LEWIATAN

Warsaw, 2 October 2020

Remarks of the Polish Confederation Lewiatan on the General Product Safety Directive review

The General Product Safety Directive is a generally effective framework ensuring the safety of non-food products to the extent that they are not regulated by more specific sector rules for almost 20 years on the EU internal market. Product safety rules apply to offline and online environments and therefore no additional rules focused on online channels are needed. There are however some current challenges that enable unsafe products getting to consumers, both online and offline. Those existing gaps need to be addressed by reliable evidence-based analysis.

We can indicate some areas requiring special attention:

- while assessing the GPSD in the context of new technologies, we have to take into consideration that separate streams of work are opened in the EU to deal with those challenges;
- product safety challenges linked with online sales should be tackled with experiences from existing voluntary commitments like Memorandum of Understanding on counterfeits goods on the internet and Product Safety Pledge. Those initiatives should be strengthened and further extended.
- engagement and responsibility of the whole value chain essential to tackle product safety problems and guarantee an effective and coherent recall framework. Authorities should have adequate resources, expertise and engagement to provide complete information in notices;
- one of the most important issues linked with the effectiveness of the GPSD is to improve its enforcement provisions, particularly in respect of products imported from outside the EU. Dialogue and better cooperation between competent authorities is essential to strengthen market surveillance.

Product safety challenges linked to new technologies

The EU is leading several discussions on how to regulate new technologies in parallel including the review exercise of the horizontal Product Liability Directive (PLD), as well as sector-specific initiatives such as the revision of the Machinery Directive (MD) and updates to the Radio Equipment Directive (RED).

The consultation document notes the proliferation of connected devices as a possible rationale for updating the GPSD; however, the regulation of these devices is either already taking place or being contemplated through both existing vertical and horizontal legislation. The current consultation follows the relatively recent

adoption of legislation including the Goods Package, and specifically Regulation (EU) 2019/1020 on market surveillance of products and the Cybersecurity Act. Moreover, the contemplated update of the GPSD comes amid ongoing debate around the potential introduction of a dedicated legislative framework for Artificial Intelligence (AI) and the Regulation for Fairness in Platform-to-Business Relations, as well as ongoing consultations, such as for the Digital Services Act.

Each of these forthcoming, ongoing, or recently concluded legislative processes bear significant implications for the manner in which technology firms across a wide spectrum of business models market safe and effective products and services in the EU. These efforts in parallel will help understand what, if any, gaps remain, and how to best resolve any remaining challenges. In addition, such coordination will mitigate potential contradictions and help to prevent the inadvertent development of any technical barriers to Trade.

As a general matter, it is our view that the existing essential requirements of the GPSD, coupled with existing and emerging requirements in other legislation and harmonized standards, provide sufficient assurances regarding the safety of connected and AI- embedded devices on the EU market.

While legal clarity would be useful, including by recognizing existing legislation such as the Goods Package, we recommend such clarification adhere to a technology-neutral approach that provides for reliance on global, industry-driven, voluntary consensus standards, and ensures the GPSD is future-proof, i.e., can keep up with the fast pace of technological innovation.

Extensive legislative efforts have either been completed or are currently underway that seek to address the potential safety concerns of the new technologies cited in the Roadmap/Inception Impact Assessment. For instance, under the auspices of the Cybersecurity Act, we understand that the European Commission and the European Cybersecurity Agency (ENISA) are contemplating the development of a cybersecurity certification scheme for internet of things (IoT) baseline security.

Especially when it comes to cybersecurity considerations, we encourage the Commission to fully think about how any revision to the GPSD would interact with the existing EU body of law, including the Network and Information Services Directive and the EU Cybersecurity Act, as well as the schemes being developed by ENISA under the latter.

Any potential updates to the GPSD should consider the risk level associated with new technologies, with particular consideration to areas of application. Targeted legislation is an effective way to address risks that new technologies might pose, as opposed to a blanket product safety requirement for any product that may include or utilize software.

member of BUSINESSEUROPE

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

- 2 -

Possible revision of the GPSD and other related laws like the PLD or MD should consider the potential risks which result in the novel application of emerging technologies, as different applications may produce different risk levels and therefore require different approaches.

If a need for future action is identified in specific application areas, such action should be addressed in a sector-specific manner, with new regulation or suggested legislation filling clearly identified (and quantified) gaps.

Product safety challenges in online sales

The current consultation follows the 2019 adoption of Regulation (EU) 2019/1020 on market surveillance of products, which amended existing harmonized legislation with a view to improving the quality and consistency of market surveillance activities across the EU.

