CP Code aims to safeguard consumers and their rights, whilst at the same time enhancing the impacts of increased energy access for low-income consumers. We believe that widespread industry action on consumer protection is required to mitigate sector risk and accelerate responsible and impactful market growth. A growing number of companies and investors have adopted the CP Code through Commitments and Endorsements<sup>3</sup>, showing that the industry recognises that what is good for consumers, is good for businesses and the sector as a whole.

To help the industry further improve standards of consumer protection, GOGLA is developing a series

of tools and resources for companies. Using lessons and best practice from other sectors and across the OGS industry, GOGLA aims to help companies implement the CP Code, particularly in more challenging areas such as Personal Data Privacy. As many OGS companies are becoming more digitalized; using IoT technology and leveraging a growing volume of consumer data to improve products and services and refine their business model, data privacy and protection is at the same time becoming a growing concern.

This briefing note calls on OGS companies to ensure that consumers are empowered to make decisions about how their personal data is used, and for shared responsibilities between consumers and providers to protect data integrity. It calls for enabling consumers to make informed, meaningful choices about their data and exercise their rights. It calls on providers to secure data privacy across the data lifecycle and act in consumers' best interests. The information shared is based on findings from consultations with GOGLA members and industry experts, and lessons learned from other sectors in which consumer protection is more mature, such as microfinance, financial inclusion and telecommunications<sup>4</sup>. The good practice for strengthening data privacy practices, highlighted within this briefing note are summarised in Figure 1.

**Figure 1 - Good practice for strengthening data privacy practices within OGS companies**

**Start with...**

1. Understand and address specific business model vulnerabilities
2. Take stock of consumer data via a data register

**Empower OGS consumers**

3. Improve OGS consumer contracts
4. Improve mechanisms for consent
5. Empower OGS consumers to exercise their data rights

**Act as a fiduciary for consumer data**

6. Minimize the consumer data footprint
7. Train staff and agents on data privacy
8. Strengthen data security protocols

<sup>2</sup> See [Lighting Global, The 2022 Global Off-grid Solar Market Trends Report](#) and [The off-grid sector can 'Power 1 Billion Lives by 2030' – Here's how.](#)

<sup>3</sup> See [Commitments & Endorsements | GOGLA](#).

<sup>4</sup> See [Center for Financial Inclusion – Consumer Protection and SPTF Standard 4d-Privacy of Client Data.](#)

## Introduction

This briefing note provides specific guidance for OGS companies, but there are existing resources that can also be used. For example, Consumers International is one of three industry groups that has endorsed a global consensus on [privacy and security guidance for consumer IOT](#). It has also developed guidance and recommendations for [IoT standards](#) that OGS manufacturers and software providers can consult to ensure consumer protection is embedded in the product development phase<sup>5</sup>. The [GSMA standards for mobile money providers](#) can assure PAYGo companies that their payment-system partners are upholding required standards. A few other noteworthy data privacy frameworks have informed the recommendations in this brief<sup>6</sup>.



**Responsible data protection policies are the bare minimum. It is crucial to go beyond policies and ensure that these are effective in protecting the privacy and integrity of client data.**

FMO<sup>7</sup>



© M-Kopa

<sup>5</sup> See [Trust by Design Guidelines](#), Consumers International (2019).

<sup>6</sup> See [GOGLA Consumer Protection Code and Indicators](#) (2019); [UN Principles for Responsible Digital Payments](#), Better Than Cash Alliance (2021); [Client Protection Standards for Digital Credit](#), CFI (2019); [Handbook on Consumer Protection for Inclusive Finance](#), CFI (2019); [Making Data Work for the Poor](#), CGAP (2020); [Guideline Note on Data Privacy for Digital Financial Services](#), AFI (2021).

<sup>7</sup> See FMO: [Mitigating Consumer Risks in a Digital Age: Recommendations for Funders](#).

“

**Data privacy and  
consumer protection**

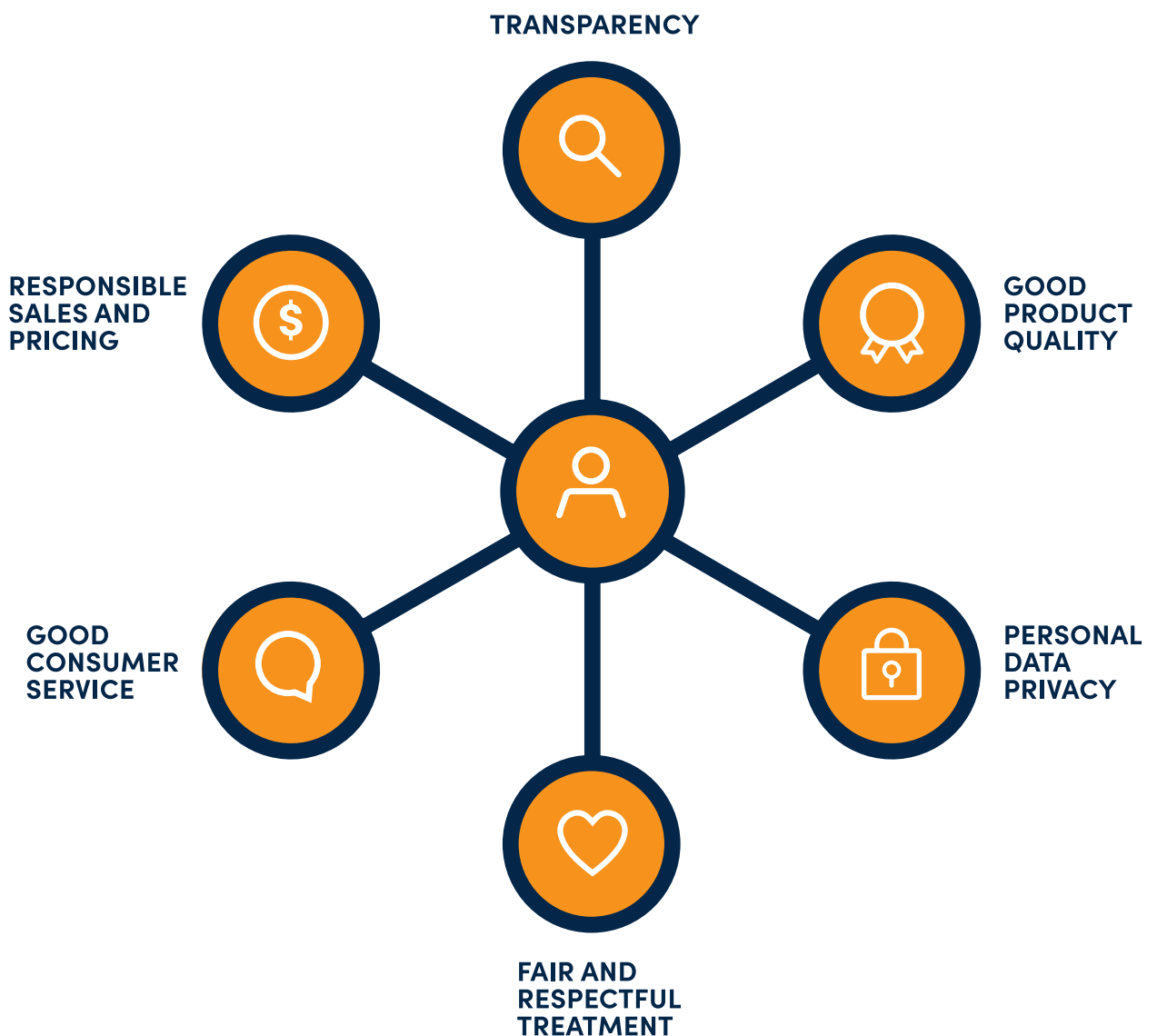
”

# Data privacy and consumer protection

The CP Code consists of six principles, each with a set of indicators, and an assessment framework to help companies measure, demonstrate and improve their performance against the Code – regardless of business model. The Code provides investors and other stakeholders with a framework to promote good practice. The six principles are transparency, good product quality, data privacy, fair and respectful treatment, good consumer service and responsible sales and pricing. The principles are considered the minimum standard of practice that should be expected of OGS companies.

**Data Privacy** is a growing concern within the OGS sector as the volume of personal data collected by companies increases, and globally, the number of exposed records is increasing exponentially<sup>8</sup>. As OGS companies leverage more and more data from consumers, and partner in new and different ways with a range of actors to improve access and services, they will need to do so in a way that respects consumer choices, minimizes exposure and protects against the risk of increasing data-driven attacks.

