Bundeskartellamt

open markets | fair competition

- Sector inquiry smart TVs -

Conclusion and recommendations for action

Sector inquiry smart TVs -
Conclusion and recommendations for action
Az. V-22/17
July 2020

Contact
Bundeskartellamt
Decision Division Competition and Consumer Protection
Kaiser-Friedrich-Straße 16
53113 Bonn
poststelle@bundeskartellamt.bund.de
www.bundeskartellamt.de

Contents

F. Conclusion and recommendations for action

The sector inquiry on smart TVs provides more than investigation results and a corresponding legal assessment. It gives important advice on how the situation regarding this sector of the economy and IoT devices in general, which is unsatisfactory from a consumer rights perspective, can be dealt with in the future.

Besides offering convenient benefits for users, smart TV devices can also be used to collect large amounts of data on consumers and their usage behaviour. Providers of smart TVs could use these for advertising purposes, even if they are not yet exploiting their full potential for data collection.

However, the sector inquiry revealed that even smart TV providers' current behaviour violates a number of German consumer law provisions, namely rules on data protection, unfair competition and civil law. In addition, the sector inquiry detected gaps in current consumer protection legislation.

The options currently available to remedy the identified violations are not satisfactory. Consumers find it difficult to enforce their rights and protect themselves due to information overload and rational apathy. Associations enforcing consumer rights have generally proved effective; however, they reach their limits because it is difficult for them to obtain evidence and to achieve a broader impact in some important problematic areas identified by the sector inquiry. So far official consumer law enforcement has either not been effective enough (data protection law) or non-existent (rules on unfair competition, civil law).

In order to increase the impact of consumer protection in the area of smart TVs, the consumer-friendly handling of user data should be established as a competition parameter for sellers of smart TVs. To this end, however, the communication of essential information on the quality of data protection to the consumer would have to be vastly improved. New ways have to be found to mitigate the informational asymmetry that currently exists to the detriment of consumers. One way of achieving this aim would be to include visual forms of consumer information in advertisements, in shops or on the product packaging. Possible solutions would be voluntary commitments or a cooperation between authorities and manufacturers (co-regulation). Providing consumers with meaningful information and effective control over their data could also be promoted by digital technologies like data protection apps and "dashboards".

The current legal framework covers the issue and use of visual means of providing information. The General Data Protection Regulation (GDPR) for example sets out that companies can use certificates or standard icons on a voluntary basis. However, it is very time-consuming to develop the structures intended for this purpose and the process has not been concluded yet.

Building on this report, the Bundeskartellamt thus makes the following recommendations to decision-makers, companies and researchers:

- continue to raise consumers' awareness of the extensive data processing options of smart TVs and IoT devices in general,
- take legislative action to clarify any liability issues arising from the interaction of various players in the IoT sector and embody in law the consumer's right to receive software updates from the manufacturer,
- work towards the complementation of existing transparency requirements by providing meaningful, simple information on data protection that is available prior to the purchase to enable the consumer to accurately retrace the path of the data disclosed,
- provide the consumer with options to effectively monitor, adjust or, as the case may be, terminate the processing of his personal data,
- establish the quality of data protection as a competition parameter through labelling and new technologies and
- conclude the relevant statutory accreditation and certification procedures and encourage smart TV providers to use visual means for providing information.

In detail:

I. The role of smart TVs in data business

Smart TVs can be used for far more purposes than just watching TV. According to the results of the inquiry smart TVs are technically equipped to be integrated into data business to an extent consumers had previously only known from mobile devices. Moreover, some data protection regulations are broad enough to facilitate such use. Device manufacturers, HbbTV providers, operators of TV portals and app stores, app providers and operators of recommender systems collect user data and use them for their own purposes.

The sector inquiry showed that smart TV manufacturers process data to widely varying extents. While some providers already collect a considerable amount of data, others are more hesitant. The latter's devices, however, often feature third-party software which was not part of the investigation and which presumably collects usage data as well. As almost all privacy policies are largely unclear, there is no way to determine which data collected (and, for instance, which storage periods) are covered by the user's consent. Even where users refuse to give their consent it is often impossible to decide which specific user data might be caught by the legal basis of "legitimate interests" which is unilaterally defined by controllers.

Given the technological possibilities and the ample wording of privacy policies smart TVs could process even more data.

