



Bundeskartellamt



open markets | fair competition

Sector inquiry into smart TVs shows gaps in consumer protection

Bundeskartellamt series of papers on "Competition and Consumer Protection in the Digital Economy"

December 2020

9



Sector inquiry into smart TVs shows gaps in consumer protection
Bundeskartellamt series of papers on "Competition and Consumer Protection in the Digital Economy"

December 2020

Contact

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

Contents

A. Introduction.....	4
B. Findings of the Sector Inquiry	5
I. Data collected via smart TVs	5
II. Consumer rights issues	7
1. Non-transparent consumer information in privacy policies	7
2. Lack of legal bases for data processing	10
3. Incomplete consumer information prior to purchase.....	11
4. Failure to provide software updates	12
C. Need for action and possible solutions.....	13
I. Need for action despite (or because of?) privacy paradox.....	14
II. Establishing data protection as a competitive factor.. ..	14
1. Creating more transparency.....	14
2. Enforcing data protection rules.....	16

A. Introduction

In December 2017 the Decision Division for Consumer Protection at the Bundeskartellamt launched a sector inquiry under consumer protection law into the smart TV sector.¹

TV sets are usually categorised as “smart” if they have more than only rudimentary internet functionality. This means that users can e.g. stream videos and use social networks and apps with their smart TVs. At least the latest smart TVs also have a red button on the remote control to access HbbTV² content (*red button* function). Via HbbTV televiewers can access additional programme-related information, such as information on a programme currently showing, matching advertising or a direct link to relevant teleshopping offers. On account of their internet functionality, smart TVs are also part of the Internet of Things (IoT).

In the last few years smart TVs have become standard equipment in German TV households. The smart TV share of total TV sales in Germany is constantly increasing and between January and September 2020 amounted to 88%.³ Since 2012 altogether over 44 million smart TVs have been sold in Germany.⁴

According to the Bundeskartellamt’s investigations, over 5.2 million smart TVs were sold throughout Germany in the year of reference 2017. The market leader was *Samsung* with a market share of approx. 30 to 35%, followed by *Panasonic*, *Sony* and *Vestel*⁵, with market shares between 10 and 15%. *Arçelik*⁶, *LG* and *TP Vision*⁷ each accounted for 5 to 10%. All the other manufacturers together accounted for a market share considerably lower than 5%. Apart from the smart TV manufacturers, other companies also contribute to the functioning of smart TVs; these companies were not covered by the sector inquiry and include HbbTV providers, independent operators of TV portals, app providers and operators of electronic programme guides.

¹ See press release of 13 December 2017, available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/13_12_2017_SU_SmartTV.html?nn=3591568. All internet sources were retrieved on 26 October 2020.

² *Hybrid Broadcast Broadband TV*.

³ *Deutsche TV-Plattform*, Smart-TV sales in Germany increase by 14% (not dated), available at <https://tv-plattform.de/en/smart-tv-absatz-in-deutschland-wachst-um-14-prozent/>.

⁴ *Deutsche TV-Plattform*, Smart-TV sales in Germany Q1-Q3 2020, available at <https://tv-plattform.de/medien-center/infografiken/>.

⁵ Best-known TV brands of *Vestel* in Germany: *Hitachi*, *Telefunken*, *Toshiba*.

⁶ *Arçelik* sells its TVs in Germany under the brand name *Grundig*.

⁷ *TP Vision* sells its TVs under the brand name *Philips*.

The fact that the Bundeskartellamt can conduct sector inquiries not only in the area of competition law but also consumer law is a new development. This was made possible by the entry into force of the 9th amendment to the German Competition Act (GWB) in June 2017.⁸ The Bundeskartellamt can initiate a sector inquiry where it has reasonable grounds to suspect substantial, permanent or repeated infringements of consumer protection law provisions which, due to their nature or scale, harm the interests of a large number of consumers. Prior to the sector inquiry there were increasing reports in the media about possible consumer law infringements in the smart TV sector. Such violations being widespread they have far-reaching effects, which is one of the reasons which motivated the Bundeskartellamt to launch the sector inquiry. A sector inquiry is not targeted against specific companies but is intended to examine a specific sector of the economy for possible infringements of consumer rights.

