Information Law and Policy Lab

TRACKED MORE THAN YOU KNOW

How smartphone SDKs form a major privacy breach

Report for *noyb* – European Center for Digital Rights

Glushko & Samuelson Information Law and Policy Lab

Maxime Bax, Francien Giebels & Sasun Sepoyan

Final version – August, 2021

TABLE OF CONTENTS

ABSTRACT

Software Development Kits (SDKs) are widely used in smartphone applications. However, they are often not built by the app creator itself, but by a third party. These parties collect personal data through their SDK once it is implemented in an app and use and sell it for profit, often unbeknownst to even the app developer. These practices endanger the privacy of the end user and violate their fundamental rights as enshrined in the General Data Protection Regulation (GDPR). Despite this risk, the precise legal implications of the problem are relatively unexplored. This report aims to give an introductory description of how SDKs are used and in what ways they are at odds with European privacy legislation. Contributing to the body of knowledge about SDKs, this report is specifically designed to be useful when drafting a complaint directed at national data protection authorities.

Our research suggests that SDKs do not adhere to key provisions in both the e-Privacy Directive and the GDPR. The practices of both the SDK developer and the app creator make it impossible for the end user to give their consent in a legally valid manner. The result: neither party has a sound legal base upon which they can rely to process personal data, that is - additionally - often special in nature. Furthermore, most apps and SDKs lack any proper form of transparency, purpose limitation and data minimisation. Moreover, many apps and SDKs base the transfer of personal data to countries outside the EU on decommissioned mechanisms. In short: these gross violations result in unlawful processing.

LIST OF ABBREVIATIONS

API	Application Programming Interface
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
EC	European Commission
EDPB	European Data Protection Board
ePD	e-Privacy Directive
EU	European Union
EU Charter	Charter of Fundamental Rights of the European Union
GDPR	General Data Protection Regulation
IMEI	International Mobile Equipment Identity
SDK	Software Development Kit

1. INTRODUCTION

This report aims to contribute to the understanding of the legal issues that arise from the use of Software Development Kits (SDKs) in apps. Whereas much attention is given to the practice of using cookies, mobile apps and their usage of SDKs has gotten less attention. This report lays out what SKDs are and how they are violating European law, most notably the General Data Protection Regulation (hereinafter: "**GDPR**") and the ePrivacy Directive 2002/58/EC (hereinafter: "**ePD**"). This report is conducted by students of the Information Law Policy Lab (ILP Lab) of the Institute for Information law (IViR) at the University of Amsterdam (UvA) to support the work of NGO None of Your Business (*noyb*) and paving the way to explore the possibility to file complaints against illegal practices identified.

1.1. Statement of purpose

What is happening?

An SDK is a package of tools that helps an app function. App creators can use the, often freely available, SDKs from third parties for certain functionalities that they otherwise would have to build from scratch. There is a wide variety of kinds of SDKS. For example, you would need an Android SDK toolkit to build an Android app, but other SDKs are used to gain insight in the usage of your app through analytics (e.g. Firebase Analytics, Facebook Analytics). Because SDKs are easy to use and mostly free, they offer app creators a convenient solution to build their apps rapidly and cheaply. This means that in practice SDKs are prevalent in almost all apps. Research on over 950.000 apps of the UK and US Google Play store found that the average number of SDKs within an app was 10 and that 90.4% included at least one, and 17.9% more than twenty.[1] This widespread use of SDKs and relative lack of attention that is given to the practice, makes looking into the legality of SDKs relevant.

SDKs are often built not only to offer some form of functionality, but also to generate income for the SDK developer through the sale of personal data collected via the SDK. As a result, the widespread use of third-party advertising and analytics SDKs in apps comes at a cost to end users. In addition to the code in the SDK that implements certain functionalities, for example automated translation, other code is then purposely incorporated in the same SDK to track users and send this data to the SDK developer. This means that the SDK developer receives

[1] Binns, et al., "Third party tracking in the mobile ecosystem", *Proceedings of the 10th ACM Conference on Web Science* 2018.

user data, often unbeknownst to the user, and that data can be further sent to third parties, like advertising companies, ad brokers, aggregators and possibly even national intelligence agencies in exchange for a fee.[2] Apart from being sold directly to other parties, the SDK developers themselves can process the data for their own purposes, leaving the users in the dark about what exactly happens to their data.

Why is it a problem?

Smartphones have access to a great deal of sensitive sensors (e.g. camera, microphone and GPS), private data from users (e.g. user email and contact lists), and other identifiers (e.g. IMEI). Apps often use permission to access this data, and additionally collect data through the app itself. Given this vast amount of (sensitive) data, it is crucial to protect this information.

These SDKs turn apps into spies that collect personal data, the magnitude of which remains unknown to the subjects. This is obviously at odds with privacy and data protection laws. Users are often unaware that their data is collected, for which purposes it is used, and to whom the data is transferred. This is especially problematic considering the sensitivity of the data to which SDKs have access. Some of the data being collected might even be considered special data in the sense of the GDPR.

