JOINT OPERATIONS PURSUANT ARTICLE 62 GDPR CARRIED OUT BY NL, HU, IT, AND LI SAS ON THE SMART TVS STRATEGIC CASE

FINAL REPORT

Nemzeti
Adatvédelmi és
Információszabadság
Hatóság

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

AP | bescherming in een digitale wereld

Table of contents

INTRODUCTION

Following the Vienna Statement on enforcement cooperation issued on 28 April 2022[1], the EDPB selected a case proposed by the Dutch Supervisory Authority (hereinafter also "NL SA") concerning Smart TVs as a Strategic Case. Through internet connected TVs, large volumes of data are exchanged during the ordinary use of the devices. NL SA proposed to start an ex officio investigation into what personal data is being processed during the ordinary use of smart TVs, from the moment of their first installation in a private home, during their use and when receiving and activating software updates. The Hungarian, Italian and Liechtenstein Supervisory Authorities (hereinafter HU SA, IT SA and LI SA) decided to join the Dutch proposal in order to strategically combine their investigation capacity.

[1] https://www.edpb.europa.eu/system/files/2022-04/edpb_statement_20220428_on_enforcement_cooperation_en.pdf

1 THE JOINT OPERATIONS

During the summer of 2022, the NL SA proposed an investigation plan regarding personal data processing through telemetry traffic in internet-connected televisions. The EDPB decided that this case should be one of the strategic cases on 10 October 2022. NL SA has invited other SAs to start work on an investigation in this area. The SAs from Hungary, Italy and Liechtenstein committed to join this investigation.

1.1 Cause of investigation

The EDPB has identified a need for a common investigation into internet connected devices as they are now widespread in all Member States and in many sectors. Almost every European consumer is now using one or more connected devices in their home. Therefore, there is a need for monitoring compliance of devices that are continuously connected to the internet with data protection law. One of the most common household appliances is still the television. Given the numerous additional functions that have been added to televisions over the past years, the EDPB expects that an inquiry into internet connected televisions will remain relevant now, and in the near future. EDPB decided to take on a very practical approach, by simply investigating what data flows occur when installing an internet connected television for the first time and during its ordinary use in a home. The EDPB thus aims to reveal data flows that normally remain covert for the consumer.

1.2 Scope of investigation

The participating SAs investigated three different devices from three different manufacturers. The selection was based on the most popular models of the manufacturers with the largest market shares in the EU and EEA. From a legal perspective, the investigation focussed on the principle of transparency and the principle of data minimisation. This limited scope enabled the four participating authorities to engage in a uniform and manageable operation.