As far as technology is concerned, the surveys of device manufacturers, consultations with technical experts and the research carried out by the Bundeskartellamt itself revealed that smart TVs contain the necessary components and software to analyse TV usage behaviour by means of Automatic Content Recognition (ACR).

With regard to legal aspects the analysis of privacy policies undertaken as part of the investigation showed that many of the policies provide for an analysis of users' TV usage behaviour as described above. This is done either based on the user's consent or based on broadly defined processing purposes and/or legitimate interests. Moreover, some of the contracts concluded between smart TV manufacturers and providers of content recommendation engines, operators of TV portals or app stores, which the Bundeskartellamt had formally requested, include the processing of user data for marketing purposes.

This means that the consumer's TV usage behaviour can be monitored in detail. From a technological point of view, it is no problem to collect statistical data for reach measurement and individual data on interactions with programs or apps regarding the actual viewing behaviour. As a result targeted commercials can be displayed either in the TV portal itself or in a split-screen or full screen while the user is watching TV. Users can be redirected to the advertiser's website by clicking on the commercial. By analysing the TV viewing behaviour the combination of commercials displayed can be tailored to the device location or the viewer's interests and missed commercials can be rerun. It is also generally possible to display targeted commercials on different devices belonging to the same user by using unique identifiers, but this form of advertising has been used less frequently so far.

These opportunities for automatic content recognition for targeted advertising on smart TV devices cannot be expected to remain untapped in future. Initial approaches for the practical implementation of these opportunities have already been observed among smart TV manufacturers. Consumers thus need to be aware that not only mobile devices process personal data on a large scale, but that also everyday objects like TV sets are technically and legally equipped to do so.

II. Violations of and gaps in consumer protection law

Although the way in which smart TV providers currently collect data can still be described as moderate given the opportunities they have, the sector inquiry still revealed a number of consumer rights violations and gaps in the existing law governing consumer protection.

1. Data protection law

The following comments primarily refer to the GDPR.

The inquiry showed that smart TV manufacturers themselves primarily process device-related basic data and only to a lesser extent usage data. More sensitive personal data are mostly collected upon activation of additional services (e.g. voice assistants) or (third-party) apps. While the current data processing practice of the smart TV manufacturers may largely be considered as moderate, it is in many cases still likely to be in violation of the requirements of the GDPR even at the current level. In many cases this is particularly due to opaque privacy policies and often inadequate legal bases for data processing. Transparency issues are mostly

due to the “one fits all” approach which forms the basis of most privacy policies. As far as possible, manufacturers want data protection policies to cover all current and future services and devices they provide, even if the consumer does not use most of them. Even in cases where privacy policies make at least a rudimentary distinction based on usage processes and devices used, consumer texts are unintelligible due to generalised and vague wordings, unnecessary information and incoherent text structures. What is more, it is often difficult to exercise one’s consumer rights in an effective manner because the corresponding information provided in the privacy policies is not always correct or because it is difficult to contact the manufacturer.

The inquiry showed that the larger part of data processing activities may be carried out by parties other than the manufacturer that contribute to the functioning of the smart TV set. Examples include in particular operators of TV portals, app providers (e.g. streaming services) and providers of services such as content recommendation engines. However, the extent to which the manufacturer is liable under data protection laws for actions carried out by these parties (which do not belong to the economic sector analysed) is entirely unclear in legal terms. As the consumer in most cases can only get hold of the manufacturer and the retailer, this is a considerable gap in consumer protection.

2. Rules on unfair competition and civil law

Furthermore the inquiry revealed some violations of and gaps in rules on unfair competition and civil law.

The privacy policies of the smart TV provider or the TV portal operator are normally not accessible until the initial device setup. As a consequence, consumers are only informed about the scope and purpose of data processing at a stage where they can normally not revoke their purchase decision. This may possibly constitute a violation of the transparency obligations pursuant to Section 5a (2) of the Act Against Unfair Competition (UWG), especially if certain non-smart basic functions of the TV set are conditional on the disclosure of personal data which is not necessary from a technical point of view.

There are a few cases in which the device manufacturer or a third party displays advertisements for commercial goods on the start page of the TV portal (home screen). Unless explicitly pointed out upon purchase and if this is not to be reasonably expected by the customer due to the overall circumstances, such advertisements violate Section 7 (1) sentence 1 UWG.