Why is it illegitimate?

The use of SDKs in an app in itself can be legitimate. However, there is strict legislation when it comes to the processing and collecting of personal data. When SDKs are used without complying with the legislation. We will focus on privacy legislation in the European Union (hereinafter: "**EU**"): the GDPR and the ePD, read in light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter: "**EU Charter**"). We will conclude that SDK developers that create tools which illegally track users and exfiltrate personal data, as well as app creators using those SDKs, violate several provisions of the GDPD and ePD.

1.2. Introduction to legal issues

In the EU, the use of SDKs must comply with the GDPR and ePD. The GDPR is applicable from the moment personal data is being processed. The ePD applies to the reading and writing of information stored on devices, such as a mobile phone.

[2] See for example: Middle East Eye and Vice.

Many SDKs will involve processing activities that trigger the material scope of the GDPR and the ePD. It triggers the GDPR because much of the data exfiltrated by an SDK is personal data. And it triggers the ePD because information is read from a device in line with Article 5(3) ePD.[3]

A number of provisions of the ePD particularise the provisions of the GDPR. Under the *lex specialis* principle, special provisions prevail over general rules. Thus, in situations where the ePD particularized the rules of the GDPR, the provisions of the ePD shall take precedence.[4]

This is particularly important in the case of SDKs when personal information is stored on the mobile phone, as article 5(3) ePD provides that, as a rule, prior consent is required for the storing of information or to gain access to information already stored. Specifically, that means that article 5(3) ePD will take precedence over article 6 GDPR which means that there are less legal grounds to choose from when processing the personal information.

The next section will explain why the ePD is applicable to both the app creator and the SDK developer. In the subsequent section, the violations of the GDPR will be analyzed in more depth. Because the requirement of "consent" within the ePD is derived from the interpretation of the GDPR, the analysis of the concept of consent will take place within the GDPR section.

In the extensive analysis of the GDPR that follows this section, we will show how even within the broader framework of the GDPR, the use of SDKs still involves violations. This means that both legislative acts can be violated by the use of SDKs in mobile apps.

1.3. Scope and structure of the report

This report provides a first insight into the practices of SDK developers and app creators, and the ways in which they violate key provisions of the GDPR and the ePD. In order to understand how SDKs are being used to track users and obtain personal data, chapter two will elaborate

[3] The Article 29 Working Party stated that "If as a result of placing and retrieving information through the cookie or similar device, the information collected can be considered personal data then, in addition to Article 5(3), Directive 95/46/EC will also apply." The use of SDKs within apps can be considered to be a similar device, retrieving information. See WP171, Opinion 2/2010 on online behavioral advertising, p. 9. See also WP148, Opinion 1/2008 on data protection issues related to search engines, section 4.1.3, p. 12-139.

[4] EDPB, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.

on SDKs, which parties are involved, which types of data are collected, how this data is processed and which legal issues are connected to the use of illegal SDKs.

Subsequently, chapter three and four will look at SDKs in light of the European data protection and privacy law and identify how SDKs can violate the law. Chapter three will outline the applicability to the ePD, whilst chapter four will analyze the GDPR and violations that can occur on multiple articles and legal principles. Chapter five will contain our conclusion.

2. PERSONAL DATA EXFILTRATED FROM DEVICES WITH SOFTWARE DEVELOPMENT KITS (SDKS)

Widely used and still unknown to the broader public, SDKs are an effective tool to track smartphone users. They pose a great risk to the privacy of smartphone users. The following chapter of this report will illustrate how SDKs are being used by (big) tech companies and how personal data is being processed in violation with existing privacy laws like the ePD Directive and the GDPR.

2.1. SDKs are modules developed by third parties which app developers can use to build apps

SDKs bring together different sets of tools in one easily installable package which can be used to create mobile applications for specific platforms, like Google's Android and Apple's iOS. In general, SDKs simplify and accelerate the process of building and adding functionalities to apps, which can be very difficult and time consuming to build from scratch. Commonly, SDKs are used for advanced and hard to build functionalities like showing advertisements and offering push notifications. An example is Firebase, an SDK and an analytic tool developed by Google. The Firebase SDK, which can be built into apps, offers a convenient and accessible way to provide insight into the use of an app for the developers.