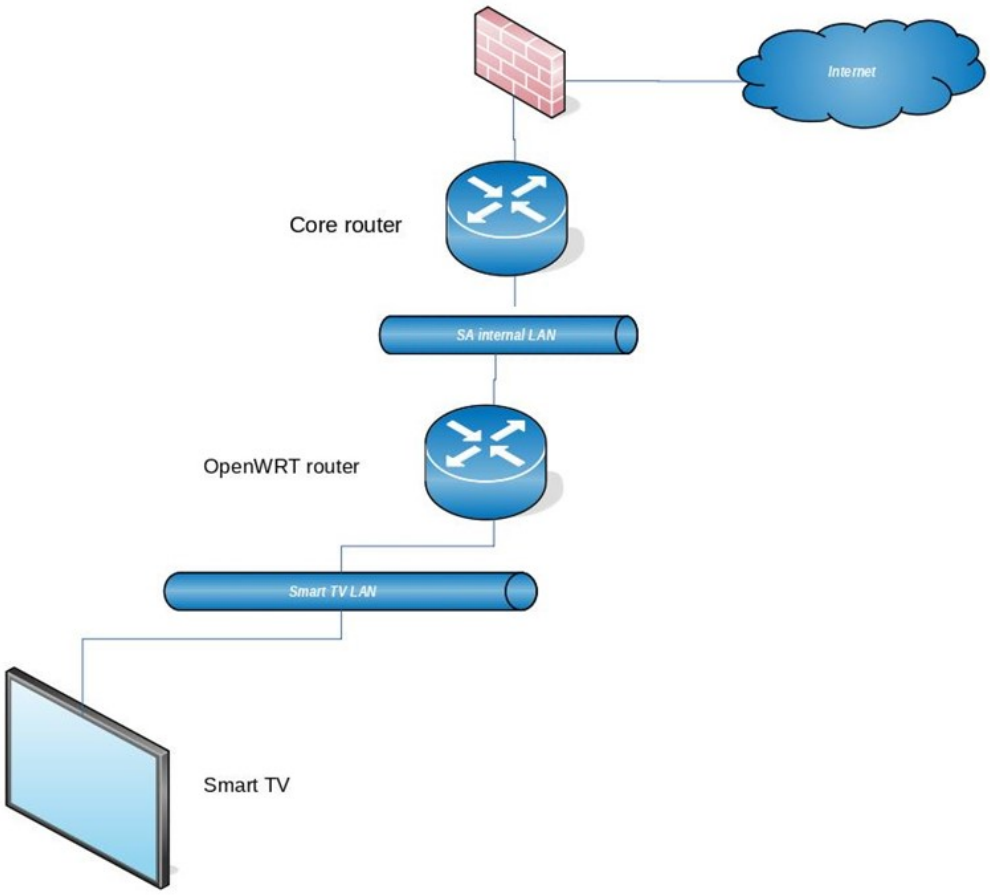
1.3 Methodology of investigation

In August 2023, the four participating SA performed a series of technical inquiries, simultaneously on the same day. The method of investigation was coordinated beforehand and similar for all brands investigated.

The goal was to capture internet traffic between the device and the router. This analysis was tied to four specific moments in time:

- During first installation
- During stand-by / idle time
- During ordinary use the device
- When device is switched off.

After the technical investigation, the SA have shared their results with the device manufacturers and asked them for an explanation of the data flows to the controller(s). Additionally, the SAs have requested further information from the manufacturers.


Internet
Core router
SA internal LAN
OpenWRT router
Smart TV LAN
Smart TV

2 SUMMARY OBSERVATIONS

The SAs might continue their investigations after the joint operation is finalised. Considering that, at the time of finalising this report, some of the investigations are still ongoing the SAs chose to only provide their general observations, without referring to the specific entities which were investigated.

The SAs found that there are a number of observations that occurred with all selected devices.

The first observation is that significant data flows were detected during the technical inspection. In Chapter 3, the findings regarding captured traffic data are presented, deriving from four stages of the investigation: first installation of the Smart TV, idle time, during ordinary use of the device and while switched off.

The second observation is that the ecosystem in which internet connected televisions operate is opaque. As a result of the data flows seen in the investigation, the contractual relationships which have been unveiled and the privacy policies which have been studied, we found that there is an advanced ecosystem of different types of parties, such as the device manufacturer, third party apps developers, operating system provider, advertising networks, viewing data traders, and potentially more. In Chapter 4 we elaborate on the opacity of the Smart TV ecosystem.

In this Chapter, because there are many parties involved, we consider that it is difficult which party should be designated as (joint) controller for the processing of personal data. Identifying the data controller alone is not enough. Besides allocating this legal role, the responsibilities that come with that must be exercised in practise. It became apparent from the joint operation that device manufacturers have the role of data controller, in some situation jointly with others. However**,** device manufacturers contacted seem to regard their role as data controller very limited. It is our impression that they are reluctant to adopt a role as (joint) controller for the whole of data processing activity that is sparked through use of the device they have brought onto the market.

In our investigations we found that data subjects encounter situations where they have no other realistic option than to accept terms, conditions and privacy policies in order to use the device. Considering our previous observations, it is no surprise that data subjects could find it difficult to address the correct data controller with regard to the processing of their personal data.

The final observation is that on all Smart TV's investigated we found pre-installed applications on the device. In some situations, these apps could not be deleted from the TV's. This raises concerns with regard to the principle of data minimisation and the effective exercise of data subjects' rights. In Chapter 5 we elaborate on these concerns.

In Chapter 6 the SAs conclude on their experiences in this joint operation.

3 SIGNIFICANT DATA FLOWS DETECTED

Smart TVs generate many data flows to many different parties (domains). This occurs during first installation of the device, during stand-by and during ordinary use of the device. For all devices even data flows are present while the device is switched "off".