Figure 2 - The Consumer Protection Principles<sup>9</sup>



<sup>8</sup> See [The Evolution of the Nature and Scale of DFS Consumer Risk – A Review of the Evidence](#), CGAP (2022).

<sup>9</sup> See GOGLA's [Consumer Protection Principles](#).

# Data privacy and consumer protection

Figure 3 – Personal Data Privacy: Principle and Indicators from the CP Code<sup>10</sup>

## The data privacy principle

- The company applies good practices and complies with relevant laws and regulations governing consumer data privacy.
- The company only collects, uses, retains and shares personal information that is necessary for the stated consumer service and legitimate interests of the business.
- The company ensures consumer data is kept secure and confidential.

## The data privacy indicators

- E1 The company complies with all relevant laws and regulation governing data privacy in its country of operations.
- E2 The company only collects, uses, shares and stores personal data (including KYC, energy usage and payment information) for which there is a legitimate interest.
- E3 The company obtains meaningful consent from consumers for the sale of personal information (and for purposes other than legitimate interests) to third parties such as advertisers.
- E4 Personal data (in both paper and electronic copies) is adequately protected/encrypted to minimise risk of data theft or misuse in all storage and transmission.

Data Privacy also overlaps significantly with the principle of Transparency, given the need to ensure consumers are well informed and understand the terms of the data privacy clause within a PAYGo contract. For consent to be more effective, consumers should understand what personal data is collected, with whom it will be shared, and how it is handled<sup>11</sup>.



**Data privacy is not a key concern until there is an alignment and understanding on what can happen. If they [consumers] were told their personal data could be used for marketing, they wouldn't want that to happen.**

Ben Wallingford,  
MFR, Regional Manager  
for Anglophone Africa



**We still need to address data privacy and protection, as there are risks with digital financial services such as data abuse, identity threat, etc.**

Dr. Alfred Hanning,  
AFI Executive Director<sup>12</sup>



<sup>10</sup> See GOGLA's Indicators for Consumer Protection: Data Privacy.

<sup>11</sup> See GOGLA's Indicators for Consumer Protection: Transparency. In particular, see indicators A1 and A7.

<sup>12</sup> See Speech at Financial inclusion virtual workshop on data usage and data protection and their implications for financial inclusion (2020).



# Data privacy and consumer protection

As PAYGo companies in particular evolve and build innovative business models with increased reliance on personal data to offer products and services to consumers, it has never been more important to ensure that personal data is adequately handled within the industry.

In addition, for PAYGo companies reliant on mobile money transactions, a weak data ecosystem (i.e., lack of cybersecurity rules and regulations, or weak connectivity that result in frequent failures) and increasing consumer demands – such as “growing demand for superfast, easy transactions”<sup>13</sup> – can compromise transaction integrity. Globally, attackers are getting more and more creative, and it is hard for providers and regulators to stay ahead of the game and anticipate attacks or at least respond to them quickly.



**Data privacy is important not just in our sector, but in daily life. The topic is relevant in every part of the world.**

OGS company



Researching the impact of poor data privacy across the Digital Financial Services (DFS) landscape, CGAP determined that from 2016 to 2020, data vulnerabilities rose significantly as “the increase in records exposed was more than double the increase in data created.”<sup>14</sup> Furthermore, it is estimated that globally, the number of records compromised in just one year during 2020 represents a 141% increase compared to 2019, which is “by far the most records exposed in a single year” since data-breach reporting began in 2011<sup>15</sup>, and risks are exacerbated by increasing sophistication of fraudsters.

Lack of adequate protection of databases has been shown to lead to exposure of OGS consumer

data. In 2016, an unprotected database containing personal information of close to 19,000 consumers from Guatemala and South Africa was discovered by a researcher. The database was accessible for months and exposed the consumers name, address, exact GPS location, occupation, phone number and photo IDs<sup>16</sup>. While a rare case on record, this example shows that the off-grid solar sector is not exempt from these attacks.

## Data protection regulation

Data protection laws aim to put more control in hands of customers while also making providers accountable. There have been many advances in data protection policy regulation over the last few years – both globally and within off-grid markets. The European General Data Protection Regulation (GDPR)<sup>17</sup> stipulates that processing personal data should have a positive benefit on society and give individuals control over their data<sup>18</sup>. It has become a global reference for data protection laws, including for countries where OGS companies operate (e.g., Kenya, Uganda). Across OGS markets, data privacy laws are increasingly commonplace, and companies should be aware of the regulations that govern their operations. This [Map of Data Protection Laws](#) helps to keep track of advancements in data protection laws.

The GDPR approach is anchored around a set of 7 core principles<sup>19</sup>:

1. Lawful, fair, and transparent processing
2. Purpose limitation
3. Data minimization
4. Accurate and up-to-date processing
5. Limitation of storage in the form that permits identification
6. Confidential and secure
7. Accountability and liability

Given the prevalence of the PAYGo model in the OGS sector and its dependence on mobile payments, on IoT technology to remotely control and monitor devices, and on agent-based sales networks, these areas should be given special attention when addressing data privacy and ensuring compliance with local laws.

13 See [Handbook on Consumer Protection for Inclusive Finance](#), CFI (2019).

14 See [The Evolution of the Nature and Scale of DFS Consumer Risks – A Review of the Evidence](#), CGAP (2022).

15 Cyber Risk Analytics identified 37 billion records that were exposed in 2020 and estimates that this number is grossly underreported. See [2020 Year End Report – Data Breach QuickView, Risk Based Security](#) (2020).

16 See [An unsecured database leaves off-the-grid energy customers exposed](#), Zero Day (2018).

17 See [General Data Protection Regulation](#), European Union (2018).

18 See [GDPR Recital 1](#): Everyone has the right to the protection of personal data concerning him or her; [GDPR Recital 4](#): The processing of personal data should be designed to serve mankind; and [GDPR Recital 7](#): Natural persons should have control of their own personal data.

19 See [GDPR: Know the Seven Key Principles](#), Information Security Buzz (2017). For more details, see Annex 1.

# Data privacy and consumer protection

## What is personal data?

In the OGS sector, companies process a wide range of consumer data. In addition to collecting data directly from consumers such as basic Know Your Customer (KYC) data (e.g., name, address) and income-related data (e.g., housing type, family size, education/literacy level) PAYGo companies also generate a large amount of financial and transactional data, as every payment, SMS or call creates a data point. Internet of Things (IoT) technology embedded in the solar devices also enables companies to capture a wealth of transactional data about usage. All that data – to the extent it can be traced back to individual consumers – is considered personal data and is protected under data privacy laws.

## Data privacy risks for OGS consumers

Consumer risks related to data privacy are numerous and can be exacerbated by the nature of PAYGo business models.

Risks are present along the entire data lifecycle, from collection to use, to sharing it with third parties and eventually disposing of it. Understanding how data can be compromised at the different stages of the data lifecycle helps to develop appropriate mitigation strategies (such as policies, training, system security). Each stage of the data lifecycle presents distinct risks, driven

by the individuals involved on each side of the data transaction and the policies and protocols pertaining to data processing, the security of the systems and the channels involved. The data lifecycle and associated risks are shown in Figure 5 on the next page.

Data can potentially be compromised by anyone who has access, including internal staff, agents, third-party providers – or even consumers themselves, who can fail to safely guard their contracts or share PINs with others. Personal data processing can be compromised due to inadequate systems, policies or processes or inappropriate practices (whether policies or processes are adequate or not).

The risks from processing personal data can take many forms and result in varying degrees of harm to consumers including a range of “physical, material or non-material damage”. For example, personal data processing can lead to “discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorized reversal of pseudonymization”<sup>20</sup>. Other risks include suffering from economic or social disadvantages due to loss of control over one’s personal data.

Figure 4 - Poor data privacy harms both consumers and companies



20 See GDPR Recital 75: Risks to the Rights and Freedoms of Natural Persons. Processing sensitive data in particular (health, religion, political opinions, racial or ethnic origin, etc.) can be done maliciously to discriminate or harm individuals or impersonate and manipulate them. While compromising the privacy of sensitive information (i.e., health, religion, etc.) can also lead to psychological harm (i.e., blackmail, harassment, reputation damage, shame) this is less likely to be the case in the OGS sector given the nature of the information that is collected and handled.

# Data privacy and consumer protection

Figure 5 - Risks across the data lifecycle



# Data privacy and consumer protection

## Differences across OGS models

Not all OGS companies are equally affected by data privacy issues. The type of business model (distributor vs vertically integrated vs software company, cash sales vs PAYGo, etc.) influences both the type of consumer data collected and the way in companies interact with it.