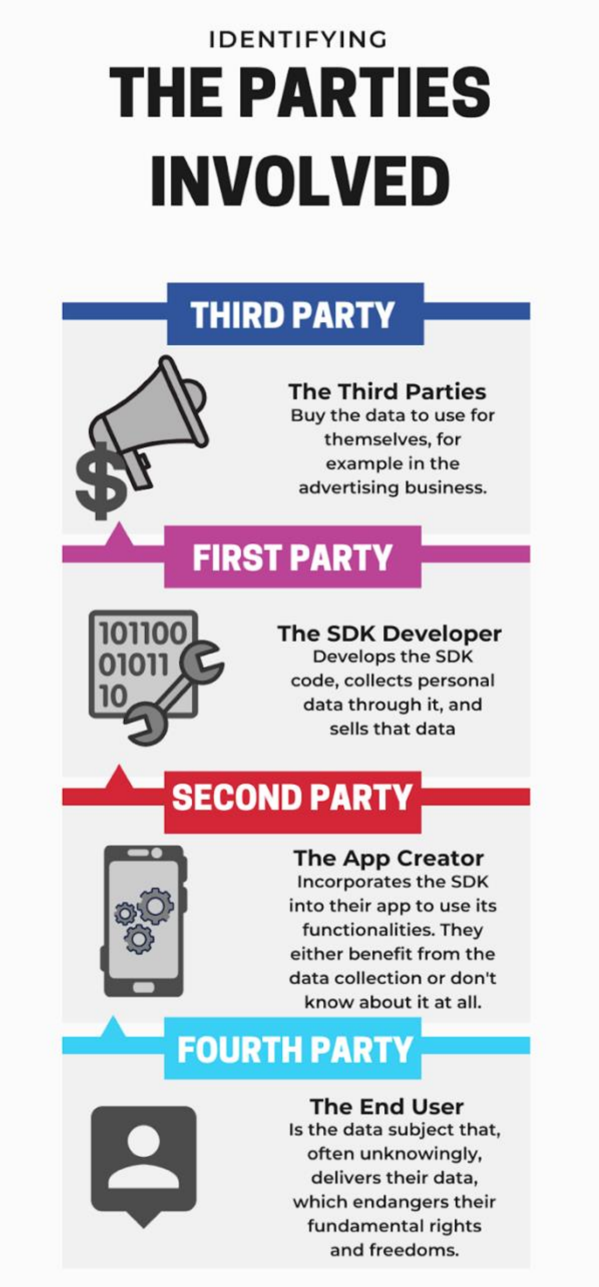
The developer of the SDK creates the various functionalities through codes that are combined and embedded into the specific SDK. Research has shown that of the codes which can be found in apps, around ninety percent consist of so-called open source or third-party tracking codes, which are usually offered in the form of an SDK.[5]

2.2. Identifying parties involved

There are four parties involved in the development and use of SDKs. Parties one through three are capable of violating legal rights and rules. The fourth party is the **end user** and the victim of these violations. The first party is the **SDK developer**. This is the party that writes the code, including a possibility to extract personal data from phones. The OS SDKs of Apple and

[5] Binns, et al., "Third party tracking in the mobile ecosystem", *Proceedings of the 10th ACM Conference on Web Science* 2018.

Android are necessary for an app to function on the respective platforms. These SDKs in itself already regulate the access to the tools of the phone, like connecting to the camera, enabling push notifications, and accessing your location. Additionally, most apps contain a variety of other SDKs, that are created by the developers of that particular SDK. The second party is the **app creator**, who incorporates the SDK into their own code to access convenient functionalities. This party then uses that app to offer their services to the fourth party. It is possible that the creator is unaware the SDK collects personal data. However, creators can also benefit from the collected data, as it can aid them in their endeavours such as influencing end users through advertisement. This is the party that embeds the SDK into its product before making it available to the user.


IDENTIFYING THE PARTIES INVOLVED

THIRD PARTY

The Third Parties
Buy the data to use for themselves, for example in the advertising business.

FIRST PARTY

The SDK Developer
Develops the SDK code, collects personal data through it, and sells that data

SECOND PARTY

The App Creator
Incorporates the SDK into their app to use its functionalities. They either benefit from the data collection or don't know about it at all.

FOURTH PARTY

The End User
Is the data subject that, often unknowingly, delivers their data, which endangers their fundamental rights and freedoms.

Lastly, there are **third-party** organizations that stand to benefit from any personal data collected by the developer and sold to them. Often, these organizations are active in the ad tech industry by facilitating the distribution of advertisements, using the acquired personal data to increase effectiveness. Usually, these parties are unknown to the end user as they have no direct relationship with the end user. These organisations can range from data brokers, to analytics specialists and even platforms (such as Facebook). As the revenue in ad tech has grown, so has the number of organisations which are gaining access to SDK-collected data.

2.3. Identifying types of data collected

The GDPR applies only to personal data, which covers information that can directly or indirectly identify a natural person. This definition includes unique identification numbers, which can include Advertising IDs, location data, and online identifiers such as IP addresses.[6]

[6] Article 4(1) GDPR.

In the privacy policies of companies that offer open source SDKs, there is an emphasis on the rules of the GDPR and the fact that non-personal data is collected. However, the so-called Advertising ID is always collected. For example, Google Analytics states in its privacy policy that by default Advertisement IDs, Operation Systems, and geography are collected.[7]

Each Android device with a connected Google account has such an Advertising ID. This ID is unique for every device and can be read by any app installed, no permission or user interaction is necessary. The Advertising ID provides linkability, as it enables advertisements to easily connect the dots between different apps and sources. Although the Advertising ID might not allow you to identify individual users, it can be linked to other information to provide insights into identifiable individuals. The European Commission (hereinafter: "**EC**") explicitly named Advertising IDs on a phone as an example of personal data.[8] This means that the rules of the GDPR apply when processing this data.