Some warranty declarations do not comply with Section 479 (1) sentence 2 no. 1 of the German Civil Code (BGB). As this provision is regarded as regulating market conduct, this also constitutes a violation of Section 3a UWG. In exceptional cases Section 5 (1) no. 7 UWG is violated because the consumer is misled by wrong statements on his warranty rights.

3. Data security

The sometimes very short period of time during which smart TV providers keep their sold devices updated does not in itself constitute a violation of consumer rights. It leads, however, to a significant protection gap. Even if the inquiry did not reveal any obvious indications of smart TV manufacturers currently selling devices that are unsafe from a technological point of view, it shed a critical light on how the devices are updated after being placed on the market for the first time. While most manufacturers provide security updates for 2 to 3 years after placing the devices on the market, this period becomes shorter for customers opting for TV models from the previous year or the year before that. In some exceptional cases the devices are not updated at all, even if security flaws of the device software become publicly apparent. A certain improvement regarding consumer information is to be expected after full entry into force of EU Regulation 2019/2013[1] on 1 March 2021. Article 3 lit. h) of this Regulation stipulates that suppliers of devices with a display size exceeding 100 cm^2 must provide sellers with a product information sheet. Pursuant to Annex VIII no. 4, the seller must ensure that the product information sheet is displayed near the product price when selling the product online. Annex V table 4 of the Regulation stipulates the following mandatory information to be contained in the product information sheet:

	Angaben	Wert und Genauigkeit	Einheit	Anmerkungen
21.	Mindestens garantierte Software- und Firmware-Aktualisierungen (bis):	TT. MM. AAAA	Datum	Gemäß Anhang II Buchstabe E Nummer 1 der Verordnung (E

Figure 1: Extract from Annex V of Regulation No 2019/2013

Based on current legislation, consumers have no sound claim to software security updates, and not just information thereon, being provided by manufacturers of smart TVs during a certain period of time. Neither warranty law, consumer contract law, GDPR, UWG nor product or producer liability provide a basis for such a claim.

Considering the importance of up-to-date device software for data security, this is a serious protection gap with regard to the consumer's data security. Consumers have a strong wish to receive security updates and pertaining information. A survey commissioned by the Verbraucherzentrale (consumer advice centre) of Rhineland-Palatinate showed that approximately 90 % of consumers would like to receive information on the fact that smart phone operating systems are no longer updated and would like to see manufacturers obliged

[1] Commission Delegated Regulation (EU) 2019/2013 of 11 March 2019 supplementing Regulation (EU) 2017/1369 of the European Parliament and of the Council with regard to energy labelling of electronic displays and repealing Commission Delegated Regulation (EU) No 1062/2010.

to provide updates. On average, the respondents advocated a security update period of 5.4 years.[2]

III. Unsatisfactory law enforcement

According to the findings of the sector inquiry law enforcement in areas where current consumer law has no protection gaps, but where concrete violations of applicable consumer law have been identified, is in some parts unsatisfactory.

1. The individual consumer

Individual consumers normally either do not at all exercise their data protection rights regarding information, revocation and other areas or only very rarely,[3] either because of an information overload or rational apathy when it comes to taking legal steps.

An example of this is that smart TV manufacturers have users consent to extensive data processing or simply base that data processing on very broadly defined legitimate interests. They hardly ever risk being punished for such conduct, even if the justifications they state would not stand up to legal review. Consumers face the dilemma that without their acceptance of privacy policies or consenting to certain forms of data processing the TV set they just bought cannot be used at all or not as intended. At the time of disclosure it is also impossible for the consumer to assess the potential future disadvantages resulting from the disclosure of his data. This is even more true as consumers normally cannot clearly see which personal data are collected, where and for how long they are stored and, for example, what data would be covered by a withdrawal of consent. It is true that consumers could exercise their right to information to obtain this information, but it is very time-consuming and may involve the disclosure of further personal data if they have to identify themselves to the smart TV manufacturer. Furthermore they do not necessarily receive the requested information in

---

2 See Verbraucherzentrale Rheinland-Pfalz, Verbraucher wünschen sich fünf Jahre lang Smartphone-Updates, press release by Verbraucherzentrale Rheinland-Pfalz of 21 May 2019, available in German only at https://www.verbraucherzentrale-rlp.de/pressemeldungen/digitale-welt/verbraucher-wuenschen-sich-fuenf-jahre-lang-smartphoneupdates-36517.