In its sector inquiry the Bundeskartellamt first surveyed approx. 30 companies. 20 of these companies which were found to have sold significant quantities of their smart TVs in Germany received a second, more detailed questionnaire. The vast majority of the companies were cooperative and willing to provide information. However, the investigations sometimes proved difficult due to language barriers and international corporate structures.

The following statements are based to a large degree on findings gained from the survey of companies. The final report on the sector inquiry was published on 1 July 2020.⁹

B. Findings of the sector inquiry

Firstly findings on data collection via smart TVs are presented (I.) before secondly outlining consumer rights issues based on these findings (II.).

I. Data collected via smart TVs

Whilst some companies practically manufacture their smart TVs exclusively themselves using self-produced components, others purchase their sets already assembled with pre-installed software from other suppliers. All variations are possible within this spectrum. Third parties frequently provide the operating system and/or

⁸ See Section 32e (5) of the German Competition Act (GWB) as published in the Federal Law Gazette of 26 June 2013 (I p. 1750, 3245); most recently amended by Article 1 of the 10th Amendment to the GWB of 25 May 2020 (Federal Law Gazette I p. 1067).

⁹ *Bundeskartellamt*, Sector Inquiry into Smart TVs – Report, July 2020 (in German), available at the Bundeskartellamt’s website: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_SmartTVs_Bericht.html?nn=11563702. A conclusion in English is available at: https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/AktuelleMeldungen/2020/17_07_2020_Sektor_inquiry_smart_TV_s_conclusion.html

TV portal¹⁰. *Google*, for example, is responsible for the entire operating system *Android TV* including the user interface. Companies such as *Foxxum* or *Netrange* offer a web-based TV portal, via which web apps can be accessed. HbbTV providers and sometimes operators of electronic programme guides are further players in the sector. Pre-installed apps on smart TVs, on the other hand, are often not provided by the device manufacturers themselves but by independent app providers. In view of the many players, it is sometimes difficult to define each company's responsibilities and examine the liability requirements. According to the information provided by the TV manufacturers questioned, the latter generally have no knowledge about what data other players collect from users. In cases where e.g. manufacturers and app providers have entered into contracts with one another, these largely stipulate that each party is to be responsible for complying with all relevant legal provisions in their area of activity.

A joint liability of several players would be advantageous for private plaintiffs as well as authorities because the operators of the "smart TV platform" could also be penalised. For one thing, these are often easier to identify than third party providers on this platform. And secondly they are also often well suited to effectively terminate a violation (also by third parties). However, the requirements for joint liability are usually not satisfied. Rarely do the parties jointly decide on the purpose of data processing which would establish joint responsibility within the meaning of the General Data Protection Regulation (GDPR). Liability under tort law cannot usually be established due to the lack of intention to participate required in this case. Under the rules on unfair trading practices, interferer's liability (*Störerhaftung*) would require either knowledge of the wrongdoing or at least the existence of control and monitoring obligations aiming to avoid possible violations of another party's rights. It is quite possible that the requirements for joint responsibility will be lowered in the course of the further development of case law or more extensive duties of care introduced for manufacturers of IoT devices. However, there are currently no concrete signs of such a development.

The analysis of the data-processing activities specified by the manufacturers has shown that in particular device-related data are collected using the pre-installed system-related software (IP address, device ID(s), MAC address, device location, individual device configuration, connected devices, installed apps, etc.); only in individual cases are user data processed for statistical purposes or to further develop the software. Additional services such as e.g. voice assistants and electronic programme guides, on the other hand, transmit a significant amount of usage data, especially those collected via automatic content recognition (ACR).