Additionally, it is possible that SDKs collect special categories of personal data, which as a general rule are prohibited, unless certain criteria are fulfilled.[9] Profiling can create special category data by inference from data which is not special category data in its own right but becomes so when combined with other data.[10]

Researchers at Mnemonic, a company that helps businesses manage security risks, protect data and defend against cyber threats, carried out an in-depth investigation into mobile applications and the data shared with third parties through SDKs. The research on 10 well known apps showed that although the privacy policies of the apps state that no direct identifiable information is gathered or shared, data such as age, gender, GPS were commonly shared and Ad IDs were shared with multiple SDK developers in all cases.[11] This is not only problematic because it means that illegitimate processing may take place, but it also makes it impossible to know for users what is actually happening.

[7] See Google's support page regarding Firebase.

[8] See the European Commission's website regarding personal data.

[9] Article 9 GDPR.

[10] WP251, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

[11] Norwegian Consumer Council, Mnemonic Technical Report "Out of Control" - a Review of Data Sharing by Popular Mobile Apps.

2.4. What happens to the personal data?

The factual flow of the personal data

Because of the ecosystem becoming extremely complex, data flows resulting from all this tracking via SDKs have become very diverse and difficult to analyse. In general, the flow of the personal data is as follows:

- A user downloads an app and uses the app. The app can contain multiple SDKs of which the user is not aware. The user usually consents to the privacy statement upon installation on the device, and sometimes is asked specifically through the permission framework of the OS if the app can use certain functions on the phone, such as location and camera.
- The app collects personal data as a user interacts with the application. Within the app the different SDKs may get access to the personal data. It has to be noted that this depends on the SDK and the amount of data and type of data can differ between various SDKs within the same app. For example, X-Mode, a location broker, consciously created SKDs which contain codes that specifically collect location data, which usually can be considered personal data. The collected location data through X-Mode's SDKs then are sold to parties interested in the data. X-Mode has even sold data to the United States intelligence agencies which used the data to monitor the movement of Americans, without obtaining the required warrants.[12]
- Through the third-party SDK which is being used in an app, the SDK developer gets access to the data. Most of the time this concerns data about the app user's (GPS) location, also called tracking data. The access to personal data of app users is gained through (sometimes hidden) parts of the codes in the SDK that are designed to track the user and store the data. The data is bundled and is subsequently sent to the SDK developer.
- Depending on the SDK, the data can then be forwarded to various companies and organisations. SDKs can be designed in such a way that it serves to collect and hold personal data that can be accessed by either the SDK developer or the app creator. The SDK developer itself often also uses the data that it receives from the apps for its own purposes. By using the SDK, an agreement is signed with the owner of the SDK that usually includes something like "Developer hereby grants SDK developer a nonexclusive, license fee free and royalty free right and license to access, copy, distribute, process and use all information, data and other content provided by Developer or received by [SDK developer] in connection with Developer's authorized

[12] See Vox and Techcrunch.

> use of the Services, including, without limitation information provided through any Application that Developer makes available for testing through the Services (collectively, "**Developer Data**")".[13]

Thus, in short, an SDK developer usually concludes an agreement with the app creator that the SDK developer itself can use the data that it receives when it for example helps to improve the app's functionality. Once an SDK developer has collected the data, it often uses it for its own purposes, but it can also be sold to third parties for advertising purposes. It is clear that the process often is so complex that it is impossible to know if, how, and to whom your data collected by a single app is sent.

[13] This is an example taken from Google's policy regarding their Firebase SDK. However, similar provisions can be found across a broad spectrum of other policies that are about use of SDKs.

3. SDK DEVELOPERS AND APP CREATORS VIOLATE THE EPRIVACY DIRECTIVE

Article 5(3) ePD prescribes that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a user requires, as a rule, prior consent. The consent requirement applies to *any* information, without regard to the nature of the data being stored. Importantly, the scope of the ePD also applies to every tracking technology on a device. Consent must be understood in the same way as in the GDPR. Given the broader scope of the ePD, this means that for access, processing or transferring of *any* data on the device consent is needed. The use of SDKs fails to meet this clear requirement.

3.1. Applicability of the ePD

Under the ePD a smartphone is terminal equipment that stores information, regardless of the information being personal data or not.[14] The provision on confidentiality of terminal equipment, article 5(3), is applicable to providers of information services. Mobile applications qualify as information society services, which means that the ePD is applicable.

To the extent that the app creator gains access to information that is stored on the device, the ePD applies and therefore must comply with the consent requirement as stated in article 5(3) of the ePD. Additionally, when a third party, such as an SDK developer, can access information via the app, the third party shall also have to comply with the requirements of article 5(3) ePD.

