BEUC The European Consumer Organisation

The Consumer Voice in Europe

PRIORITY LIST FOR THE DEVELOPMENT OF NETWORK CODES AND GUIDELINES ON ELECTRICITY FOR THE PERIOD 2020-2023 AND ON GAS FOR 2020

BEUC's contribution to the commission's consultation

Contact: Jaume Loffredo – energy@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2020-038 - 14/05/2020

Why it matters to consumers

The energy sector is becoming more digitalised, as smart meters and other smart devices and connected appliances are entering peoples' homes. The digitalisation of energy can enable companies to provide innovative services but it represents also risks. For instance, with low cybersecurity, hackers could hack smart products to steal consumers' information or to attack the energy system causing blackouts, or consumers' data could be used at their detriment if data protection rules are not implemented and enforced by Member States. Therefore, rules governing electricity markets need to be designed with consumers' interests at their core and additional measures are needed to ensure the electricity grid and devices connected to it are secure.

Summary

The energy sector is undergoing radical changes: it is becoming more digitalised and decentralised, with an increasing number of consumers playing an active role either by producing electricity in their homes or offering flexibility in their electricity consumption to the market. In this context, we welcome that the European Commission is consulting stakeholders on the priority list for the development of network codes. As there is still limited practical experience in the matters that are being regulated, it will be key to ensure that stakeholders are thoroughly consulted not only in the context of the definition of the priority list, but also during the development of the network codes. This will ensure that the best possible regulatory outcomes are achieved and that the new network codes are designed with consumer interests at their core.

In order to ensure a consumer-centric digitalisation of the energy sector, network codes should be designed in line with the following principles:

1. **An effective and protective legal framework for consumers is key when it comes to electricity grid and associated products.** First**,** due to the potential cybersecurity risks for the grid and for consumers arising from energy digitalisation, it is key that the process is accompanied by a sound legal framework which establishes mandatory minimum security requirements for all connected products and associated services. Second, when things go wrong with these products, consumers should have an enforceable right to claim compensation.
2. **Energy markets should be open to new players and services without cutting corners.** It is important to ensure that consumers are empowered and can benefit from demand response, i.e. they are fairly remunerated for their flexibility. At the same time, adequate protections must be in place so that consumers do not experience bill shocks. A clear definition of roles and responsibilities is key so that all market participants, including independent aggregators, can participate in the market on an equal footing.
3. **Rules on data access should ensure that consumers are in control.** Rules on access to data from Distribution System Operators, energy suppliers and aggregators should be designed having consumers' interests at their core. In particular, they should ensure that data protection risks are tackled by ensuring compliance and enforcement of the General Data Protection Regulation.

1. Building an effective and protective legal framework for consumers when it comes to electricity grid and associated products

1.1. Ensuring high cybersecurity requirements

Recent cyberattacks confirmed the need for strong IT security of critical infrastructure such as electricity grids.

The Directive on security of network and information systems ('NIS Directive') obliges Member States to improve the cybersecurity resilience of critical sector operators, including from the energy sector. It is key that the European Commission ensures that the network code on cybersecurity is aligned with the principles and obligations of this Directive.

Furthermore, the experience from other sectors teaches us that the increasing number of connected products may result in increased risks for the electricity system. Hence, rules ensuring the cybersecurity of connected products should urgently be put in place. This will also protect the resilience of the energy system.

In October 2016, a massive attack used hundreds of thousands of insecure consumer devices infected with a specific malware called Mirai to disrupt the internet and brought down websites such as Twitter, Amazon, Spotify and Netflix. A similar attack against the electricity grid would lead to dangerous blackouts.

Therefore, it is key that not only rules on the security of the electricity network are set, but also that the security of appliances is addressed by legislation. The grid is only as secure as its least secure part, and this includes consumers' products that are connected to it.

BEUC recommends that the new network code on cybersecurity:

- **is designed in line with the principles of 'security by design and by default'.** Every connected product, including smart meters, should comply with a set of mandatory minimum cybersecurity requirements. These should ensure that connected products intended for consumers should by default only accept high-level security authentication methods (e.g. for products which use a password, the password must be unique and contain a certain level of complexity and length in accordance to current best practices). These requirements should also ensure that security updates solving vulnerabilities of connected products, including products with high level of energy consumption (e.g. heat pumps, kettles), are swiftly provided to consumers.
- **ensures that consumers are informed and can react to products' vulnerabilities.** Whenever a product has a serious security vulnerability, manufacturers and service providers shall inform their users without undue delay and provide them with the necessary information to enable consumers to mitigate the adverse effects of the vulnerability.

In addition, if cybersecurity attacks on connected products become more frequent, Distribution System Operators (DSOs) may resort to controlled disconnection to address these issues. Rules should ensure the protection of consumer interests.

1.2. Ensuring full compensation for consumers when things go wrong

Currently, the legal uncertainty as regards who is liable for any harm caused by connected products is high. At the EU level, the relevant legislation is the Product Liability Directive of 1985.

However, this Directive is clearly outdated and nowadays shows many shortcomings when it comes to Internet of Things. This is because the EU product liability framework has been designed with traditional business models and traditional products in mind.

Products that the drafters of the Product Liability Directive had in mind in the 1980s are only a far cry of those surrounding consumers today. It is for instance unclear whether the Directive covers defects other than those causing safety issues.[1]

Furthermore, under the Directive, the injured party bears the burden of proof and must establish the damage, the defect and the causal relationship between the damage and the defect. In practice, the burden of proof is the pivotal element upon which rests the right to compensation.