ACR software is now pre-installed on most smart TVs. This software is intended to identify and compare content (e.g. audio or video signal) reproduced on a device connected to the internet (in this case: smart TV) based on the specific features of the content with a special database for this purpose. Based on the TV viewer's interests, which may also have been identified via other IoT devices in the same WiFi network, tailored advertising can for example be displayed on the user's smart TV.

¹⁰ In this context TV portal means the user interface with the essential apps which is displayed as the default setting after the TV set has been switched on.

Users in Germany can usually refuse to have ACR functions activated on their TV without having to accept a limited scope of service. However, this is problematic because users are generally unaware of this and usually click as quickly as possible through the instructions when setting up their new TV for the first time. The user navigation when setting up the smart TV plays its part in this by making it more difficult to select options where only limited data are shared or by blending such options into the background.

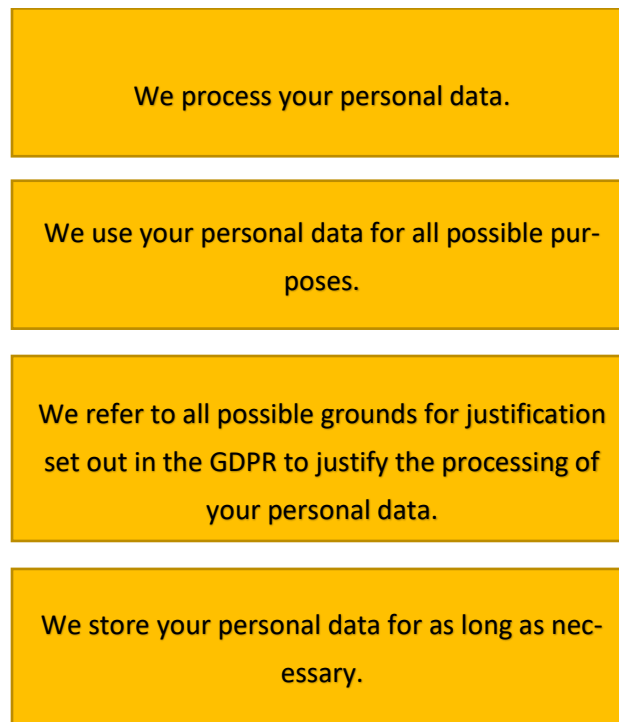
If one looks at the software architecture of smart TVs in the context of potential data protection violations, it can be assumed that for particularly cautious consumers the use of (third-party) apps probably poses the greatest risk. In this connection it was noteworthy that all the smart TV manufacturers stated that they had no knowledge of the data processing involved in the use of certain pre-installed apps.

II. Consumer rights issues

The sector inquiry has exposed various illegal practices which, however, did not always occur at the same time and not in the case of every smart TV manufacturer surveyed. Four of these practices are examined in the following section.

1. Non-transparent consumer information in privacy policies

One of the biggest problems in formulating privacy policies are the different expectations of consumers and companies. Consumers expect intelligible, easily accessible and concise information limited to the data processing activities actually triggered by the use of a specific product or service. From a company's perspective, however, it can seem advantageous to at least formally legitimise not only actual current but also potential future data processing activities. A company can also reduce the costs of implementing and "maintaining" its privacy policies if it uses standardised privacy policies for all current and, ideally, future products and services it offers (one fits all purposes approach). In practice, easy to use all-purpose privacy policies follow the following extremely simplified pattern:



Structure of a “one fits all purposes” privacy policy

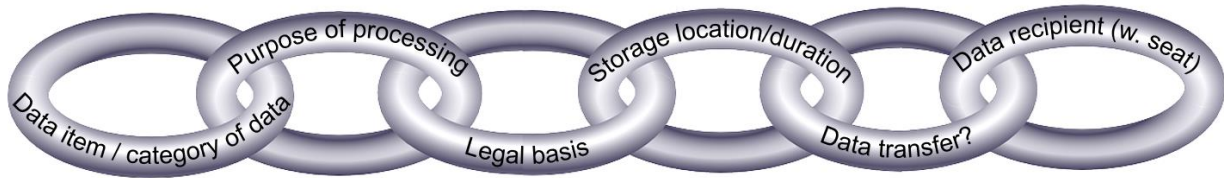
For companies the advantage of this structure is that, at least at face value, it seems to cover all possible current and future case scenarios and thus seems to establish long-term compliance with the GDPR. This sometimes helps to conceal particularly critical data processing activities.