Data vulnerabilities are exacerbated by the volume of data processed, number of external partners and complexity of the OGS business model. The risks therefore related to personal data increase as business models become more complex and involve more partners, or arm's length relationships with an outsourced workforce such as sales agents. The risks also increase with the size of a company's database and the sensitive or financial nature of data, which is more valuable to hackers and therefore more likely to be used maliciously. Ultimately, the security of the underlying systems used to process data – from collection to transfer to storage – and the robustness and effectiveness of data privacy practices determine whether data will be compromised.

## Understanding and addressing specific business model vulnerabilities

Companies are advised to review their business model and identify the elements that are more relevant to data privacy practices. For example, where in the value chain is data exchanged most frequently, and who/how many parties are involved? Where are processes digitised or data flows increased because of fragmentation between value-chain actors? How is consumer data protected?

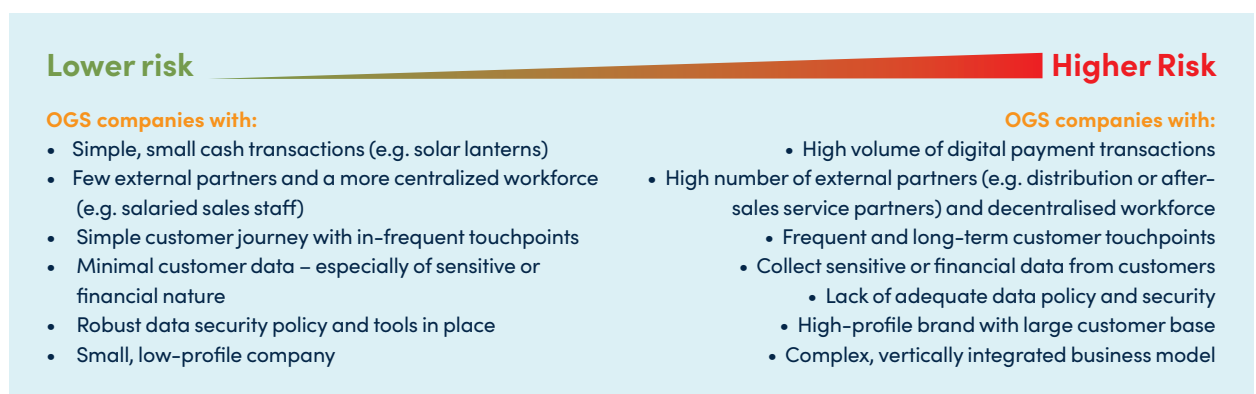
More specifically, companies should note the following areas of their business model when reviewing data privacy practices:

- Consumer-facing activities within the value chain (e.g., sales and aftersales services) – especially any that are outsourced to agents or third-party providers.
- Management of digital credit, digital payments and partnerships with mobile-money providers
- B2B partnerships that involve end-user consumer data (e.g., PAYGo software services)

For example:

- Companies that **manage agent networks** should be mindful of the incentives, training and audit needs that ensure that agents will embrace good practices and only have access to personal data that is relevant for them to perform their duties.
- **Distributors** should process data within secure software platforms or should ensure that secure protocols are in place if the data is exported.
- Companies that offer **software or hardware solutions** should pay particular attention to the data security protocols of their offering. A software company that provides a platform to distributors may be agnostic to the data that is collected and processed, much like Google does not concern itself with the data processed by Google Sheet users. For them, the issues lie more on the data security side: ensuring that the software platform has robust security.
- **Manufacturing companies** should integrate data privacy considerations in the product design phase, especially related to IoT protocols.
- Companies that are not working directly with the end consumers (e.g., PAYGo software providers) can encourage their clients to embrace good practices to protect consumer data. See box at page 14 for an explanation of how this is being done by Solaris Offgrid.

Figure 6 - Factors affecting data-risks in OGS companies



# Data privacy and consumer protection

## Identifying risks through the implementation of a data registry

**OGS companies are encouraged to take stock of consumer data by implementing a data registry.**

The objective for the data registry is to identify each type of data that is collected and used, where it comes from and the business purpose for processing the data.

Reasons for processing data could include legal obligations (KYC, AML/CFT<sup>21</sup>), checking credit worthiness (with credit registry or credit bureau), and/or offering and servicing the OGS product, financing the OGS product (PAYGo).

Typical sources of data include the consumers themselves, the data collected through observation or a credit bureau. Legal basis for processing

includes for legal obligation, for the performance of a contract or with explicit informed consent from the consumers.

## Benefits of a balanced risk mitigation approach

When data privacy is ‘working’, everyone is doing their part: consumers are empowered and providers embracing and living up to their fiduciary duty. Providers offer only choices that benefit consumers and include an option to use as little data as needed to offer the basic service. Consumers decide if they allow their provider to use more of their data in exchange for additional benefits. In the following sections, we will look at recommendations for OGS companies to empower consumers and improve data privacy practices.

**Figure 7 - Illustrative example of a basic data registry<sup>22</sup>**

Reason for processing	Data owner	What data			Data processing				Control
		Type of data	Source of data	Purpose / basis of collection	Point of collection	Update frequency	Storage Location	Retention	
Provision of OGS product and related services	Customer	Name	Customer interview	Customer Identification	PoS / Sales agent	As re-quired	CRM software		Head of Sales
		Telephone number	Customer interview	Customer identification and service provision	PoS / Sales agent	As re-quired	CRM software		Head of Sales
		Geo-lo-calisation coordinates	GPS location / W3W	To supply installation and aftersales services	Product installation	No, unless correction required	CRM software		Head of Sales
		National ID number	Consumer interview	Verification of customer identification – required by CRB	PoS / Sales agent	N/a	CRM software		Head of Sales
		Housing type	Customer interview / visit	KYC for product financing	Credit check (call centre)	N/a	CRM software		Head of Credit
	Size of household	Customer interview	KYC for product financing – verify capacity to repay	Credit check (call centre)	N/a	CRM software		Head of Credit	
	Guarantor	Name	Customer interview	Provision of guarantor for product financing	Credit check (call centre)	N/a	Contract – manual record	Until end of repayment	Head of Credit
	National ID number	Customer interview	Provision of guarantor for product financing	Credit check (call centre)	N/a	Contract	Until end of repayment	Head of Credit	
Provision and improvement of predictive aftersales service (IoT products)	Customer	Energy usage – kWh and times	Product – automated GSM transfer	Consent from customer	From installation	Daily	PAYGo software – BMS	10 years	Head of After-sales
		Payment data	Mobile Money provider	Payment for product/ service	From installation	Daily	PAYGo Software – Payments		Head of After-sales

<sup>21</sup> Anti-Money Laundering/Combating the Financing of Terrorism. Definitions from the International Monetary Fund

<sup>22</sup> Based upon the example provided at: [Data protection compliance: Part 1: Know your data: Mapping the 5 W's](#), Isle of Man Information Commissioner (2021).

# Data privacy and consumer protection

## Case Study: Solaris Offgrid is creating incentives for partners to protect data privacy

Having made an Endorsement of the GOGLA Consumer Protection Code, [Solaris Offgrid](#), through its software PaygOps, is working to support the distributors it works with in adopting good data security practices – helping OGS companies to fulfil the minimum standards of practice in their treatment of customers, particularly related to the processing of personal data. They do this through education, incentives, and nudges. In addition, as a third-party service provider, Solaris Offgrid doesn't sell or take ownership of the distributor's data – a feature written into all their B2B contracts and outlined in discussions with clients. Here's a look at what they're doing:

### Educate

Solaris Offgrid shares an example consumer contract with distributors using its PaygOps software service and points them to initiatives outside the OGS PAYGo sector, such as [www.tosdr.org](http://www.tosdr.org) (terms of services didn't read), to illustrate how companies can summarize key information in contracts in a concise yet transparent manner to help consumers better understand. The idea is to give consumers a better sense of what they are signing off on, in a simple and easy to comprehend format. GOGLA's [Key Facts Statement](#) can also help here.

### Incentivize

Solaris Offgrid incentivises distributors to stay within their PaygOps secure platform for any data analysis needs (i.e., use their Business Intelligence/BI tools). They partner with other BI tool providers so that instead of using Excel or other offline programmes, distributors can use more secure tools and avoid storing data on personal computers which puts consumer data at risk.