3 The German Federal Government registered only 76 cases in which data subjects exercised their rights with regard to all ministerial online presences within roughly 10 months after the GDPR entered into force. As cases were registered according to five different data subject rights it can be assumed that the actual number of individuals filing claims is considerably lower than 76, see *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Müller-Böhm, Thomae, Aggelidis u. a. der Fraktion der FDP*, Parliament Printed Materials 19/8618 of 5 April 2019, p. 6, available in German only at http://dipbt.bundestag.de/doc/btd/19/091/1909168.pdf.

appropriate detail.[4] As there is no monetary damage customers will often refrain from taking legal steps, which are often time-consuming and costly, to enforce their rights, especially as there are practically no decisions by higher courts in this area.

2. Associations enforcing consumer rights

Associations can pursue some of the important problematic issues identified by the sector inquiry without major difficulties, for example regarding errors in warranty statements. However, associations reach their limits when it comes to the complex issues assessed by the sector inquiry.

It can be difficult to provide evidence because it cannot be unambiguously stated which data are transmitted to which specific recipient as data streams are encrypted.[5] Associations have no access to technical certificates or encryption keys to clarify which data are actually processed or which technical possibilities exist to generate such data streams, even if they are not yet used. The Bundeskartellamt found out that even with the help of analysis software basically only the data recipient's IP address, the transmitted data volume and the time of transmission can be revealed. From this it is not possible to draw reliable conclusions regarding violations, not even regarding indications of violations. In contrast to that, an authority would have the necessary powers to clarify such matters. Official requests for information are an appropriate tool to be used in this context; they were also used in the present sector inquiry. Another helpful way to support investigations are independent technical examinations of the relevant devices, as can be carried out, for example, by the Federal Office for Information Security under Section 7a of the Act on the Federal Office for Information Security (BSIG).[6]

Associations are not always able to pursue violations of consumer rights in connection with smart TVs on a sufficiently broad basis. It is true that they can initiate a court review of the data protection policy issued by smart TV manufacturers, but in practice only some individual sample proceedings are realistic. Only some manufacturers (albeit with high sales volumes) publish their data privacy policies online; the majority of manufacturers do not disclose their provisions until the device has been purchased and the setup process has been initiated, which makes private law enforcement considerably more difficult. Authorities like the Bundeskartellamt can send official requests for information to oblige companies to disclose

---

4 See for example the negative example of unsatisfactory information provided by video streaming services, which led to eight complaints by the organisation NOYB: https://noyb.eu/de/netflix-spotify-youtube-acht-strategische-beschwerden-zum-recht-auf-zugang-eingereicht.

5 See Frankfurt Regional Court, judgment of 10 June 2016, case no. 2-3 O 364/15, juris para. 147 ff. – *VZ NRW/Samsung*.

6 Act on the Federal Office of Information Security of 14 August 2009 (Federal Law Gazette (BGBl.) I p. 2821), most recently updated by Art. 13 of the Act of 20 November 2019 (BGBl. I p. 1626) – BSIG.

their privacy policies, general terms and conditions and other relevant texts for consumers either on paper or electronically and to keep this information updated at all times.

3. Consumer law enforcement by authorities

Authorities' enforcement of consumer law concerning the problematic issues described here has either not been effective so far or is not provided for by any applicable law.

In principle, as far as the GDPR requirements are concerned, data protection authorities are in place to enforce the corresponding rights. As far as can be seen, however, there is no sign of any compelling interventions having taken place so far, which may in part be due to the GDPR provisions on competencies. In the event of cross-border data processing[7], as is the case here, the lead supervisory data protection authority is the authority located in the country where the controller is headquartered. However, the headquarters of smart TV suppliers are located all over the EU. As a consequence, it would take a concerted approach by the lead supervisory authorities of the Member States concerned. It may also be the case that in view of the vast amount of GDPR violations the supervisory authorities set other priorities first.

There are no authorities pursuing violations of the rules on unfair competition or civil law. In Germany provisions from these areas of law that are intended to protect consumers are normally enforced by private plaintiffs. The Bundeskartellamt's efforts to obtain at least competencies to complement private enforcement[8] as part of the 10th amendment to the German Act against Restraints of Competition (GWB) have remained unsuccessful.