Looking at the type of data that is processed, it contains personal data in terms of the GDPR. This is because the private IP address of the consumer is processed in all cases and because that is processed in combination with numerous other data (e.g. date and time, device ID, account ID, advertising ID, firmware version, country, app start/stop, remote control battery level, power on/off date and time, TV settings, TV serial number). The main purposes of this combined dataset are: (i) to deliver the service to the individual device; (ii) to identify the device and the user during the TV's operation; (iii) to collect information about TV usage; (iv) to deliver personalized information, such as recommendations, advertising to the consumer.[2]

The majority of data flows are encrypted by all manufacturers under investigation. The content of detected data flows is a possible direction for further investigation of SAs, where appropriate. Another direction for further investigation is: whether all data streams detected are in fact necessary for the ordinary use of the TV by a consumer.

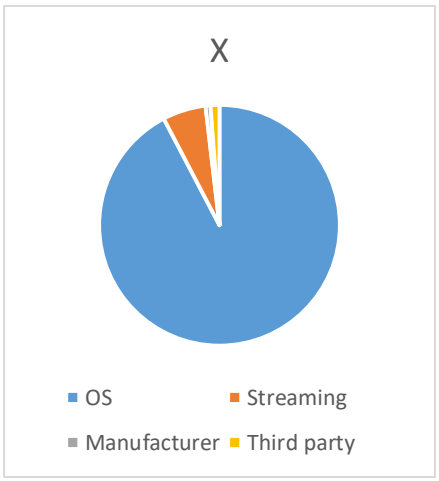
From the dataflows collected during the installation we can categorize four types of parties:

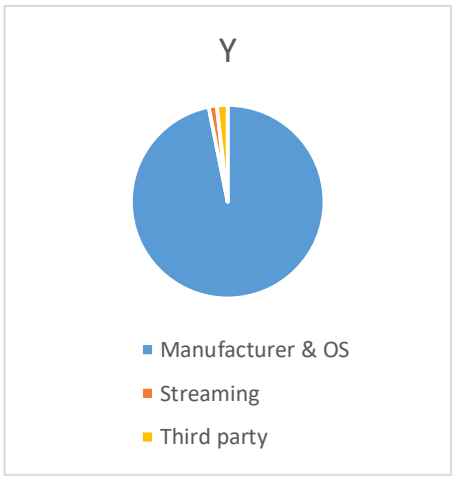
- *Manufacturer:* in some cases the manufacturer of the connected television provides also the Operating System (OS). In these cases data flows are presented as OS data flows.
- *OS provider:* these are data flows to domains connected to the provider of the Operating System (OS) installed on the connected television.
- *Streaming service providers:* these are data flows to third parties who provide streaming services, including but not limited to YouTube, Netflix, Amazon Prime Video or Disney Plus.
- *Third parties:* these are parties which might perform analytics, or deliver other services such as tracking or personalized advertisements, regardless of the data protection role they assumed (e.g. data processor, joint-controller, autonomous controller).

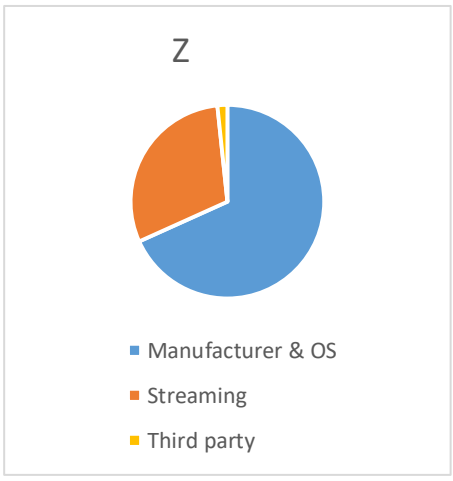
[2] These purposes are derived from the privacy policies of the companies in the ecosystem, the answers received from the manufacturers and the investigation results of the SAs.

3.1 Installation

During the installation almost all of the data flows are OS related. Furthermore, data flows to streaming services, manufacturer and third parties are present.