### Nudge

Solaris Offgrid has developed several "nudges" to steer distributors towards better data privacy and security practices. These nudges are a collection of small incentives embedded in the PaygOps software itself that set the default settings of the software to the highest level of security – meaning that distributors need to take action to disable the secure settings. A few examples include:

- **Nudges to stay in Solaris Offgrid's PaygOps platform secure environment**, such as a new function that makes the dashboards and sheets more visible so that people are more inclined to use these rather than using the spreadsheet exports.
- **Nudges to enforce good practices for data security**, such as putting in place two layers of authentication on the mobile app by default to encourage them to adopt strong password policies.

“

**Empowering OGS  
consumers through  
better control of  
personal data**

”

# Empowering OGS consumers through better control of personal data

Good practice for OGS companies, their agents and partners is to ensure that OGS consumers:

- Know what personal data is collected and generated, and how the OGS company processes it:
  - o the OGS company staff or agent explains the key terms contained within the contract, and the contract is easily understood in the consumer’s own language.
- Are equipped to make an informed decision and decide what is best for them:
  - o Consumers clearly understand what they are getting in exchange for consenting to share more personal data with the OGS company and its partners. OGS company staff or agents are trained to explain how this additional data benefits them (e.g., product-use data can help provide preventative maintenance).
  - o They have choices, and are not forced to share more data than the minimum required to offer the service. Consumers can consent to give away a little or a lot of their privacy in exchange for different levels of service.
- Know their rights and how to exercise them:
  - o OGS companies explain what their data rights are (see Figure 8) and provide channels for them to exercise them.

Companies can achieve these outcomes by following the steps shown in the orange box.

## Relevant indicators

**CP Indicator E3:** The company obtains meaningful consent from consumers for the sale of personal information (and for purposes other than legitimate interest) to third parties such as advertisers.

**(Transparency indicator) A1:** Consumers are informed of key terms and conditions of the contract.

**(Transparency indicator) A7:** The company informs consumers which of their personal data is collected and stored.

## Good practices to help consumers make better decisions about their data

### Improve OGS consumer contracts:

- Make sure consumer contracts are complete and readable
- Improve the delivery of the contracts

### Improve mechanisms for consent:

- Give OGS consumers choices
- Protect consumers by default

### Empower OGS consumers to exercise their rights:

- Make it easy for consumers to access their data and enact their rights.

Figure 8 - Empowering consumers through data privacy\*

My data	My rights	My choice
<b>Personal data</b>	<b>Data rights</b>	<b>Data choices</b>
ID, name	Have access	Informed consent
Transactions	Be forgotten	Meaningful consent
Financing	Be notified	Mandatory choices
Behaviour	Object	Optional choices

\* Illustrative examples



# Empowering OGS consumers through better control of personal data

## Improving data privacy clauses in OGS consumer contracts

PAYGo contracts can be long, complex documents. Data privacy may not jump out as a highlight, but evidence shows that consumers care deeply about data privacy. When looking at Digital Financial Services, evidence shows that consumers not only value data privacy, but they are willing to pay more for it and use it as a differentiator when it comes to choosing who to engage with<sup>23</sup>. Nonetheless, the challenges of communicating this type of information to consumers in a meaningful way are enormous.

Companies should seek to avoid being vague in clauses related to data privacy. For example, when identifying partners that consumer data may be shared with, companies should be clear about who these are – or at least the types of organisations (such as credit reference bureaus) in which current or future data-sharing partnerships might occur. Companies are encouraged to audit contracts and terms of service for content completeness, clarity, and readability.

## Making sure consumer contracts are complete and readable

First, OGS companies should ensure that what they are asking consumers to consent to (whether a data privacy policy, terms of services or contract) contains all the relevant information of how data will be processed and who it will be shared with.

OGS companies should also ensure that the information is understandable. There are several tools available to help companies evaluate the readability of contracts<sup>24</sup>. [The Gunning Fog Index](#), for example, is one of the most reliable and simplest to apply and could be used by OGS companies to evaluate the readability of their policies. With a simple formula, it generates a “readability score” and estimates the level of education that is required to understand the text analysed. This could be especially helpful in contexts where consumers have low levels of literacy.



**The contract is 8 pages long, with 20 different clauses. The data protection clause is half a page and not a focus of the communication with the consumers or the training.**

OGS company



**The contract is very long and detailed, but agents may be in a rush and just asking customers to ‘Sign here’.**

OGS company



**We agree that contracts in their current forms are often not understandable.**

OGS company



**We have the contract with a simplified version that summarizes the most relevant information, but the summarized version does not have anything on data privacy.**

OGS company



<sup>23</sup> See [Is Data Privacy Good for Business?](#), CGAP (2019).

<sup>24</sup> Examples of readability scoring mechanisms include the following indexes: Flesch-Kincaid Grade Level, Gunning Fog Index, Coleman-Liau Index, SMOG Index or Automated Readability Index. See [Digital Finance and Data Security – How Private and Secure is Data Used in Digital Finance?](#), CFI (2018).

## Empowering OGS consumers through better control of personal data

### Improving the delivery of contracts

In many cases, OGS companies depend on sales agents to convey the key information needed to enable consumers to make informed decisions. Ensuring that agents abide by company policies and do not take shortcuts in explaining the key contract features to new customers is important. Implementing a Terms and Conditions (T&C) script for agents, a Key Facts Statement (KFS), a welcome call managed by a centralized customer service team, and monitoring customer complaints – can all help improve company practices and provide assurance of implementation<sup>25</sup>.

### Improving mechanisms for consent

As rightful owners of their personal data, individuals should decide how it is processed and with whom it should be shared. Apart from the few exceptional cases (e.g., data that is required by law), consumers “should be empowered to decide” what happens to their personal data, through the mechanism of informed and explicit consent.

The desire of OGS companies to improve consent and transparency around data privacy came out overwhelmingly in the consultations conducted in preparation for this briefing note. Such companies are advised to first determine where there is a legitimate purpose for processing consumer data, and only then ask for consumer consent. Consent should not be used as a justification for data processing unless there is a legitimate purpose for it, as highlighted later in the briefing note.



© Solaris

# Empowering OGS consumers through better control of personal data

## Consent is broken

Unfortunately, it is widely recognized that current practices for seeking consent do not work<sup>26</sup>. While the notions of ownership, control, and rights are well intended and needed, they are, in their current practice, not yielding the desired outcomes for data privacy. Consent can give a false sense of protection and ownership – a consumer may ‘check a box,’ but this may be neither meaningful nor informed, rather a necessary evil to gain access to a service. Further, consumers often don’t know their rights, and these are complicated to exercise.

Where “consent documents” (contracts, terms of services, privacy policies, sales agreement, etc.) are not written according to transparency best practices, they do not enable informed choices and explicit consent. Long bodies of text, small print and legal jargon do not aid consumer understanding nor empower consumers to determine what trade-offs exist between privacy and services.

The below figure is based upon internet usage, but illustrates the point that very few people realise the specifics about the data they share on a daily basis. Consumers wrongfully assume that companies will play a fiduciary role and look out for their best interest.

This blind trust phenomenon is exacerbated for individuals with lower levels of education, as recent research demonstrates: “adults with lower levels of education are more likely to falsely assume that when a company posts a privacy policy, it ensures the company will keep all of the information it collects on users confidential”<sup>28</sup>.

More often than not, consent in its current form is neither informed nor meaningful:

- Privacy policies are unclear and complex – that means it is unrealistic to expect consumers to

read (and understand) the information that is shared with them<sup>29</sup>.

- Consumers are often not given a choice between levels of privacy and service. Where a service is valuable to the consumer, they are therefore likely to sign consent forms without reading them.
- The default mechanism is too often set to ‘opt-out’ rather than ‘opt-in,’ meaning consumers have to take proactive action to protect their data. Rather, companies should be asking consumers to take action to share their data.



**Why do we not have any global way of saying no to tracking across the board, as we do to the world when we ...lock our doors? We don't because, more than two decades ago, it was easier to put servers in charge of what consumers could do, and we got stuck there."**

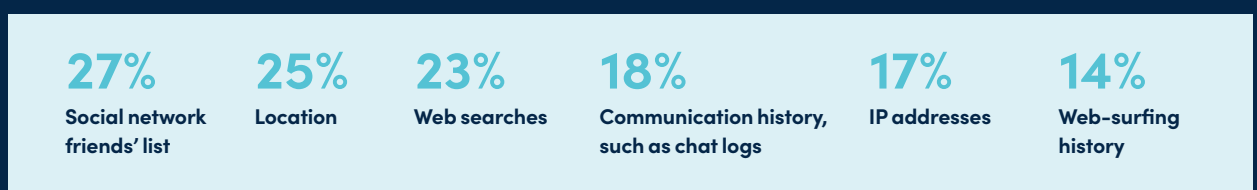
Online commentary,  
Doc Searl, OGM, May 18, 2021



## Is trying to “fix consent” enough?

While the best efforts to improve consent are likely to always be a step behind given the fast pace of data-driven innovation and increasing complexity around data, companies are advised to seek ways to make improvements. and supplement with complementary measures. One such measure is to shift the onus of responsibility for data privacy onto providers<sup>30</sup>. In doing so, companies can leverage the opportunity to raise awareness with consumers and empower them to make choices about their data. Consumers should then also have the opportunity to change their minds and withdraw consent if desired.