However, at a closer look it becomes clear that such a modus operandi is in clear contradiction to the requirements of the GDPR. In several places the GDPR emphasizes the importance of transparency in all privacy policies. The GDPR not only lays down a whole range of specific information obligations, in particular in Articles 13 and 14. In Article 5 (1) (a) it also stipulates that personal data be processed in a manner transparent to the data subject. Article 12 (1) GDPR determines that the information on data processing referred to in Articles 13 and 14 GDPR be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

In order to meet these transparency requirements, privacy policies must always clarify for each personal data item or clearly outlined, narrowly defined category of personal data, whether¹¹ and how exactly the data will be processed. According to the broad definition in Article 4 (1) GDPR, the term of data processing covers the entire life cycle of a data item from the cradle (collection) to the grave (erasure). As according to Article 5 (1) (a) GDPR transparency includes in particular clarity regarding the processing, it must also be ensured that the

¹¹ Due to wordings including “possibly”, “if applicable”, “depending on the circumstances” it is often not at all clear for the data subject whether data are being collected in the first place.

data subject can also easily identify the individual elements of data processing. In this connection, one can speak of a legitimacy chain¹² which has to be reflected in privacy policies:








pixabay/Clker-Free-Vector-Images, modified

chain of legitimacy for data processing

Based on these considerations, the Bundeskartellamt investigated in its sector inquiry the extent to which the most important transparency obligations of the GDPR are complied with in respect of smart TVs. To this effect it analysed the privacy policies of all TV manufacturers with significant market shares in Germany. The privacy policies of *Google* and *Foxxum* were also analysed. With 'Android TV' *Google* distributes an important operating system which is used, for example, on television sets of the brands *Sony*, *Philips*, *TCL*, *Sharp* or *Xiaomi*. *Foxxum* provides a web-based TV platform which is used on *Medion* and *Vestel* and other smart TVs. The use of these devices is subject to the privacy policies of the above-mentioned companies. At any rate, it is estimated that the altogether 14 privacy policy texts evaluated are likely to apply to over 90 % of the smart TVs currently sold in Germany.

The key results of the analysis can be seen in the following table:

¹² The identifiability of such a legitimacy chain in privacy policies should of course not automatically be equated with lawful data processing.

	Number of companies which have implemented the relevant GDPR information obligations in their privacy policies ¹³ ...				
	 ...excellently.	 ...well.	 ...so-so.	 ...unsatisfactorily.	 ...very unsatisfactorily.
Identifiability of the data collected	1	4	1	7	1
Identifiability of the intended purpose(s) of the data processing activities	2	--	3	3	6
Identifiability of the legal basis/bases for the data processing activities	1	1	2	2	8
Identifiability of the legitimate interests	--	--	4	1	5
Identifiability of data recipients	2	1	2	4	4
Identifiability of data transfers to third countries	--	--	1	--	9
Description of data protection guarantees and possibilities to access information on data transfers to third countries	--	1	3	3	3
Identifiability of storage periods	2	2	1	1	8

Overview of the implementation of key GDPR information obligations

In the Bundeskartellamt's assessment, at least the ratings "unsatisfactorily" and "very unsatisfactorily" are tantamount to violations of the relevant provisions of the GDPR.

Lack of legal bases for data processing

The question as to whether valid legal bases exist for data processing is closely related to the issue of non-transparent privacy policies. Of the legal bases for data processing listed in Art. 6 GDPR, three play an important role in respect of IoT devices such as smart TVs:

¹³ In some cases, not all the aspects examined were applicable (e.g. because the processing was not based on a certain legal basis or data were not transferred to a third country) with the result that not all of the 14 companies were evaluated in each case.