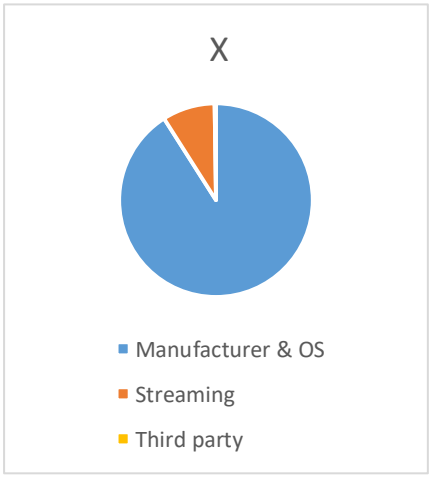


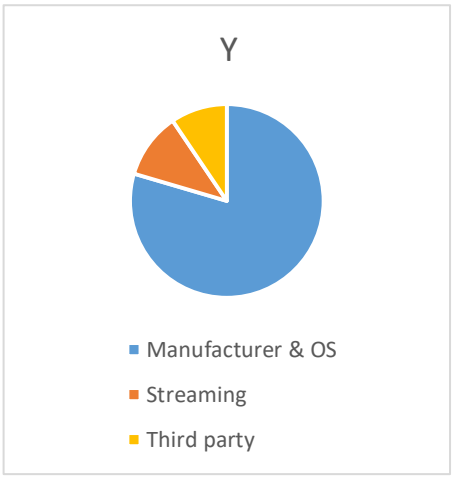


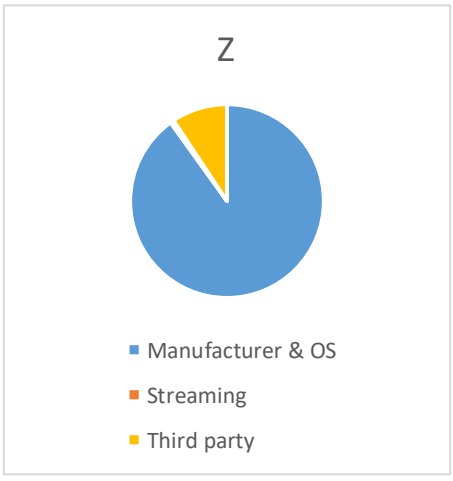
TYPE OF PARTY	SMART TV X	SMART TV Y	SMART TV Z
OS	92,32 %	96,85 %	68,26 %
STREAMING	5,81 %	1,35 %	30,08 %
MANUFACTURER	0,66 %	-	-
THIRD PARTY	1,2 %	1,80 %	1,66 %

3.2 Stand-by

Whilst the connected television is put in stand-by mode, the majority of data flows were registered to the OS provider. The second largest category of data flows are streaming services.



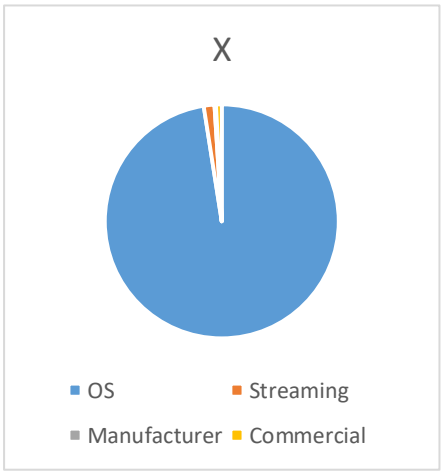


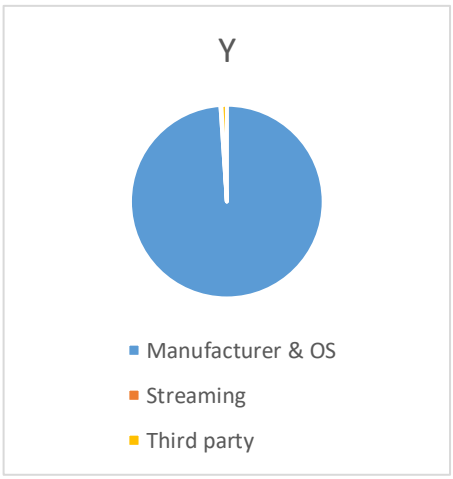


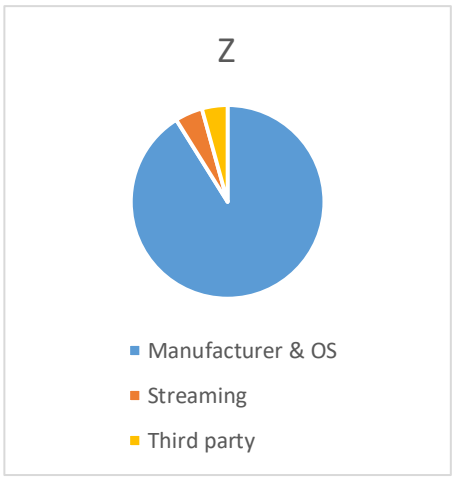
TYPE OF PARTY	SMART TV X	SMART TV Y	SMART TV Z
OS	90,98 %	78,85 %	90,09 %
STREAMING	8,79 %	10,9 %	0,60 %
MANUFACTURER	-	-	-
THIRD PARTY	0,23 %	9,37 %	9,31 %