Figure 9 - In the dark about data<sup>27</sup>



26 See [I Do Not Accept These Terms & Conditions](#), CGAP (2020).

27 See [Customer data: designing for transparency and trust](#), Harvard Business Review (2015).

28 See [Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans](#), Washington University Law Review (2017).

29 See [Making Data Work for the Poor](#), CGAP (2020).

# Empowering OGS consumers through better control of personal data

## Giving OGS consumers choices about their data

With respect to data privacy, there cannot be meaningful consent in the absence of choice<sup>30</sup>. The GSMA Code of Conduct reiterates this point as well<sup>31</sup>. Instead of asking consumers for a blanket consent as is often the case (i.e., 'consent to everything'), providers should be more discerning and give consumers a choice.

Since GDPR went into effect in 2018, companies across the globe have scrambled to update their online presence to be GDPR compliant. One of the consequences of this is the option presented to consumers when they visit a website, to choose how they agree for their data to be tracked (through "cookies"). While more needs to be done to make this process effective and reduce the annoyance for consumers, it allows to see a glimpse of what better framed consent options could look like.

Choices presented to consumers should include at minimum a distinction between mandatory and optional data sharing:

- **Mandatory data sharing** should be what is required to offer the product or service, or required by law (e.g., reporting to a credit bureau).
- **Optional data sharing** is everything else, and may or may not impact the functionality of a product or service. For example, if a consumer 'opts-in,' this may provide enhanced functionality

or personalisation; or have no impact on the service, but support analytics to encourage improvements over time, or enable targeted communications or marketing.

**Companies are encouraged to ensure consumers understand the difference between what is mandatory vs optional, and be transparent about the trade-off between functional/service benefits and privacy.**

For example, if an OGS company collects more data (e.g., usage data) than is needed to offer the service, consumers should be aware of the intended use for this data. This could include providing customised customer support or analytics for product improvements.

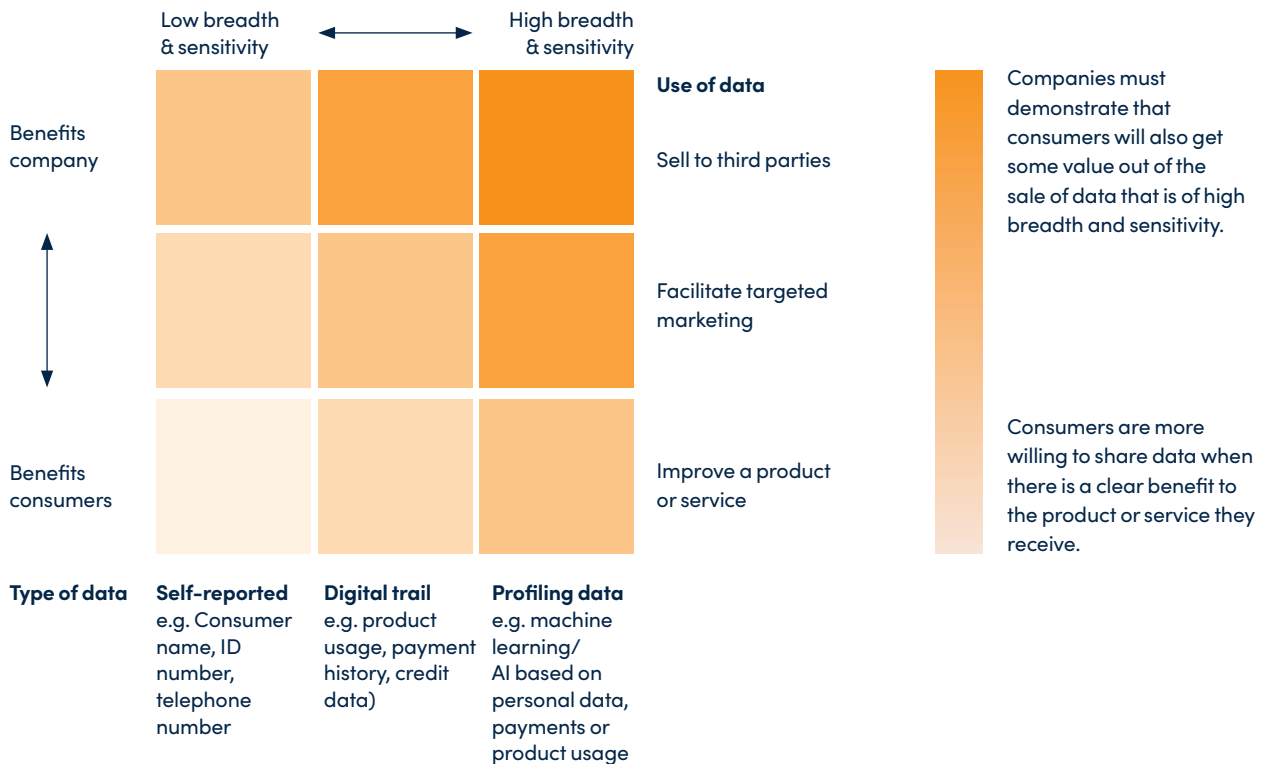
This type of trade-off is illustrated in Figure 10 below. There is a relationship between the use and type of data, and the sensitivity and who benefits from it. For instance, if self-reported data is sold to third parties, the sensitivity of the data is likely to be low and so consumers expect less in return. On the other hand, consumers may only be willing to give up more sensitive data (such as payment behaviour) for company benefit, if they in return receive something of demonstrable value.

30 See [GDPR Recital 32](#): Conditions for consent: "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement." "Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them" and [GDPR recital 42](#): Burden of proof and requirements for consent: "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

31 See [GSMA Mobile Money Certification Principles](#), GSMA (2018) Indicator 8.3: Customers' control of their personal data: Providers shall ensure that customers are informed of their rights and have opportunities to exercise meaningful choice and control over their personal information.

# Empowering OGS consumers through better control of personal data

**Figure 10 - Swapping value for data – The more people value data, the more they expect companies to provide in return for it**



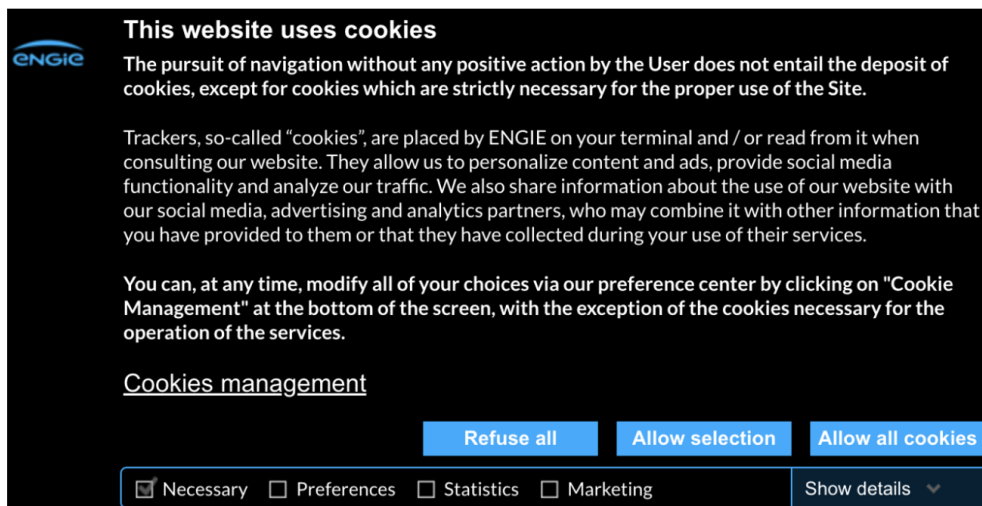
Adapted from: *Customer data: designing for transparency and trust*, Harvard Business Review (2015)

## Protecting consumer data by default

**Companies implementing best practice protect consumer’s personal data by default.** To implement this, PAYGo companies can add an option in the contract asking consumers to opt-in to allow them to process more data than is currently needed – provided it brings potential benefits to

consumers. Similarly, any OGS company with an online presence should ensure that their website asks users to opt-in to share more data than the minimum needed to operate – “reject all/refuse all” should be the default option for cookies settings<sup>32</sup>.