Requirements introduced in the Goods Package were explicitly geared at guaranteeing "that products placed on the Single Market, including products traded online, comply with [our] high common EU rules, are certified and meet the quality and safety standards."

The Roadmap/Inception Impact Assessment suggests that many e-commerce companies are already taking important steps and voluntary commitments to ensure that products sold on their platforms are safe for consumers. Signatories of the Memorandum of Understanding on counterfeits goods on the internet (voluntary agreement facilitated by the European Commission to prevent offers of counterfeit goods from appearing in online marketplaces) and Product Safety Pledge (voluntary commitment to ensure high level of safety of non-food consumer products sold on their online marketplaces by third party sellers) cooperate on a regular basis with public authorities and law enforcement agencies. They provide them with dedicated contact points, fast tract reporting. Those initiatives should be strengthened and further extended.

Online marketplaces are one of many players in the e-commerce value chain and often look at the product safety from the perspective of an entity that facilitates transaction but is not a party thereof. Therefore, any considerations should take into account the multi-faceted nature of marketplaces and dynamic business models, and should not place overly oppressive, impractical, or technically infeasible requirements on platforms.

Given the updates of the blue guide and the creation of new definitions in the Goods Package, we believe that it is not productive to add further definitions at this stage which would further fragment the definition of economic operator and responsibilities appointed to each actor within that framework. Rather, we propose

member of BUSINESSEUROPE

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

- 3 -

providing additional guidance where there may be ambiguity with "older" definitions that were drafted prior to the emergence of such new technologies.

Recalls

We agree that it is important to have an effective and coherent recall framework. This is in the best interest of European consumers and gives clarity to businesses as they identify and take action on potentially dangerous products.

Given the complexity and fragmentation of national market surveillance authorities (over 500 MSAs across Europe), it is important to have guidance for regulators when issuing both recall notifications and authorities' takedown requests to ensure consistent communication. We would support the definition of mandatory key elements to be included in recall notices. Authorities should have adequate resources, expertise and engagement to provide complete information in notices. It also requires adapting the tools they use to the requirements of the digital economy (Safety Gate/RAPEX functionalities, CPC sweeps methodology).

Ultimately, manufacturers should retain control of any corrective action. Manufacturers prefer to manage issues that occur with their products with the customers' best interest at heart. There should be no general obligation for platforms to inform customers when they become aware of product recalls or sales of illegal goods. First, a number of factors (level of engagement into transaction, GDPR data limitation principle, data storage limits) may impact the amount of information the platform possesses on the transaction and consumers. Second, in some instances a product recall does not always necessarily imply consumer harm. Right-holders should be engaged in providing complete information in notices and enforce their rights against infringers in court proceedings. Interested third party stakeholders are also very important, if made in good faith (ie. not as an attempt to take a business dispute to a platform).

Recall fatigue may also play a factor, and regulations which may potentially increase the number of notifications must be carefully considered. We know that the current system can be seen as less effective offline than online. When buying online, we know that customer take up of recall actions is much higher than when buying offline.

member of BUSINESSEUROPE

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

- 4 -

LEWIATAN

Market surveillance

We need to stress that one of the most important issues linked with the effectiveness of the GPSD is to improve its enforcement provisions, particularly in respect of products imported from outside the EU (including customs authorities reinforcement). Products which are imported from third countries (mainly from Asia) should fulfill the EU safety requirements.

The lack of resourcing and financing of enforcement activity needs to be adressed. We notice the need for investing in better cooperation, data sharing, and collaboration with businesses.

In addition, the current framework is not being implemented effectively – there are over 500 MSAs in Europe with no minimum standard for recall or NTD notices – sometimes the information provided is incomplete or leads to significant delays in businesses being able to take action, putting customers at further risk.

Before making any regulatory changes, we need to fix the current system. We see data as key: we need better quality data that is complete and actionable; better access to data (both for businesses to inform proactive systems and for regulators to understand trends in order to assess where action may be needed); and better sharing of data (to help governments and businesses enforce against rogue actors).

We should also not forget that the key legislation which will solve some of these challenges has not yet entered into force or their effectiveness is impossible to be evaluated due to its relatively short duration – such as the Goods Package, the Platform to Business Regulation, and the Omnibus Directive (revising key consumer legislation). These need to first be implemented, given the time for companies to comply, and then assessed. If, following assessment, gaps are identified; these can then be amended, if needed.

Identifying the current issues with the market surveillance framework and potential solutions to resolve them will require cooperation from all actors in the value chain. Further pursuing joint actions on critical product groups and identified challenges is a key to success.

Yours faithfully,

Maciej Witucki
Prezydent Konfederacji Lewiatan