3.3 Off

In the 24 hours the connected television was turned “off” there were data flows measured to all the four categories of domains. The majority of the data flows that were recorded while the device is turned off, is related to domains concerning the OS provider. Nevertheless, it remains interesting to see that even when the device is turned off connection are still made with streaming services, the manufacturer and other third parties.



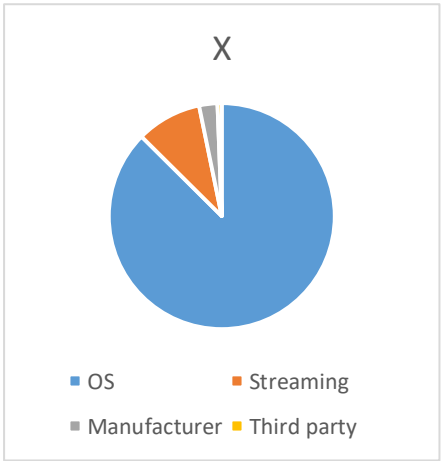


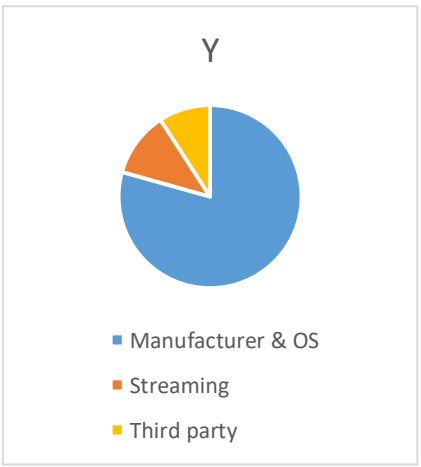


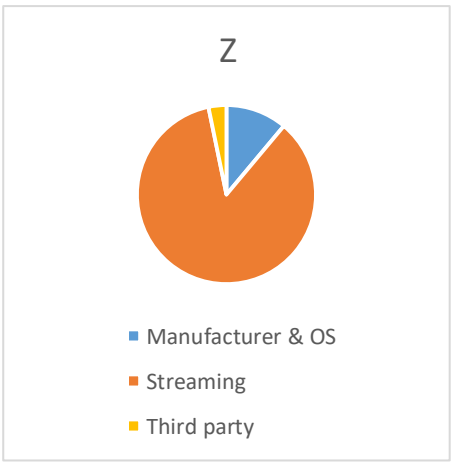
TYPE OF PARTY	SMART TV X	SMART TV Y	SMART TV Z
OS	97,52 %	98,84 %	91,10 %
STREAMING	1,48 %	0,17 %	4,61 %
MANUFACTURER	0,22 %	-	-
THIRD PARTY	0,78 %	0,89 %	4,29 %

3.4 Second stand-by time

After 24 hours the television was turned on again and left in standby. Here again the majority of the data flows are to domains connected to the OS manufacturer, second category are domains belonging to streaming services. But data flows are also to the manufacturer of the connected television and other providers.