- The consent of the data subject (Art. 6(1) subpara. 1 (a) GDPR),
- The necessity of processing for the performance of a contract (Art. 6(1) subpara. 1 (b) GDPR) and
- The necessity of processing for the purposes of legitimate interests (Art. 6(1) subpara. 1 (f) GDPR).

The companies surveyed used these legal bases to a varying degree. On some occasions, companies' invoked different legal bases with regard to the processing of comparable data (categories).

Where users were asked for their consent, the requests practically always failed to present all the essential details required for informed consent. According to the definition in Art. 4(11) GDPR, the user's informedness is, however, absolutely necessary for any freely given consent. Accordingly, declarations of consent would in most cases be regarded as ineffective.

An inconsistent pattern became apparent where the necessity of data processing for the performance of a contract was given as the reason for data processing. Some suppliers outlined the necessity in a transparent manner, e.g. the necessity to transfer certain device-related data in order to carry out software updates. However, in most cases the problem was that it was not at all clear exactly which data were considered necessary for the performance of a contract and processed. In these cases a justification based on Art. 6(1) subpara. 1 (b) GDPR does not apply because there never really is a general necessity to process for contract purposes the whole set of personal data whose collection is outlined in privacy policies.

Serious doubts also often arose with regard to the legitimate interests which the companies claimed in their privacy policies. The vast majority of the legitimate interests were broadly and abstractly formulated, in some cases in extremely broad and abstract terms. It was also not possible to sufficiently flesh out these broadly defined interests by linking them to clearly defined processing purposes. And again there was the general problem that it was often unclear exactly which data processing was to be justified on the basis of legitimate interests in the first place. It is therefore impossible from the outset to weigh these interests against those of the persons concerned. For instance, in many cases the manufacturers referred to the improvement of their own product or service as a legitimate interest. However, it was unclear what improvement could be achieved and which of the processed data, if any, should be used for this purpose. Moreover, such vague information makes it impossible to appraise whether the intended improvements could not be achieved just as well with anonymised data.

Against this background it can be assumed that in the case of most smart TV manufacturers or TV portal operators, a significant proportion of the data processing is performed without any legal basis and therefore illegally.

2. Incomplete consumer information prior to purchase

Retailers usually offer smart TVs and other IoT devices without instructing the buyer about the general terms and conditions or privacy policies which form the basis for the later relationship between the buyer and TV portal operator governing the use of the product. The full use of the device may, however, be conditional on

the user's consent, which is requested only after the purchase and during the first product set-up. Also, product descriptions of smart TVs usually do not contain information about the operator of the TV portal pre-installed on the device which might be a different company than the manufacturer. Information about the necessity for a user to have a user account to make full use of the smart TV is only provided in some cases. Such information deficits apply to the same degree to online sales as well as brick and mortar shop purchases.

According to Section 5a (2) of the German Act against Unfair Competition (*UWG*), consumers may not be deprived of material information which they need to take an informed purchase decision. As far as can be seen, there is no relevant case-law on the provision of information prior to the purchase of IoT devices. However, the Bundeskartellamt assumes that, for example, consumers expect to be informed in advance if essential functions of the smart TV (such as the provision of firmware updates or the streaming of films on popular platforms) are unavailable if they do not open a user account with the TV manufacturer or the operating system provider. In the Bundeskartellamt's view, it would be desirable if a different TV portal operator than the TV manufacturer or the relevant conditions of use and privacy policies for the subsequent operation of the device were specified prior to the purchase. However, in view of the consumer's expectations when buying a smart TV, this is unlikely to be classified as material information within the meaning of Section 5a (2) of the German Act against Unfair Competition.