Whereas the applicability of the ePD on cookie practices is well established, less is said about SDKs within mobile applications. Given one of the Directives intended goals - regulate hidden identifiers and other similar devices that can enter the user's terminal to gain access to information or trace activities - it is clear that article 5(3) ePD applies to applications and SDKs on mobile phones of users. Moreover, there is a general consensus that "cookies" must be understood as including tracking tools such as SDKs.[15] This is true when SDKs are used solely for purposes of app improvements, but also when the SDKs use the data for their own purposes.

[14] WP202, Opinion 02/2013 on apps on smart devices, p. 7.

[15] See the blog on ESRB.org.

Thus, article 5(3) of the ePD is applicable to both app creators and SDK developers whenever they access information through the app on the mobile device

3.2. Article 5(3) ePD

Article 5(3) ePD, which has been implemented by the member states in national laws, prohibits for example the use of cookies, as cookies store information on the user's (or data subject's) terminal equipment (mostly their PC). Although article 5(3) ePD has been called the "cookie provision", its scope is greater. It, for example, also covers the collection and processing of information through APIs and SDKs, as these systems gain access to already stored information on for example a smartphone. This means that users of SDKs, be it the app developer or a third party, must also comply with the rules set out in article 5(3) ePD and that the use of data collecting and processing SDKs must be based on prior consent (see paragraph 3.2.1).

SDK-usage by app developers and third parties does not comply with the rules regarding consent. Almost every researched app which uses SDKs that store or access information on data subject and fall within the scope of article 5(3) ePD, does not ask permission at all or asks permission is such a way that it makes it impossible for data subjects to give specific, informed, unambiguous and free consent prior to the collection and processing by these SDK-users. As the ePD refers to the GDPR for the meaning and interpretation of consent, the exact meaning of the requirement will be explained in detail in section 4.2.1.

Why the exceptions do not apply

The final sentence of article 5(3) ePD states that the prior consent requirement to access or store information from terminal equipment shall not prevent:

> "Any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information service explicitly requested by the subscriber or user."

The EC stated that the former exception can be seen as “allowing the use of mere session cookies”.[16] This is not the case in situations in which the data accessed by either the app or the SDK is used to process personal data. The latter exception which includes “strictly necessary” has been described to mean essential, rather than reasonably necessary and to be restricted to what is essential to provide the service requested by the user, rather than what is essential for the service provider.[17] The use of (personal)data by apps or SDKs do not constitute as essential in that sense. Therefore, both exceptions to the consent requirement will not be applicable for app creators or SDK developers.

3.3. Relation between the ePD and the GDPR

Whilst the ePD and the GDPR have a different material scope, there are many examples of processing activities which trigger both scopes, such as the use of cookies.[18] In section 1.2 the lex generalis - lex specialis relationship between the GDPR and the ePD was mentioned. This can clearly be found in recital 173 and article 95 GDPR, stating that the GDPR shall not impose extra obligations when matters are subject to specific obligations with the same objective set out in the ePD.

This would mean that when *personal data* is collected through SDKs from the terminal equipment (the mobile phone), thus triggering both scopes, the stricter rules of the ePD must be followed. Since article 5(3) ePD stipulates that consent must be a legal ground for accessing and retrieving data, the additional legal grounds that are available under the GDPR would not be an option. Most notably, the legitimate interest ground of article 6(1)(f) GDPR would not exist or apply. In chapter 4, the legal ground for consent as well as the additional grounds available under the GDPR will be explored in depth.

However, the interaction between the two instruments remains complicated. As the EDPB mentioned:

[16] European Commission, ‘ePrivacy Directive: Assessment of Transposition, Effectiveness and Compatibility with Proposed Data Regulation’.

[17] UK Information Commissioner’s Office (ICO), ‘Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 2: Security, confidentiality, traffic and location data, itemised billing, CLI and directories, v.3.4’ (30.11.2006), p. 7.

[18] EDPB, Opinion 05/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and power of data protection authorities, p. 11.

> “Even if the processing of personal data (e.g. profiling) in part relies on access to information stored in the end-user’s device, the data protection rules which are not provided by the ePrivacy Directive (e.g. data subject rights, principles of processing) for any processing of personal data that takes place following the access to information stored in the end user's device shall be subject to the provisions of the GDPR, including the cooperation and consistency mechanisms.”[19]

In short, the provisions of the GDPR covers more than the ePD, amongst others additional transparency requirements, general principles of processing and users’ rights.

When both the ePD and the GDPR are applicable, their enforcement is bound to intersect. A violation of the rights enshrined in the GDPR often leads to a complaint directed at the national DPA. The manner in which the ePrivacy directive is enforced, however, is largely left up to member states. It is not mandatory for one particular national body to be appointed in this matter, which is unlike the responsibilities the member states face under the GDPR. As only the goals member states must achieve have been defined, such institutional flexibility is possible. The result: DPA’s are only competent to scrutinize the data processing operations governed by the ePD if national law confers this competence on them. However, the data protection authorities are always competent to enforce the GDPR, the fact that a subset of the processing falls under the ePD does not limit the competence.