**Figure 11 - Embedding privacy by default: Opt-in**



SOURCE: Engie’s Website (accessed March 2022).

32. See [GDPR Recital 32](#): Conditions for consent: “Silence, pre-ticked boxes or inactivity should not therefore constitute consent.”

# Empowering OGS consumers through better control of personal data

Some OGS companies have found that consumers (valuing higher levels of privacy) will block all SMS messages from a company in order to avoid receiving marketing messages. However, this means that they miss important service, transaction or account information. To avoid this, companies can distinguish between transactional and marketing messages – implementing separate communication channels for each. In doing so, consumers are able to ‘opt-out’ of or manually block marketing messages but stay informed about critical product or service information.

## Empowering OGS consumers to exercise their data rights

GDPR incorporates a number of key data consumer rights that are intended to help consumers ensure their personal data is being used according to their consent. These include:

- Right of access
- Right to rectification
- Right to erasure (“to be forgotten”)
- Right to restriction of processing
- Right to be notified
- Right to data portability
- Right to object
- Right not to be subject to automated individual decision-making, including profiling

Nevertheless, consumers are generally not aware or empowered to exercise these rights, and this may be exaggerated in a consumer base that has low levels of digital literacy, such as the OGS context. Furthermore, exercising data-related rights is too often overly complex and impractical.

To help empower consumers beyond consent, CGAP has suggested that companies implement a ‘Digital Bill of Rights’,<sup>33</sup> with the aim of informing consumers of their rights and educating consumers how they can be exercised. Such a Bill would “empower consumers to control their own data by allowing them to easily access, correct and port data free of charge”<sup>34</sup>.

Another approach, such as the one adopted by Engie (see Figure 12), enables consumers to exercise

their rights through their online platform – making it easy for consumers to submit a request related to the processing of their personal data (e.g., accessing it, rectifying it, deleting it, or other). As many OGS consumers may not have access to online platforms, companies should also ensure that the same request form is available via service centres, shops and call centres.

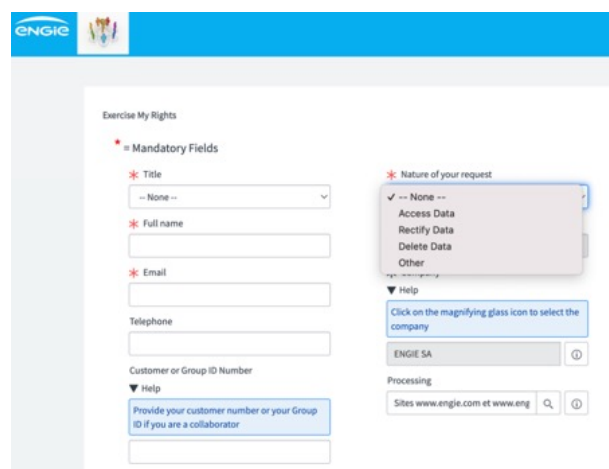
With rights, however, come responsibilities. OGS companies can also seek to raise awareness about the consumers’ own responsibility to protect their data, such as:

- How to create strong credentials (i.e., passwords, PINs)
- How to secure credentials
- How to identify and react to common frauds/scams

## The right to rectification and PAYGo payments

The right to rectification is particularly critical in the context of PAYGo models, as a late payment due to funds sent to the wrong account can result in OGS consumers having their lights cut-off until the problem is resolved. Rectification of such errors is even more important if the consumer profile is linked to Credit Reference Systems (CRS) and could result in negative credit reporting. In such cases, data should be rectified promptly, or verifications put in place to avoid errors all together.

Figure 12 - Raising awareness of data rights



SOURCE: Engie’s Website (accessed March 2022).

33 See [Making Data Work for the Poor](#), CGAP (2020).

34 See [3 Data Protection Approaches That Go Beyond Consent](#), CGAP (2019).

## Empowering OGS consumers through better control of personal data

### Case study: Partnering with MNOs to handle payment reversals for the benefit of the consumer

For person-to-business transfers (e.g., PAYGo payments), Mobile Network Operators (MNOs) do not handle mis-allocated payments on their own, as they do for peer-to-peer transfers. Rather, they ask the OGS to take action such as executing a refund (if the transfer was made by mistake) or crediting the appropriate customer account (if money was sent to the wrong account number).

In order to better address this issue by pre-emptively addressing data errors, and avoiding negative consequences for customers, one PAYGo company in Kenya has established an effective partnership with mobile money provider, Safaricom.

Before any payment is allocated, staff from the PAYGo company cross-check and confirm that the money will go to the right account. While this approval process delays the payment slightly, it ensures that credit is allocated to the right account and that no corrections will be needed. From a consumer perspective, the trade-off is waiting 5 minutes for SHS activation – and lights being turned on – for a reduced risk of misallocation that may result in additional time/days spent without power whilst they and the company rectify the error.



“

**Protecting privacy for  
OGS consumers by  
assuming a fiduciary duty**

”



# Protecting privacy for OGS consumers by assuming a fiduciary duty

OGS companies should assume a fiduciary duty and act in consumers' best interests. As CGAP highlights, a fiduciary duty "can help establish the trust and confidence among customers that their data are being used responsibly, making them more willing to use new products and services"<sup>35</sup>.

OGS companies can achieve this by following the good practice shown below:

## Good practices for adopting responsible data practices in OGS

### Minimize the data footprint to reduce exposure

- Conduct a legitimate purpose test
- De-personalize the data

### Train staff and agents to ensure robust implementation of data protection practices

### Strengthen data security for OGS companies and third-party providers.

**Minimizing the consumer data footprint**  
OGS companies can aim to minimize the consumer data footprint, by processing only data absolutely needed to offer the service and only data for which there is a legitimate purpose. As personal data is data that is identifiable, OGS companies can also minimize their personal data footprint by "de-identifying" it and making it "no longer personal".

## Ensuring legitimate use of consumer data

A core element of good practice in data privacy is that personal data should only be processed when there is a legitimate purpose to do so. Implementing a data register as described earlier in this briefing note can help companies determine what their data needs are, how critical each data field is for various business functions, and what the purpose is for processing it.

## Relevant indicators

**CP Indicator E2:** The company only collects, uses, shares and stores personal data (including KYC, energy usage and payment information) for which there is a legitimate interest.

**CP Indicator E4:** Personal data (in both paper and electronic copies) is adequately protected/ encrypted to minimize risk of data theft or misuse in all storage and transmission.

CGAP's approach to legitimate purpose which is adopted in this brief is clearer than the existing GDPR guidelines, which allow for legitimate purpose to be over-written by consumer consent and use a more open-ended language in terms of what is permissible.

*"Consumers' personal data should be processed in ways that are consistent with reasonable expectations they have formed based on their relationships with services providers [...] Providers should be limited to collecting, creating, using, and sharing data necessary for or compatible with the services being provided. [...] Hence, when the data are no longer necessary for legitimate uses, these data should not be retained in identifiable form. A key feature of a legitimate purposes approach is that it cannot be overridden by obtaining individual consent."*<sup>36</sup>

A legitimate purpose for processing data exists if it is necessary to provide or complementary to a product or service. For OGS companies, this may include processing data:

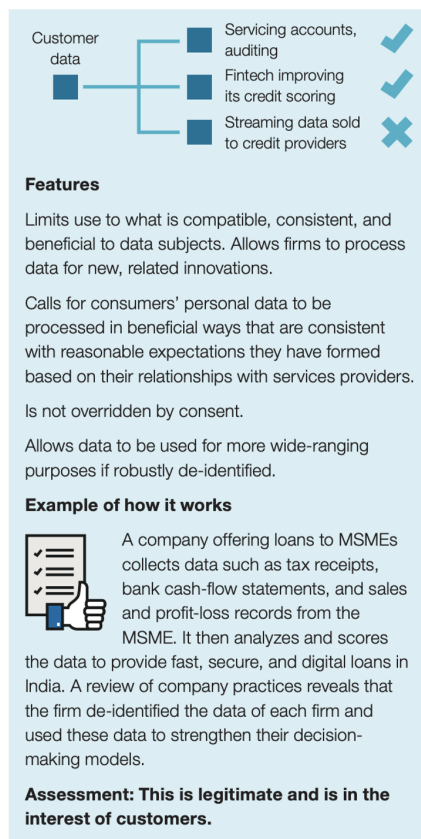
- To make decisions about product financing
- To report to the credit bureau
- To process payments
- To control access to OGS devices in cases of non-payment
- To make sure the service is working properly
- To monitor the functioning of the OGS product, to provide predictive servicing or to fulfil warranty terms.