IV. Smart information for smart TVs

The Bundeskartellamt favours primarily market-related solutions to close consumer protection gaps, overcome the enforcement deficits identified and increase the impact of data protection issues with regard to smart TVs. The consumer's perception is key when it comes to promoting the quality of data protection as a competitive advantage. Consumers should therefore be made more aware of the extensive data processing possibilities of smart TVs and IoT devices. Consumers' subjective perception will ultimately determine the ways in which information is sought and intellectually processed.[9]

---

7 See *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, p. 314 ff. for interpretations of the term "cross-border data processing".

8 See *Bundeskartellamt*, Stellungnahme des Bundeskartellamts zum Referentenentwurf zur 10. GWB-Novelle of 25 February 2020, p. 25, available in German only at https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Stellungnahmen/Referentenentwurf_10_GWB_Novelle.html.

9 See *Matten*, Management ökologischer Unternehmensrisiken, 1998, p. 203.

1. A smart set of instruments for making data protection a competitive factor

All options for communicating information have to be carefully checked for their **fitness** for the purpose. Market-related remedies must first of all take into account the customer's perception and behaviour as described by the *privacy paradox*. Compliance with this requirement has to be monitored regularly.

It is very likely that the volume and especially the inaccuracy and complexity of information provided by the smart TV manufacturers are already overwhelming consumers.[10] Whenever decision-makers in politics and law enforcement deal with data protection rules, they should therefore work towards simplifying the way in which companies communicate information.

When striking new paths in communicating information, regard should be had to a variety of measures proposed by economic research to mitigate information asymmetries for the benefit of consumers.

For example in the medium term it would be a conceivable screening measure to enhance the quality of data protection by letting consumers choose from a differentiated selection of criteria allowing them to express their individual willingness to take risks. However this would only work if consumers were clearly aware of their own objectives and the interaction between risk and price. As many consumers find it difficult to assess their own information needs and the value of their personal data, these conditions are not yet fulfilled. Furthermore it will take more time to develop the relevant instruments.

Signalling measures could be a more suitable way to address consumer rights issues in the short term. A potentially successful way of signalling the quality level of data protection to consumers could be the use of certifications/test seals or icons. Certifications will only add value for users and consumers if the level of data protection they stand for is considered high and the certifying body is trusted. The effective use of icons depends in particular on their being unique symbols that are not established in other contexts and their being sufficiently clear and meaningful without requiring further explanations.

To ensure that supply of and demand for privacy-friendly smart TVs can emerge, market-related measures need not only communicate all relevant information on the combined transaction – the purchase of the product and the ensuing data business – in a way tailored to the target group. Trust in the provider's fairness after conclusion of the contract is also an important factor on which consumers should be informed. For example, providing regular programme updates and making data security updates available is essential to ensure long-term functionality of IoT such as smart TVs. If updates are not provided at all or not provided

---

10 For "information overload" or "information frustration" for finance products, see *Buck-Heeb/Lang* in: BeckOGK, as of 1 March 2020, Section 675 German Civil Code (BGB) para. 237 – 239 with further references from case law and literature.

over a sufficiently long period of time, the scope for using the smart TV device may become very limited after a certain time. If consumers are unaware of such behaviour before concluding the contract and find out about this through experience only afterwards, this will open doors for manufacturers to implement their hidden intentions or hold-ups. As stated above, there is normally no realistic way so far to enforce a claim to software updates against sellers or manufacturers of smart TV devices.

2. Five symbols for selected aspects of data protection

With this report the Bundeskartellamt would like to give an impulse to a consumer-friendly way of communicating information, which can be helpful when it comes to making the quality of data protection a competitive factor. From the above set of instruments the authority has already taken up the icon approach, which – besides data protection certificates – has the potential to be successful in the short term. By way of example, the Bundeskartellamt therefore developed intuitive icons for four data protection properties of smart TVs which the sector inquiry found to be of particular interest to consumers. Consumers should also be able to find online all the information on a device that is relevant in the context of data protection by way of a symbol with QR code and an internet link. Suitable icons could already be used prior to the purchase in order to quickly communicate to the consumer several data protection aspects in relation to the particular device at an early stage. This would permit consumers to include them as a criterion in their buying decision.