3. Failure to provide software updates

The companies surveyed in the sector inquiry specified very different periods during which they provide software security updates for their devices. These ranged from 0 to 60 months. Most companies provide security updates for 2 to 3 years after placing a certain smart TV model range on the market. The average period was 27 months. The buyer must therefore expect to receive security updates only for a relatively short period after the purchase, especially in the case of models from previous years. As no manufacturer mentions specific minimum periods for security updates in product descriptions, consumers cannot take this aspect into account when making their buying decision.

According to the current legal situation, the buyer is only entitled to warranty claims against the seller if a security flaw already existed in the software at the time the risk was transferred¹⁴ and this was known (at least to technical experts). Security flaws which only become apparent after the transfer of risk do not justify

¹⁴ The transfer of risk is the point in time at which the risk relating to the loss of or damage to the article passes to the buyer. In the case of a mail order purchase the risk does not pass to the buyer until the consumer has received the article (Section 475 (2) German Civil Code (*BGB*) as an exception to Section 447 (1) German Civil Code).

any claim to the remedy of such defects, for example through the provision of a software update.¹⁵ In view of the current state of case law, it is also difficult to establish the manufacturer's obligation under unfair competition law and tort law to avert risk by providing software updates.

The Cologne Higher Regional Court recently ruled that no obligation to provide information on the future provision of security updates for a smart phone existed either under the law governing consumer contracts or the rules on unfair competition.¹⁶ It essentially pointed out that the seller could not be expected to procure the relevant information (apparently even with regard to publicly known security flaws of the device software). However, this argument does not apply in respect of a possible information obligation on the part of the manufacturer of the device, on whom the main focus would be under normal circumstances (information obligations of the manufacturer were not the subject matter of the lawsuit before the Cologne Higher Regional Court). It is true that in its judgement the court also stated that the manufacturer did not know when a new security update of the operating system would be published.¹⁷ However, this does not prevent the manufacturer from informing the user within which period new security updates issued by the operating system supplier are definitely to be provided (passed on) for the buyer's device (possibly in an adapted form). Manufacturers can in any case develop their own security patches for their own add-ons and adjustments to the operating system. It therefore does not at all seem implausible to regard the failure to inform potential buyers about minimum periods for security software updates as withholding material information (Section 5a (2) UWG)).

C. Need for action and possible solutions

As already indicated, the legal situation of a consumer using a smart TV is unsatisfactory in many aspects. Firstly, it can be assumed that in many cases personal consumer data are being illegally processed, without the persons concerned being able to effectively defend themselves against such conduct. Secondly, the information available is incomplete from the consumer's perspective. This applies both to important product-based information available prior to the purchase and the subsequent processing of personal data.

¹⁵ Cf. *Raue*, Haftung für unsichere Software, *Neue Juristische Wochenschrift* (NJW) 2017, 1841, 1843; Koblenz Higher Regional Court, ruling of 30 April 2009, file ref. 6 U 268/08. In application of the national provisions which will come into force on 1 January 2022 implementing the Sale of Goods Directive (Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, (amending Regulation (EU) 2017/2394 and Directive 2009/22/EC and repealing Directive 1999/44/EC, published in the Official Journal of the European Union No. L 136 on 22 May 2019, p. 28), the seller has to provide updates for a period of time that the buyer can reasonably expect. However, Article 7(5) of the Sale of Goods Directive provides for an exception as long as the buyer expressly agrees.

¹⁶ Cologne Higher Regional Court, ruling of 30 October 2019, file ref. I-6 U 100/19.

¹⁷ Cologne Higher Regional Court, *loc. cit.* juris para. 73.

I. Need for action despite (or because of?) privacy paradox

On the one hand, it is undisputed and sufficiently empirically proven that consumers place great emphasis on privacy, but at the same time often neglect to protect their personal data in everyday situations. On the other hand, there is a whole range of plausible explanations for this seemingly contradictory behaviour (so-called privacy paradox). For example, the persons concerned are usually unaware of all the relevant information for their decision when disclosing their personal data. One reason for this can be that the information is unavailable, incomprehensible or (e.g. due to the load of information¹⁸) cannot be identified as such. It is also especially difficult to picture the potential distant future risks which might be associated with the disclosure of the personal data. To make things worse, the average consumer is already known to tend to place more emphasis on instant benefit than future disadvantages. A further key factor is that in many cases consumers, whether objectively or at least in their own perception, simply have no easily available alternative. Switching to another product or service may not be an alternative because of network effects, qualitative reasons or simply because the alternatives are not noticeably more privacy-friendly than the offer at hand.