<sup>35</sup> See [Making Data Work for the Poor](#), CGAP (2020).

<sup>36</sup> As stated by CGAP "GDPR and Convention 108+ provide that information must be collected for explicit, specified, and legitimate purposes and not processed in a way incompatible with those purposes. However, there is a significant difference between requiring the uses be compatible with the purpose for which information is collected, as is the case for a legitimate purposes approach, as opposed to not being incompatible, which seems to permit a broader range of uses beyond what consumers would likely expect." See [Making Data Work for the Poor](#), CGAP (2020) for more details.

# Protecting privacy for OGS consumers by assuming a fiduciary duty

Figure 13 - Legitimate purposes test



SOURCE: Making Data Work for the Poor, CGAP (2020).

OGS companies are becoming more digitalised and data driven – and many are now using business analytics and experimentation to innovate and improve products and services for consumers. Consequently, there is an inherent tension between the concept of legitimate purpose and the notion that ‘you don’t know what you don’t know.’ Processing only data that is currently needed limits exploration of what could be done with more data.

Nonetheless, there are significant developments being made in data analytics and many companies see the potential in mining transactional and repayment data to improve service terms and delivery. For example, one productive use off-grid solar company analyses the extent to which usage is correlated with repayments and layers automated messages to increase usage and provide improved after-sales support; and some

companies are developing algorithms from payment data that improve KYC checks. Companies should always act as a fiduciary of consumer data. To support innovation whilst protecting consumer data, companies should think about and articulate the benefit to the consumer. Companies are also encouraged to ‘de-personalise’ consumer data.

## How one PAYGo company is minimising its consumer data footprint through ‘legitimate-purpose’ testing

Being a data-driven PAYGo company, it is key that only data with a clear business purpose is collected and processed. To ensure data minimisation, the company started by mapping out its business processes and transactions, and identifying how different departments and functions use personal information.

Mapping out the information and making an inventory of data collected at customer interaction points was relatively easy: what do you get from sales, what do you get through customer care or others who interface with the customer. For business operations that do not have a consumer interface (e.g., data analysts), more work was needed around business processes to understand how and why consumer data is used and its connection to potential consumer benefits. For example:

1. Beyond KYC data, what additional data is collected or processed? What data is not used?
2. What data is sensitive and a cause of greater concern?

With the data ecosystem fully mapped, the PAYGo company’s legal department is tasked with demonstrating where data is not used and should be minimized. This approach is used to ensure legitimate interest and convince decision makers not to collect certain data despite the fear of missing out on useful information.

# Protecting privacy for OGS consumers by assuming a fiduciary duty

## De-personalisation of consumer data

There are various ways in which data can be “de-identified”:

- Anonymization<sup>38</sup>
- Pseudonymization<sup>39</sup>
- Aggregation
- Tokenization (“substituting algorithmically generated numbers for a client data element”<sup>40</sup>)

A word of caution: while some data de-personalization/de-identification techniques are irreversible, such as in the case of anonymization, others could allow data to be re-identified, especially with advances in big data, where “reverse data capabilities and machine learning techniques make re-identifying data more practical meaning greater care will be required of providers utilizing such techniques”<sup>41</sup>. De-identification decisions should take these factors into consideration and companies should opt for de-identification techniques that do not put the data at risk of being “re-personalized”.

Technology is rapidly evolving, and promising technologies are currently being tested to allow processing of encrypted data without ever seeing it. It will be interesting to keep an eye on these technologies as the costs go down and they are more in reach<sup>42</sup>.

## Implementing good practice through effective training for staff and agents

Training is an important part of ensuring good practice for consumer protection, and **companies are advised to ensure data privacy practices are included in training for staff and agents.**

OGS companies should ensure that staff and agents are sensitized to the importance of data privacy and that they are clear about their responsibility in acting in the best interest of consumers and their role in protecting consumer data, whether it is handled in paper or digital form.

The Center for Financial Inclusion emphasizes the need to avoid sale of consumer data in its Handbook for Consumer Protection<sup>37</sup>:

*“Sales of client data to third parties are generally not in keeping with good privacy practice without meaningful client consent and an opportunity to opt out – preferably without loss of access to the service for which the data was originally collected. Where providers share client data with other entities for cross-selling purposes, the client should understand clearly that the data is being shared and have the right to opt out of participating in writing or through electronic means. Note that clients do not typically have the right to opt out of sharing information with third parties contracted as part of the service delivery process, such as marketing, data analysis, collections, etc.”*



**A huge, missing piece that is underrated is awareness and training. At the end of the day, it’s people who are collecting data, using it, processing it, disclosing it, breaching, reporting incidences, etc.**

OGS company



<sup>37</sup> See [Handbook on Consumer Protection for Inclusive Finance](#) (2019).

<sup>38</sup> See [GDPR Recital 26](#): Not applicable to anonymized data.

<sup>39</sup> See [GDPR Recital 28](#): Introduction of pseudonymization.

<sup>40</sup> See [Handbook on Consumer Protection for Inclusive Finance](#) (2019).

<sup>41</sup> See [Handbook on Consumer Protection for Inclusive Finance](#) (2019).

<sup>42</sup> An example of an emerging promising but still very expensive encryption technology is “homomorphic encryption” (see [Wikipedia: Homomorphic encryption](#), accessed March 2022). This technology would allow asking encrypted data questions and get answers without getting the data itself.

# Protecting privacy for OGS consumers by assuming a fiduciary duty

## Implementing functionally-focused data privacy training for OGS staff

To ensure that good data privacy practices are followed throughout the business, one leading PAYGo company has implemented general data protection training for all new employees during onboarding, and for all staff during annual refresher training. A learning management system ensures that the training is easily accessible for all staff and enables senior management to ensure it is completed.

Early in 2022, the company undertook a data privacy audit across their Kenyan operations. From the results, they identified a need to improve the training programme, and plan to implement new modules segmented by function (data processors, HR staff, customer care, etc.). The company also plans to appoint data privacy risk registrars within each functional area. These individuals will be tasked to oversee how specific data risks present themselves in the various functional areas, and tailor trainings accordingly.

Finally, the company also plans to appoint a privacy point person for each function. These individuals, part of top management, will be required to consider data privacy from their respective function and put in place appropriate controls to mitigate the risks.

## Strengthening data security protocols to enhance Consumer Protection

Effective data privacy is highly dependent on the security systems and protocols that underpin data processing of any kind, and **OGS companies should ensure that they have robust security policies and practices in place.** Implementing a data register can help companies identify areas of vulnerability and take required steps to mitigate the risk. Simple steps to take include ensuring that all staff have effective anti-virus software installed on their computers, consumer data is password protected and that third party service providers (e.g. PAYGo Software and MNOs) follow robust data-privacy protocols.

Software providers within the OGS ecosystem are encouraged to provide assurance and visibility to distributors and help them to easily evaluate the robustness of data security within the platform<sup>43</sup>. Furthermore, PAYGo companies and others with MNO partnerships should strive to partner with organizations certified by GSMA, as they are held accountable to data privacy standards that are similar to those stipulated in the GOGLA Consumer Protection Code.

Whether operating through paper-based or digital channels, OGS companies should analyse the vulnerabilities of their security processes and aim to strengthen them. The case study below highlights Greenlight Planet's journey to reduce data security vulnerabilities by moving away from paper-based contracts.

<sup>43</sup> Several tools are available and could be used to build on for the OGS sector. See [Venture Lab Data Protection Guide](#) (2019) and [Cybersecurity Resource Centre for Inclusive Finance](#) (accessed March 2022).

# Protecting privacy for OGS consumers by assuming a fiduciary duty

## Greenlight Planet is digitising contracts to reduce data-privacy risks for consumers

Greenlight Planet has a comprehensive suite of data security measures in place throughout their operations. After undertaking their annual Consumer Protection Self-Assessment, and a Third-Party Assessment – the company identified an area of vulnerability when agents use pen/paper methods to collect and process data from consumers.