Surveys have shown that consumers attach great significance to the geographic location where their personal data are stored and the minimum period during which software security updates will be provided. These surveys have also shown that the current options for consumers to take note, prior to the purchase, of the terms and conditions of use and data protection policies including any potential complementary information on details, for example a list of third-party companies receiving personal user data, need to be improved. Another relevant factor, either prior to the purchase or at the latest when consent is requested, is whether the television viewing behaviour is automatically registered (ACR) and whether biometric data are processed.

Icons for the above-mentioned aspects could look like this:

Figure 2: Examples of icons for five aspects of data protection

V. The legal framework for introducing smart symbols

State intervention to specifically enforce the use of icons and data protection certificates does not seem necessary at this stage. The GDPR offers a legal framework for promoting the voluntary use of data protection certificates and standardised icons. Data protection regulations and the rules on unfair competition contain business transparency obligations for manufacturers of smart TVs, but there is no obligation to achieve such transparency by implementing the specific information instruments mentioned above.

1. Data protection law

Companies are subject to comprehensive transparency obligations under data protection law, which are especially set out in Article 7 (3) sentence 3 GDPR (information on the right to withdraw consent), Articles 13 and 14 GDPR (information to be provided when personal data are collected) and Articles 15 ff. GDPR (rights of data subjects). Pursuant to Article 12 (1) GDPR such information must be provided in a concise, transparent, intelligible and easily accessible form. Visual communication options for the aforementioned and other information are mentioned twice in the GDPR, namely in Articles 42 and 43 (data protection certification) and Article 12 (7) and (8) (standardised icons pursuant to Articles 13 and 14 GDPR). However, none of the two options has been applied in practice so far.

a) Certification pursuant to Article 42 GDPR

Article 42 of the GDPR provides for the introduction of data protection-specific certification procedures, data protection seals and marks at the European level. Certification is voluntary and confirms that a certain way of data processing complies with the GDPR.

Existing certifications can have direct positive effects on the controller.[11] For consumers they can provide valuable guidance when buying a new device or using a service.

b) Standardised icons pursuant to Article 12 (7) GDPR

In Article 12 (7) the GDPR suggests that companies may use standardised icons to comply with their obligation to provide information on data processing in a concise, transparent, intelligible and easily accessible form (at least as far as information within the meaning of Articles 13 and 14 GDPR is concerned) pursuant to Article 12 (1) GDPR. On the one hand this is a great opportunity. A large part of consumers either do not read data protection policies at all or merely skim trough them, so icons could at least in part provide better orientation.[12] On the other hand, such transparency symbols are not universally applicable. There is reason to doubt that all necessary information can be communicated by icons in a meaningful and

---

[11] See Art. 24 (3), Art. 25 (3), Art. 28 (5) and (6), Art. 32 (3), Art. 46 (2) lit. f), Art. 83 (2) lit. j GDPR.

[12] This applies especially to the limited visualisation options of mobile displays, see *Nink* in Spindler/Schuster [Ed.], Recht der elektronischen Medien, 4. ed. 2019, Art. 12 GDPR, para. 27.

intelligible way.[13] Conversely, Article 12 (7) GDPR only mentions icons depicting information mentioned in Articles 13 and 14 GDPR. Accordingly, Article 12 (7) does not cover information that is easy to depict visually and key for consumers under data protection and data security aspects but not directly linked to Articles 13 and 14 GDPR, e.g. minimum update periods.

c) Initial difficulties

The aforementioned instruments for providing visual information are optional for companies. The GDPR provides for certain procedures for this purpose.

The certification regime for data protection is still in its infancy. Especially the accreditation of certification bodies based on criteria approved by the European Data Protection Board (EDPB)[14] has not yet started.[15] Certification bodies wishing to carry out *certification procedures in Germany* have to apply for the approval of the competent data protection supervisory authority; the accreditation itself is awarded by the *Deutsche Akkreditierungsstelle GmbH*, which has been authorised at the federal government level.[16] Pursuant to Article 43 (8) and (9) GDPR the European Commission is empowered to specify the requirements for certification in the form of delegated acts and implementing acts; however, as far as can be seen, this has not happened so far. Pursuant to Article 58 (3), lit. f) GDPR the competent

---

13 See *Specht-Riemenschneider/Bienemann*, Informationsvermittlung durch standardisierte Bildsymbole, in: Specht-Riemenschneider/Werry/Werry [Ed.], Datenrecht in der Digitalisierung, 2019, pp. 324, 338 and 343 with further references.