The aim of all possible solutions must therefore be to better inform consumers in spite of their possibly short attention span. In addition efforts must be made to ensure that consumers have recognisable and realistic options to choose from. This can be achieved firstly by improving the transparency of offers and secondly by taking legal action against illegal privacy policies and practices of companies.

II. Establishing data protection as a competitive factor

The sector inquiry has shown that companies do not place high priority on informing consumers in data protection matters in an effective way. Data protection is as of yet not a sufficiently relevant competitive factor for smart TV manufacturers. Several adjustments can be made to change this situation.

1. Creating more transparency

As yet users of IoT devices are hardly able to compare different offers in terms of quality of data protection. Significant and market-changing demand for privacy-friendly products cannot emerge under these conditions.

Firstly, improvements must be made for users of privacy policies in order to increase transparency. For every personal data item processed (which needs to be exactly specified) these should

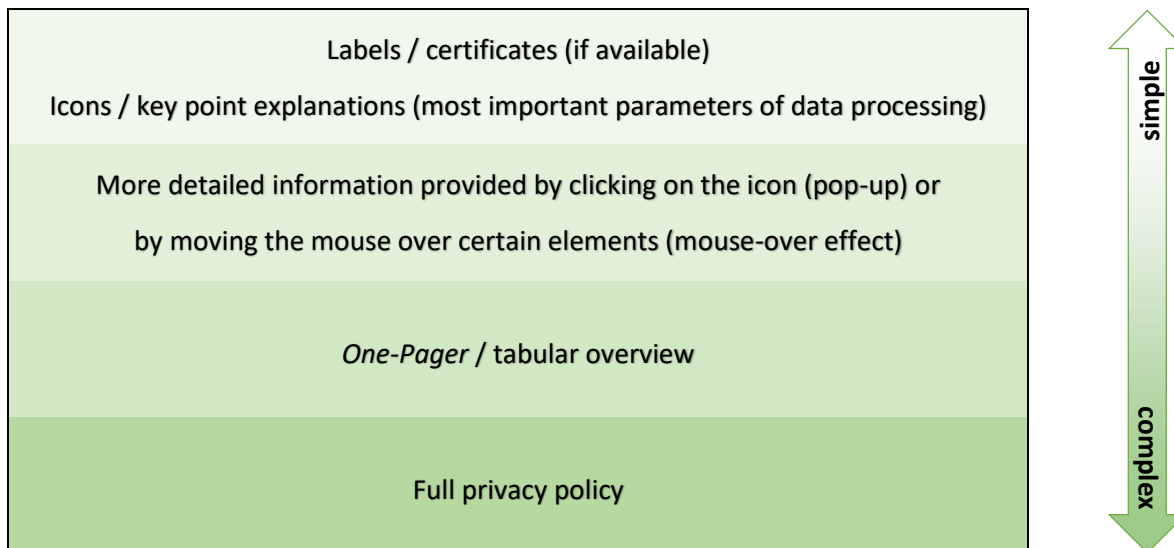
- specify the use process during which the data item is collected,
- provide a meaningful description of the purpose for which the processing is intended,
- indicate the unambiguous legal basis as stated in the GDPR,
- identify transfers of the data item within the company and to external recipients and third countries,

¹⁸ The fact that due to the increasing juridification of many areas of life, consumers are often confronted with complex legal texts such as privacy policies or conditions of use, also plays a role. From a realistic perspective consumers are not remotely capable of even reading through all of these texts, let alone understanding them.