When filing a complaint on SDKs, it is recommended to do so both in the context of the GDPR and the ePD. This could result in two scenarios:

- Firstly, a member state in which a single body is tasked with the enforcement of both the ePD and the GDPR. For filing a complaint, this is the most advantageous, as it is a one-stop-shop. However, it must not be assumed that this body has the same powers available to enforce the ePD as it does the GDPR. Though member states could be inspired by the GDPR, the powers an institution has relating to the ePD could be wholly different depending on national law.
- Secondly, a member state in which the enforcement of the ePD and GDPR is separated. Despite the overlap, the national data protection authority (hereinafter: “**DPA**”) remains competent over GDPR matters. As the ePD is a lex specialis, it might be necessary to file separate complaints with separate contents.

[19] EDPB, Opinion 05/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and power of data protection authorities, p. 23.

Thus, while the ePD might appear to be the most logical option given the stricter rules on legal grounds that are possible, there are reasons that complaints are filed under the GDPR at the relevant authorities. The GDPR has been a very publicly known piece of legislation, generating a lot of public attention, and has led to many precedents and clarification by the European and Data Protection Authorities. Additionally, if the violation includes one of the principles or user's rights specific to the GDPR, logically you would base your complaint on the GDPR instead of the ePD. In short, the interaction between the two instruments can be complex at times, and although they overlap there are also significant differences. Therefore, it is necessary to also explore the legality of SDKs in mobile apps within the GDPR framework, which will be explored in the next section.

4. SDK DEVELOPERS AND APP CREATORS VIOLATE IMPORTANT PARTS OF THE GDPR

This chapter aims to illustrate the violations that are, or potentially could be, committed by SDK developers and/or app creators who make use of these infringing, privacy-hazardous SKDs. The various (potential) GDPR-violations SDK-usage has are described below. All separate grounds form on themselves a valid ground to file a complaint at the competent and responsible DPA.

The GDPR has general principles that have to be considered, such as transparency, data minimisation etc. These principles are often enshrined within the more specific articles. Thus, the principle of transparency for example has been specified in articles 12-14 GDPR, but it is also an integral part of the specific part of "user rights" and within the consent requirement that is necessary in some cases for a lawful processing.

First will be explained why the GDPR is relevant, by elaborating on the concepts of "personal data" and "processor & controller". After it is established that SDKs fall within the framework of the GDPR, there will be focused on specific articles to show how they are not compliant. Articles regarding for example:

- Consent;
- Transparency (the general principle but specifically in relation to articles 13 and 14 GDPR); and
- Data minimisation and further processing.

4.1. SDK-developers and app-developers are joint controllers (article 26 GDPR)

Whoever determines the means and purposes of the processing of personal data of others is the 'controller'. However, in cases where several persons or legal entities take this decision together, they may be 'joint controllers'. The party which processes personal data on behalf of the controller is the 'processor'.[20]

[20] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 9, 24-27; Articles 4(7) and 4(8) GDPR.

When determining which party is the controller and which party is the processor, it is important to identify which party in the processing exercises actual and effective control. To be identified as a controller, one must decide why personal data is processed (the purpose) and how it is done (the means). Besides having to determine the purpose of the processing, a controller must also at least determine the essential means.[21] This implies that the controller must determine the means that are the closest linked to the purpose, such as which specific data is being collected and processed, for what period of time the personal data is being processed, which parties have access to the personal data and who are subjected to the processing.[22]

The processor may also determine means, as long as it does not concern the essential means. However, a processor can never determine the purpose, as the processor always processes personal data on behalf of the controller. On the other hand, controllers do not need to have access to the personal data to be marked as a controller.[23] Processors must be selected carefully by controllers, as they must offer appropriate safeguards and live up to certain criteria, such as expertise, reliability, available resources and reputation, throughout the entire processing.[24]

There is joint controllership, in accordance with article 26 GDPR, when two or more entities jointly determine the goals and means, all with decisive influence. A key indicator for joint controllership is that the processing would not take place without the involved parties.[25]

Regarding the use of SDKs, more than one party can be identified as controllers under the GDPR. Based on CJEU case law like Wirtschaftsakademie, Fashion ID and Jehova's witnesses, both the app creator which uses the SDK in its app's and the SDK developer which uses the personal data extracted though it's developed SDK can be labelled as controllers, making them joint controllers as defined in article 26 GDPR. After all, the processing of the personal data could not take place without one of the parties, making them both indispensable and necessary for the processing to take place. Both decide on crucial questions such as which data is to be collected by the app. According to article 26 GDPR, they must jointly see to the adherence to obligations in the GDPR, in particular with regard to the rights of individuals. To effectively achieve this, joint controllers must make an arrangement to allocate the responsibilities amongst themselves.

[21] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 9-16.

[22] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 14.

[23] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 16; CJEU Case C-210/16 (*Wirtschaftsakademie*), par. 38.

[24] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 29-30.