However, new technologies have exacerbated evidentiary difficulties for consumers. Due to their complexity or opacity, it is very difficult (if not impossible) for them to substantiate their claims. This means that their rights cannot be enforced and that they are denied access to justice.

BEUC recommends that the legal framework for electricity markets build on an updated Product Liability Directive adapted to IoT products and giving consumers access to justice when things go wrong with their products.

2. Open the market to new players and services without cutting corners

Although there still is limited experience of demand response in the market, especially among households, we can already observe that existing network codes may constitute some barriers to the participation of all market participants on an equal footing, including independent aggregators. Examples include unclear provisions related to product design, definition of roles and responsibilities and prequalification requirements.

It is important to overcome these barriers because making energy markets more flexible will help to avoid building additional power plants and help Europe achieving its climate targets. This, in turn, should reduce overall system costs including for consumers.

However, to maximise the potential of demand response, EU and national rules should create the right conditions that will incentivise consumers, including households, to provide their flexibility to the electricity system.

Consumers should be adequately remunerated for shifting their loads. For instance, BEUC's German member vzbv made a survey to shed light on consumers' perception on variable tariffs. The study found that two-thirds of consumers want to save money but fear having to pay too much with night and day tariffs. Ease of use and convenience were essential for consumers.[2]

Consumers should maintain control over their energy usage. BEUC member Citizens Advice organised in the UK a series of workshops with consumers to understand their position on new energy services. During the workshop, consumers expressed scepticism towards new energy products and feared loss of control, even when a cost saving could be achieved. Companies offering services for flexible electricity consumption must strike a balance between savings and a level of control consumers are comfortable with to get the consumer on board.[3]

Consumers with a contract arrangement with aggregators should enjoy similar rights as they have with their energy suppliers. They should be able to access information which is clear, truthful, complete and comparable. This will allow them to assess whether they are

[1] BEUC position paper, "Product liability 2.0: EU rules fit for consumers in the digital age", May 2020.
[2] Vzbv, "Variable stromtarife aus verbrauchersicht", 2015 (in German)
[3] Impact, "Future Energy Models", Study prepared for Citizens Advice, May 2019

on the right product at any time, to choose the best deal for them or spot and contest any error in the billing. If consumers realise a contract is not suitable for them, they should be able to terminate it in a short time. Consumers should also have easy access to a contact point for complaints and complaints resolution mechanisms.[4]

Consumers should be protected from bill shocks. Many consumers still have limited experience with dynamic price electricity contracts, which in some cases may result in high financial liability if decisions are sub-optimal. To ensure consumer participation, suppliers should provide safeguards against bill shocks. There is a range of ways suppliers can do this: through information (such as warnings of price hikes), price ceilings, or allowing switching without imposing penalties.[5]

3. Rules on data access should ensure that consumers are in control

New technologies, such as smart meters, can provide more detailed and revealing data than what is currently processed. There are risks related to the increased monitoring and tracking of consumers' activities, behavioural profiling, targeted advertising, the loss of control of the data that is being collected and the increasing risk of data breaches. For example, energy consumption data could be used for purposes completely unrelated to the provision of energy services, such as to determine behaviour that might indicate household income and creditworthiness. It is important that consumers have the right to access and control all the data generated by the smart meter and other smart devices at home and that the provisions in the GDPR are respected.[6] Data management procedures should provide consumers with an overview, as well as control of, who uses the data from their smart devices.

Policies relating to access to data by third parties should be designed with the interest of consumers at their core[7]. It is important that access to data held by DSOs is used to address market failures restricting consumer choice by preventing the development of innovative energy-related services by new entrants. This is why BEUC recommends that when laying down access to data requirements, they are based on 4 pillars: (1) guaranteeing well-functioning competitive energy and energy-related markets, (2) protecting consumers privacy and data protection rights, (3) promoting the public interest by enabling wider access to non-personal data and (4) ensuring consistent regulatory oversight and enforcement if consumer rights are not respected.[8]

Moreover, DSOs will gain more insight into their traditionally 'passive' networks and access to more granular data, to enable for the development of smart energy services. It is worth stressing that any use of network data must be compatible with the DSO's neutral market facilitator role and should not lead to discriminatory access to certain market players. It must be clear what is meant by data needed for different services (including new ones), what is the added value for consumers, how will data be used and with whom will it be shared. To access consumers' personal data (e.g. from smart meters) for network

[4] BEUC, "Electricity aggregators: starting off on the right foot with consumers", 2018
[5] BEUC, "Fit for the consumer? Do's and don'ts of flexible electricity contracts", 2019
[6] For example, consumers greatly benefit from accessing the data from their smart meters when it comes to using comparison websites. With dynamic price offers entering the market, the accuracy of price estimations provided by comparison websites may be limited, as tariffs do not depend only on the amount of energy that consumers use, but also on when it is used. If consumers are able to send comparison websites their own consumption data, this would enable comparison tools to increase the accuracy of their estimates. Consumers must be able to easily access their consumption data in a standardised format or be able to allow third parties of their choice to access that information, while respecting the GDPR.
[7] BEUC position paper, "Access to Consumers' Data in the Digital Economy", https://www.beuc.eu/publications/beuc-x-2019-068_european_data_policy.pdf
[8] For further information, see BEUC, "The Future of Energy Consumers", 2019.

planning, DSOs must demonstrate what they would use the data for and what benefits they can generate from receiving that data. They have to justify why they want a certain granularity of data.

END

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).