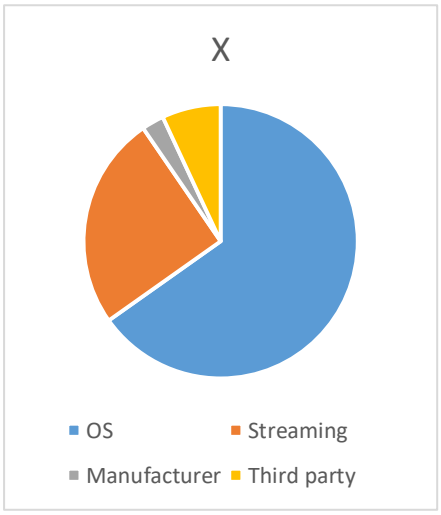


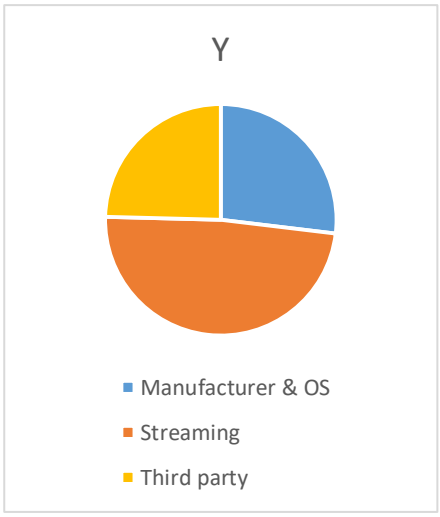


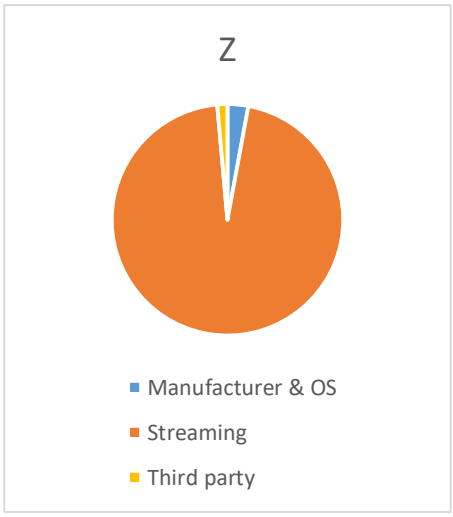
TYPE OF PARTY	SMART TV X	SMART TV Y	SMART TV Z
OS	87,43 %	79,35 %	11,10 %
STREAMING	9,34 %	11,52 %	85,67 %
MANUFACTURER	2,62 %	-	-
THIRD PARTY	0,61 %	9,13 %	3,24 %

3.5 Ordinary usage

During the ordinary use the SAs visited a couple of websites in a browser and watched 4 video's on YouTube. As you would expect the majority of data in this phase falls under the 'streaming category'. Furthermore, during the basic usage phase the 'third party' category of data flows has increased. This is also to be expected when visiting websites in the Smart TV's browser. There are significant differences in the percentages of data flows in the 'third party' category.







TYPE OF PARTY	SMART TV X	SMART TV Y	SMART TV Z
OS	65,20 %	26,90 %	2,90 %
STREAMING	25,24 %	48,51 %	95,69 %
MANUFACTURER	2,62 %	-	-
THIRD PARTY	6,94 %	24,59 %	1,41 %

4. OPACITY OF TELEVISION ECOSYSTEM

4.1 Many parties involved

It can be derived from the data flows, the contractual relationships identified by the SAs and the privacy policies of the device manufacturers that there is an advanced ecosystem of different types of entities. These entities include, but are not limited to, the device manufacturer, operating system provider, third party apps, advertising networks, viewing data traders.

In general, revenue streams have been identified by the SAs. Those reveal that device manufacturers do not only generate income from the sale of devices, but also from contracts with content service providers and the marketing of TV viewing data.

The consumer (data subject) is confronted with many companies or entities when they use their Smart TV. All device manufacturers investigated work together with partners.

Transparency is even more complicated bearing in mind that Smart TVs have usually multiple users (e.g. the whole members of a family) but this issue is not included in the material scope of this joint investigation.

4.2 Legal roles of the device manufacturers

Device manufacturers do not adopt a role as data controller, as mere manufactures, under the GDPR regarding to the data processed by their business partners.

In some cases, the device manufacturers provide also with the Operating System and some services to the users that complement those provided by third party providers. In this scenario, as confirmed by the relevant ToSes and privacy policies, the manufacturers play also a role as data controllers connected to - and limited to - theirs services, but not to the whole ecosystem. Generally speaking, the information provided by the mentioned privacy policies is restricted to the data processing carried out by the device manufactures but the smart TV ecosystem is very broad.

As a result, and given the fragmented ecosystem of smart TVs services, the data subject must read several different privacy policies from numerous parties to understand what will happen with their personal data before getting started with using the device.