[25] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, p. 40 et seq.

The arrangements between the joint controllers, if existent, do not live up to GDPR standards

Factually speaking the SDK developer and the app creators which uses the SDK that illegitimately collects personal data jointly decide on the aim and essential means of the processing. The fact that the developer does not have much say in how the creator processes the data is not relevant, as can be seen in CJEU Fashion ID. What is relevant in that respect, is that the collection of data would not be possible without the developer, which makes his role essential to the processing. The developer's role can be compared with that of the Fashion ID website in the data gathering process. That's why they have to make a transparent arrangement about the responsibilities of each controller, especially considering the appropriate measures to ensure the data subject's rights and the duty to inform. Either party is fully liable for damages suffered by data subjects. Almost none of the existing arrangements between parties, if they exist at all, do not live up to GDPR standards.

4.2. Articles 5, 6 and 7 GDPR are not complied with, resulting in unlawful processing

For the further processing of personal data to be lawful after its collection, the processing must be based on one of the six legal bases stated in article 6 GDPR. In the case of trackers in mobile apps, consent given by the data subject (article 6 (1)(a)) and processing necessary for the purposes of the legitimate interests pursued by the controller (article 6 (1)(f)) are the most relevant bases.

Furthermore, the general principles of processing of personal data that are laid down in article 5 GDPR must be adhered to. These include principles like lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limitation and integrity and confidentiality.

4.2.1. The processing is unlawful because it is not based on the foundations of article 6 GDPR

The processing cannot be based on consent - article 6(1)(a) GDPR

Consent under the GDPR, as well as the ePD, has to be specific, informed, unambiguous and freely given prior to processing.[26] This is not adhered to in the case of SDKs, as data subjects are not properly asked for their consent when they use or download an app.

[26] EDPB, Guidelines on Consent under Regulation 2016/679.

For consent to be **specific**, the data subject must know for which purposes it gives consent. This is important, as every (further) processing based upon a different purpose requires newly given consent. In order to receive specific consent, the controller must follow the following rules:[27]

- **Granularity**, which means that consent has to cover all processing activities that are being carried out for the specific purpose or purposes. In case of multiple purposes, consent has to be given for all the different purposes;
- **Purpose specification**, which serves as a safeguard against possible function creep and a potential invasion of privacy; and
- **Separating information** related to obtaining consent from the data subject from other information regarding the processing activities.

Furthermore, consent needs to be **informed**, which means that the controller has to provide the data subject with all necessary information regarding the various aspects of the intended processing of personal data (see EDPB/5/2020). This aspect is crucial and is closely related to the fundamental principle of transparency. In order to inform the data subject, controllers must refrain from using long, unreadable, data policies that are difficult to understand. The information regarding the consent must be presented in a manner which is clearly distinguishable from the other matters, easily accessible and intelligible and expressed in clear and plain language which is understandable for the data subject.

Unambiguous consent means that the data subject has given consent via a clear affirmative action. Pre-ticked consent boxes do not fulfill this requirement, as they do not clarify that the data subject has actively given his or her consent for the particular processing.

Lastly, consent must be given **freely**. Freely given consent means that the data subject has a real choice. The general rule is that consent is not valid and given freely if the data subject has no real choice, feels compelled to consent or will endure negative consequences if consent is not given. Other indications or situations that presume consent no freely given consent are:

- An imbalance of power (e.g. in employment);
- Bundling of consent as a non-negotiable part of term and conditions;
- Bundling of consent for a bundle of processing purposes (no granularity);
- No possibility to refuse or withdraw consent without negative consequences.

[27] EDPB, Guidelines on Consent under Regulation 2016/679.

Most apps and smartphone environments that use SDKs do not meet the criteria for consent, as the consent cannot be specific nor informed if the data subject in the first place does not know about any transfer of data to third parties. Furthermore, in most cases, the information provided during the installation of the app required to speak of informed and specific consent is insufficient or not present at all, making it illegitimate to process the personal data on this ground. SDKs are in most cases not even mentioned at all.

Furthermore, the data subject has a general right to withdraw consent at any given time without facing negative consequences, as specified further in article 7 GDPR. There can be no freely given consent, if the data subject is not able to withdraw consent in a way at least as easy as the way the consent was given initially. Regarding SDKs that illegitimately track smartphone and app users, consent in itself is almost never withdrawable. The permission system which can be found, for example, in Android smartphones controls the accessing rights of apps to matter such as camera, microphone or GPS location. However, it is questionable and highly possible that refusing or withdrawing the apps right to access does not affect personal data collecting and processing through the SDKs in the apps and thus withdrawal through these permission systems does not cover SDKs, making withdrawal impossible.

The processing cannot be based on a legitimate interest - article 6(1)(f) GDPR

Another provision of the GDPR that can serve as a basis to process personal data is the provision regarding legitimate interest as set out in article 6(1)(f) GDPR.