14 The draft accreditation regulations have to be submitted to the EDPB pursuant to Art. 64 (1) lit. c), 2nd alternative GDPR. The EDPB may then object to the draft and enforce its position if necessary pursuant to Art. 65 (1) lit. c) GDPR, see for example the EDPB's comment on the German accreditation regulations: EDPB, Opinion on the draft decision of the competent supervisory authorities of Germany regarding the approval of the requirements for accreditation of a certification body pursuant to Art. 43.3 (GDPR) of 25 May 2020, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202015_de_requirementscertificationbodies_en.pdf

15 The EDPB issued pertaining guidelines: EDPB, Guidelines 4/2018 on the accreditation of certification bodies under Art. 43 of the General Data Protection Regulation (2016/679) version 3.0 of 4 June 2019, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf. The supervisory authorities can also issue certifications themselves, which particularly follows from Art. 58 (3) lit. f) 2nd alternative GDPR. In this case they have to take precautions to avoid conflicts of interest, see recitals 42 f. of the aforementioned guidelines.

16 See Section 9 of the German Act on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and Directive (EU) 2016/680 (unofficial translation) of 30 June 2017 (BGBl. 2017 I, p. 2097) - EU (DSAnpUG-EU). For details see *Richter*, Zertifizierung unter der GDPR, ZD 2020, 84, 85.

supervisory authority (approved by the European Data Protection Board[17]) approves the specific criteria of certification presented by a certification body. Certifications or data protection seals and marks will therefore probably not be broadly available in the short term. However, the long start-up phase gives reason to hope that the parties will develop ambitious certification criteria not only suggesting but actually ensuring a high level of data protection.

As far as can be seen there are currently no standardised data protection icons established based on delegated acts by the European Commission pursuant to Article 12 (8) GDPR, which smart TV providers, for instance, could use.

It is hardly possible to forecast the extent to which certifications, data protection seals and marks or icons will become established. While it is to be expected that sooner or later corresponding labels designed for IoT devices will be available on the market, their success will largely depend on whether consumers will consider them reliable and meaningful. Also, it will be critical that manufacturers embrace the idea of data protection as a competitive factor.

2. Rules on unfair competition

The rules on unfair competition also force companies to ensure business transparency. In particular it is considered to be "misleading by omission" pursuant to Section 5a (2) sentence 2 UWG if companies either provide material information in an unclear, unintelligible or ambiguous manner or if they provide such information in an untimely manner. The rules on unfair competition do not contain any regulatory approaches regarding visual means to ensure the required level of transparency comparable to data protection law.

However, smart symbols on the sales packaging or in advertisements and in shops could effectively promote the level of transparency which would be desirable from an unfair competition law perspective. The use of such symbols could in particular address the situation that before the device is set up most manufacturers do not reveal to the consumer details on the intended ways of data processing or that, in some exceptional cases, manufacturers do not share details on the extent to which the use of their device and its basic or smart functions is conditional on the disclosure of personal data and the extent to which these data are processed. By providing consumers with at-a-glance information, whether displayed in advertisements, online offers or on the product itself, and regardless of whether such information is material information within the meaning of Section 5a (2) sentence 1 UWG, smart TV manufacturers can take precautionary measures which help avoid violations of the rules on unfair competition.

---

[17] Art. 64 (1) lit. c), 3rd alternative GDPR. The EDPB may also approve criteria itself, see Art. 42 (5) GDPR, for example if a supervisory authority presents certification criteria for data processing procedures affecting several Member States, see *Lepperhoff* in: Gola et al. [Eds.], DSGVO, 2nd ed. 2018, Art. 42 para 24; *Will* in: Ehmann/Selmayr [Eds.], DSGVO, 2nd ed. 2018, Art. 42 para 35 ff.

There is currently no authority enforcing the UWG and, accordingly, no authority to oversee the development and use of industry-wide standardised icons. This is unfortunate because such symbols for smart TVs, once introduced, would not only help consumers but also providers of such devices who adhere to the rules on data protection and thus do not engage in unfair competition. Their competitors are currently able to offer their devices at a lower price as they do not invest in data protection measures or to cross-subsidise their products by commercially exploiting the data unlawfully collected by their products.