To reduce the risks linked to handling paper-based contracts and strengthen their data-privacy processes, Greenlight Planet is now in the process of digitising their consumer data collection and contract system. Agents will no longer be carrying unsecured consumer data with them as they visit market areas and customers, and the risk of forgetting or losing hard-copy documents and compromising data is reduced.

## Conclusion

Understanding the spirit behind data privacy approaches is critical given the challenges in implementation. Even the best-intentioned companies can be quickly overwhelmed with the topic and with what is required to put in place a robust data privacy and protection system. Companies that understand the spirit of data protection will be better equipped to inform what needs to be adapted to lead to desired outcomes.

By following the practical examples of good practice outlined in the briefing note, we hope that companies are able to improve data privacy practices. By empowering consumers to exercise their rights and by protecting personal data privacy by default, off-grid solar companies can improve and safeguard consumer outcomes.





# Annexes



# Annex 1 – General Data Protection Regulation (GDPR)

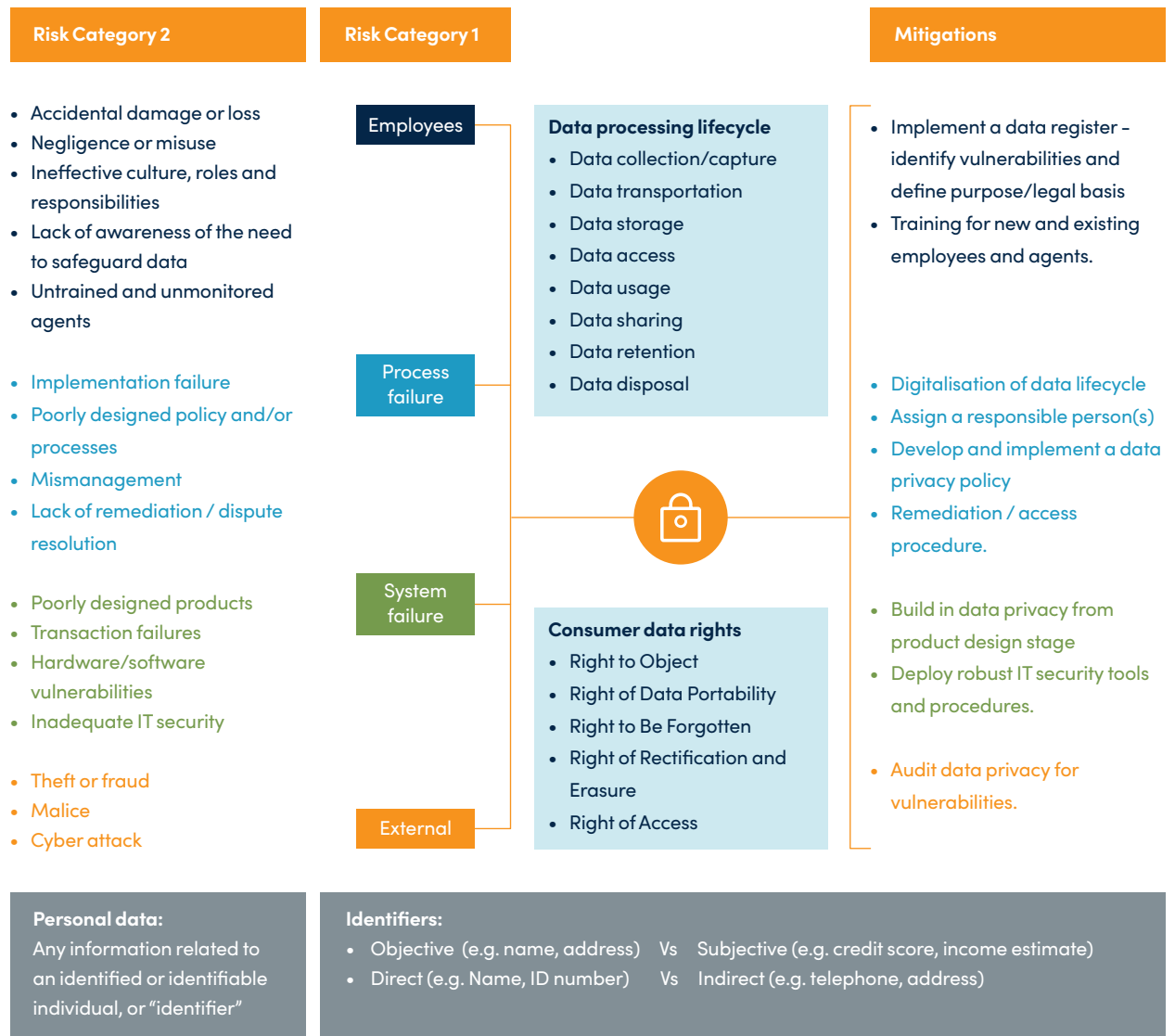
## key principles

### GDPR 7 Key Principles<sup>44</sup>

- 1. Lawful, fair and transparent processing** – this principle emphasizes transparency for all EU data subjects. When the data is collected, it must be clear as to why that data is being collected and how the data will be used. Organizations also must be willing to provide details surrounding the data processing when requested by the data subject. For example, if a data subject asks who the data protection officer is at that organization or what data the organization has about them, that information needs to be available.
- 2. Purpose limitation** – this principle means that organizations need to have a lawful and legitimate purpose for processing the information in the first place. Consider all the organizations that require forms with 20 fields, when all they really need is a name, email, shipping address and maybe a phone number. Simply put, this principle says that organizations shouldn't collect any piece of data that doesn't have a specific purpose, and those who do can be out of compliance.
- 3. Data minimization** – this principle instructs organizations to ensure the data they capture is adequate, relevant and limited. In this day and age, businesses collect and compile every piece of data possible for various reasons, such as understanding customer buying behaviours and patterns or remarketing based on intelligent analytics. Based on this principle, organizations must be sure that they are only storing the minimum amount of data required for their purpose.
- 4. Accurate and up-to-date processing** – this principle requires data controllers to make sure information remains accurate, valid and fit for purpose. To comply with this principle, the organization must have a process and policies in place to address how they will maintain the data they are processing and storing. It may seem like a lot of work, but a conscious effort to maintain accurate customer and employee databases will help prove compliance and hopefully also prove useful to the business.
- 5. Limitation of storage in the form that permits identification** – this principle discourages unnecessary data redundancy and replication. It limits how the data is stored and moved, how long the data is stored, and requires the understanding of how the data subject would be identified if the data records were to be breached. To ensure compliance, organizations must have control over the storage and movement of data. This includes implementing and enforcing data retention policies and not allowing data to be stored in multiple places. For example, organizations should prevent users from saving a copy of a customer list on a local laptop or moving the data to an external device such as a USB. Having multiple, illegitimate copies of the same data in multiple locations is a compliance nightmare.
- 6. Confidential and secure** – this principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security). An organization that is collecting and processing data is now solely responsible for implementing appropriate security measures that are proportionate to risks and rights of individual data subjects. Negligence is no longer an excuse under GDPR, so organizations must spend an adequate amount of resources to protect the data from those who are negligent or malicious. To achieve compliance, organizations should evaluate how well they are enforcing security policies, utilizing dynamic access controls, verifying the identity of those accessing the data and protecting against malware/ransomware.
- 7. Accountability and liability** – this principle ensures that organizations can demonstrate compliance. Organizations must be able to demonstrate to the governing bodies that they have taken the necessary steps comparable to the risk their data subjects face. To ensure compliance, organizations must be sure that every step within the GDPR strategy is auditable and can be compiled as evidence quickly and efficiently. For example, GDPR requires organizations to respond to requests from data subjects regarding what data is available about them. The organization must be able to promptly remove that data, if desired. Organizations not only need to have a process in place to manage the request, but also need to have a full audit trail to prove that they took the proper actions.

<sup>44</sup> See GDPR: Know the Seven Key Principles, Information Security Buzz (2017). The text in Annex 1 is taken verbatim from that article.

# Annex 2 – Personal data risk taxonomy for off-grid solar companies



**Data processing lifecycle**

- Data collection/capture
- Data transportation
- Data storage
- Data access
- Data usage
- Data sharing
- Data retention
- Data disposal

**Consumer data rights**

- Right to Object
- Right of Data Portability
- Right to Be Forgotten
- Right of Rectification and Erasure
- Right of Access





Johan Cruijff Boulevard 91  
1101 DM Amsterdam  
The Netherlands

[info@gogla.org](mailto:info@gogla.org)  
+31 202 400 729



The Voice of the **Off-Grid Solar Energy** Industry