- whenever possible, indicate the maximum period for which each data item will be stored.

To provide an easier overview, this information can also be displayed in tabular form.

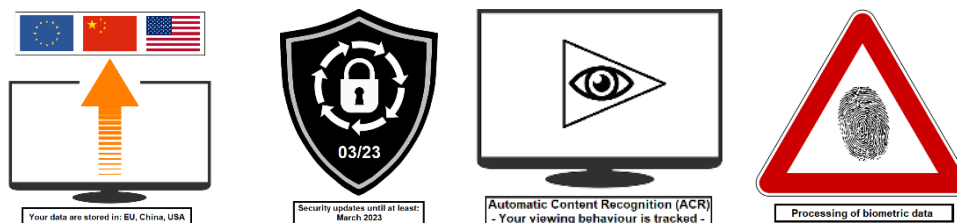
Secondly, privacy policies should not only be described in precise detail. It is just as necessary to make it easier for consumers to understand the essential information. This approach is illustrated using the following table as an example:



Data protection information in layered form

The layers described above can be completely or partially used in combination with one another or divided further depending on the complexity of the data processing to be presented. This should always be based on the guiding principle of optimal comprehensibility and provision of information.

Irrespective of the useful possibilities to introduce data protection certification mechanisms, data protection seals and marks by the data protection authorities as set out in Article 42 GDPR, the Bundeskartellamt proposes the use of several icons, which could improve consumer understanding of data processing:



Examples of icons illustrating four aspects of data protection¹⁹

At least the two left symbols could already be placed on the sales packaging or, in the case of online sales,

¹⁹ Bundeskartellamt's own representation based on public domain images.

appear directly next to the price displayed. The two right symbols could appear as a warning immediately before data are to be processed. It would also be useful to enable the consumer to access all consumer-relevant information before the purchase by clicking on an icon/link or by scanning a QR code:



[Symbol with internet link to all consumer-relevant information²⁰](#)

On the landing page the consumer could access not only the main details of the privacy policy (if possible in a layered form, see above) but also other information such as the current recipients of personal user data, where applicable.

Consumers should also have the possibility to check and adjust their decisions related to data protection at any time during the period of use of an IoT device at a central point (e.g. in the settings menu or a data protection dashboard). There must thus be a simple way for consumers to access 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.

In the medium to long term digital assistants (e.g. apps) can also help consumers to independently analyse data protection rules. First projects in this area have already been implemented.

Increased consumer education in data protection issues would be a useful accompanying measure. Presumably many consumers are often unaware in which situations they disclose which data and how they can better protect their privacy.

2. Enforcing data protection rules

Compliance with data protection provisions currently does not offer manufacturers of smart TVs and probably other IoT devices any economic advantage in competition. It may even be advantageous for them to collect a greater amount of personal user data than their rivals. Moreover, as far as can be seen, violations of data protection rules are currently only punished in very few cases. There is consequently little economic incentive for companies to actually comply with data protection provisions. Vice versa, this means that companies which fully comply with these rules might even have to suffer a competitive disadvantage.

²⁰ Bundeskartellamt's own representation based on public domain images.

Under the GDPR it is generally possible for public authorities to take action against violations of data protection rules. However, the number and scope of such proceedings are currently generally limited. One of the reasons for this could be the need for international coordination, which makes it more difficult to take uniform action against companies with registered offices in different countries. When it comes to violations of rules on unfair competition and civil law, rights are not enforced by public authorities. Private associations would have to become active in this area. At any rate more landmark decisions by public authorities and courts would promote the effectiveness and scope of law enforcement and also simplify the compliance efforts of companies.

In specific areas the legislator could contribute to more legal clarity. For example, it would be helpful to be able to also hold the operator of an “IoT platform”, e.g. of a smart TV, liable in clear cases of violation. Furthermore, from a sustainability point of view, manufacturers of IoT devices should be obliged to ensure security updates for a specific period or at least to state the date until which users can rely on such updates being made available.