3. Implementation and enforcement

Whenever the legislator, courts and authorities deal with transparency issues in the context of privacy policies, they should always demand the following information to be provided for each data item (which has to be specified exactly):

- the use process during which the data item is collected,
- a meaningful description of the processing process for which the data item is intended,
- the unambiguous legal basis (as stated in the GDPR) for processing the data item,
- transfers of the data item within the company and to external recipients and third countries,
- whenever possible, the maximum period for which each data item will be stored.

When implementing individual market-related measures all players involved are to be included. Decision-makers, companies and researchers are responsible for improving the scope for action and for creating the conditions necessary for consumers to make informed decisions.

The providers concerned should have an interest in identifying and preventing as early as possible any economic disadvantages for themselves arising from consumers not trusting them. To-the-point communication of signals is particularly relevant in this context. Self-commitments to data protection could for instance be communicated as market-driven remedies. Smart TV manufacturers could also use visual means of providing information in advertising, during the sales process and on the sales packaging, e.g. data protection certificates and standardised icons. It could be in the interest of smart TV manufacturers to prevent potential violations of the UWG by using smart icons for the issues having the highest relevance for informed consumer decisions. In this vein, some suggestions have already been made.[18]

State intervention to specifically enforce the visual means of providing information does not seem to be required at this stage. If, after a period of observation, it turns out that initiatives by smart TV manufacturers (possibly complementary to potential future requirements by the European Commission) to create truly informative data protection certificates, standardised

---

[18] See examples on *Smart Media – Zahlen, Fakten, News* (tv-plattform.de, undated), available (in German) at https://www.tv-plattform.de/de/service/thema/thema-smart-media.

icons or other smart symbols are not sufficiently ambitious and effective, it may be appropriate for the lawmaker or a designated authority to accompany this process.

VI. Ten recommendations for action

In conclusion, the following ten recommendations can be given to consumers, decision-makers, companies and researchers with regard to the examined economic sector of smart TVs:

(1) Consumers' awareness of the extensive data processing potential of smart TVs should be raised so as to promote a more conscious use of these and other IoT devices. With this report the Bundeskartellamt would like to contribute to more transparency in this area and provide specific advice for improved consumer protection.

(2) Where the sector inquiry has identified liability deficits with regard to the interaction between the different players in the smart TV business the lawmaker should consider taking action.

(3) As consumers currently do not have a reliable claim to software security updates against the device manufacturer, the lawmaker should consider introducing such a claim.

(4) The aim of any privacy policy should be to make the use, storage and, if applicable, transfer of each personal data item transparent for the consumer. Generalisations should be avoided. Supervisory authorities and associations should quickly take up suitable cases, thus creating case-law promoting truly informative privacy policies.

(5) Consumers should have access to privacy policies and all general terms and conditions relevant to the use of a device prior to the purchase. Websites providing access to such information must be free of trackers. In the event of questions related to data protection issues consumers need a trouble-free way to contact the company processing the data without having to unnecessarily disclose personal data.

(6) Consumers must have the possibility to check and adjust their decisions related to data protection any time. There must thus be a simple way for consumers to access all relevant consumer-related texts and to terminate the processing of personal data if they so wish, e.g. by withdrawing consent and/or terminating the use of services triggering data transfers or revoking data-processing permissions, which should be possible for each individual application. Such a function could be implemented in the menu of any IoT device, e.g. in the form of a data protection dashboard.

(7) To avoid information overload for consumers, decision-makers from the areas of politics and law enforcement should, whenever dealing with data protection regulations, work towards the simplified provision of information by companies, e.g. by way of multi-level or layered forms of presenting information.

(8) To establish the quality of data protection as a competitive parameter and thus to enhance the significance of data protection in the smart TVs sector as a whole, new ways of communicating information are needed. Suitable measures include visual means of providing information to be used by companies for advertising and selling their products as well as on the sales packaging. If possible, any such measures should be based on effective self-commitments rather than compulsion by state authorities. New ways of communicating information also include the use of digital technologies for protecting and empowering consumers; existing research projects and developments in this area should (continue to) be funded.

(9) The European Commission and data protection supervisory authorities should promote the existing opportunities for smart TV manufacturers provided for by the GDPR regarding the use of data protection certificates and standardised icons and finalise the corresponding accreditation and certification procedures set out in the GDPR.

(10) Smart TV providers should also take the transparency requirements set forth in the UWG as an incentive to establish smart symbols for communicating the information which based on the sector inquiry has been identified as the most relevant information. Contrary to the area of data protection, there is, however, no authority to accompany this process under current law.