4.3 Device manufacturer as data controller jointly with partners

When a device manufacturer enters into an agreement with a partner there could be a joint participation in the determination of the purposes and means, by way of a converging decision, of the data processing originating from such an agreement. The decision from the device manufacturer, either when acting as Operating System provider or just as device manufacturer, to enter into an agreement with third parties providing pre-installed apps determines a data processing by the latter. Meaning without that decision the processing would not occur.

4.4 Other findings regarding (the adoption of) controller role

As already said, device manufacturers declare themselves data controller with reference to a part of the processing of users' smart TVs personal data, but indicate third party business partners who provide additional services on the TVs as independent data controllers.

From the documentations acquired from the device manufactures under joint investigation it emerges that contractual relationships have been formally set out through binding agreements concerning the services provided that refer explicitly also to data processing obligations, with specific regard to roles

of the parties, security measures and information to be provided to users according to the legal basis the third-party relies on.

In few cases, third-party providers act as data processor. In these cases the relationship between the device manufacturer and the third-party providers is governed by data processing agreements, formally complainant with Article 28 GDPR. In general terms, third parties engaged as data processors provide for supporting services (as complementary software) or advertising services.

4.5 Data subject position in the market

Across brands, data subjects encounter situations where they have no other realistic option than to accept extensive privacy policies, in order to use the device. For example: a user account may be mandatory to use the internet-functions of a TV, or even the operating system of a device. Therewith, all privacy policies of the account provider in question are applied.

In the same vain, SAs raise concern over the legality of working with mandatory accounts in the context of the internet-connected televisions investigated.

A picture of revenue streams reveals that device manufacturers not only generate income from the sale of devices, but also from contracts with content service providers and the marketing of TV viewing data. The data subject is therefore not only a consumer of the device manufacturer, but also a source of income with regard to the data they generate.

4.6 Conclusions

Considering the above the SAs conclude that the smart TV ecosystem is rather complex. For data subjects it is difficult to identify where their personal data, originating from their smart TV, is going, considering the multitude of parties involved and their different roles. The position of device manufacturers regarding their responsibilities as not-the-data controller, when they are not the provider of the OS and when they conclude binding agreements with third party apps, limits the capabilities of SAs in their investigations. In investigating those data flows the device manufacturer's points to other entities to answer questions of the SA. This makes the whole process opaque for both data subjects and SAs.

5. PRE-INSTALLED APPLICATIONS

On all smart TV's investigated, the SAs found that devices come with pre-installed applications. This means that certain applications are already installed on the device before or during the first installation by the consumer at home. These apps process data through the smart TV, even when a user does not request or use the app. This occurs regardless of whether a user has an account with the service provider offering the built-in apps. The placement of pre-installed apps is done on the basis of contracts between device manufacturer and content service providers.

Manufactures investigated stated that they pre-install most popular applications for competition reasons in the smart TVs market, for consumers convenience.

The SAs found that these apps, in some cases, cannot be deleted from the devices.

In the joint investigation it has occurred that the installation of third-party apps has been found to be done automatically without users being informed which app will be installed and without being able to choose which app to install. This raises questions with regard to the data minimisation principle.

6. JOINT OPERATION CONCLUSIONS

A summary of observations has been provided in Chapter 2. In this Chapter the SAs provide their findings with regard to the cooperation in the joint operation.

At the beginning of the joint operation the SAs set out to investigate what data flows occur when installing and using a smart TV for the first time. Beforehand the SAs did not know what data flows would precisely be discovered.

In the preparatory phase the SAs found it to be very beneficial to cooperate with each other in determining how to conduct such a technical investigation. By following the same investigative steps the SAs could identify differences between the different device manufacturers. If the SAs would have conducted such an investigation in solitude they would not have known that such differences exist. Also in preparing request for information and in generally discussing the replies received the SAs benefitted from the joint operation. By, on a general level, discussing the challenges they encountered they gained a broader view of the smart TV ecosystem, in comparison to the situation where each SA would have investigated on its own.

Near the end of the joint operation the SAs found that, as the data flows and answers of the investigated device manufacturers differed, the next step of the investigation did no longer benefit from a joint operation. Therefore the SAs decided to conclude the joint operation and investigate the issues, specific to their respective device manufacturer on its own.

It should be noted that all investigated data controllers are located outside of the EEA and therefore fall outside of the one-stop-shop cooperation of Article 60 GDPR.