It is important to note that when the ePD, discussed in chapter 3, is applicable, the option to legitimate the processing when the information has been accessed through the terminal equipment the grounds of a legitimate interest ceases to exist. Given the *lex specialis* status of the ePD, the stricter requirement of prior consent needs to be followed.

Nevertheless, the following section will explain why the legitimate interest ground of article 6(1)(f) GDPR in itself would not be a possibility for the processing.

The pursued interests of the controller must be known to the data subject and cannot be speculative. These interests must be legitimate, which means that it must be acceptable under the law and must not override the interests or fundamental rights and freedoms of the data subjects which require protection. To decide whose interests and fundamental rights deserve to be favored, a balancing test must be carried out, which is comprised of the following four main headings:[28]

1. **Assessing the controller's legitimate interest**. Does the controller exercise a fundamental right, is there a public interest or is there another legitimate interest? The more explicitly recognised the legitimate interest is, whether by law or through culture, the more heavily the specific legitimate interest will weigh in the balance test.

2. **The impact on data subjects' fundamental rights and freedoms**. This is a crucial criterion. Several elements can be considered when assessing the impact, such as: the nature of the personal data, the way the data/information is being or will be processed, the reasonable expectations of the data subject and the status of the data subject and the controller. A certain impact in itself is not forbidden, as long as the impact on the data subject is not disproportionate with respect to the controller's legitimate interest. When assessing the impact, also the frequency, intensity and the severity of the impact, as well as the negative and positive aspects of the impact, have to be taken into consideration.

3. **Provisional balance**. It is important that the controller also makes further assessments as to the impact on the freedoms and rights of the data subject and whether it is necessary to take additional measures that could reduce the impact. Aspects that need to be taken into account are for example whether the data involved is sensitive data. This will not immediately make the legitimate interest ground unobtainable, but it weighs heavily in the weighing of the interests involved.

4. **Additional safeguards applied by the controller**. Additional safeguards can be used to influence the balance and help 'tip the balance' on the scale, making the impact on the data subject acceptable. Different types of safeguards can be considered, as long as they ensure that the consequences for the data subject are reduced enough to ensure that the data subject's fundamental rights and freedoms are not disproportionately impacted. Examples of safeguards include:
    - Technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals;
    - Extensive use of anonymisation techniques;
    - Aggregation of data

[28] WP217, Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC".

- Privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments;
- Increased transparency;
- General and unconditional right to opt-out;
- Data portability & related measures to empower data subjects.

The controller cannot base the processing on a legitimate interest when the impact of the processing is disproportionate compared to the fundamental rights and freedoms of the data subject.

If the controller or a third-party processes personal data on the basis of the legitimate interest, it does give the controller an extra responsibility to take the interests of data subjects into account and to guarantee the rights of data subjects. Like the obligation to inform the data subject in advance about that intended processing.

Although in some cases it may seem like the app creator and the SDK developer have a legitimate interest, when SDKs are put to the balancing test, the fundamental rights and freedoms of data subjects outweigh the controllers' interests. This is so, because the collecting and processing of personal data in the first place happens often secretly. The data subject is not even aware that its personal data is being processed. Furthermore, a more principled argument is that today's smartphones have become the primary holder of personal data. Uncontrolled access to the data subject's smartphone by a party like the SDK developer is a serious violation of the privacy of the data subject. Another reason why data subject's rights outweigh the controller's legitimate interest, is the fact that data subjects in most cases do not have a right to opt-out and stop the processing. Lastly, if there is sensitive data involved the likelihood of a successful appeal on the legitimate interest ground also decreases, especially in combination with poor opt-out options and lack of transparency.

4.2.2. The processing is unlawful because it is not transparent

The current use of SDKs in apps violate the requirement of transparency in two ways: firstly, the app violates its obligations to rightly inform the users about the existence of third-party SDKs being present in the application; secondly, the third party SDK itself violates its obligation as it further processes data by not providing *any* information to the users.

Transparency is one of the general principles that can be found in article 5 GDPR and relates to other articles in the GDPR. Articles 12, 13, 14 and 15 ensure the specific implementation of the principle. These obligations directly link transparency with the right to be informed (from the user's side) and the obligation to inform (from the controller's and/or processor's side). The GDPR requires data controllers to be transparent, *even when* data subjects do not specifically request information. In this case this means that the users of the app have a right under the GDPR to be informed by both the app creator when they process information, as well as by the SDK developer when their data will be used for further processing in case they receive data.

Central to the principle of transparency is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and they should not be taken by surprise at a later point about the manner in which their data is processed.[29]

Concretely, app creators are obliged by article 13 GDPR to inform the data subjects because they directly receive the data from the subjects. The SDK developers have to comply with article 14 GDPR, since they receive the information indirectly from the data subject, namely through the use of SDKs.

Article 13 GDPR: Apps violate transparency obligations

The apps collect the data directly from the user and therefore fall under article 13 GDPR.

When an app is installed, often you first need to agree with consent before using an app. While you can actively choose to customize some of the data processing related to functional usage, you do not have a choice with the necessary data processing. For example, if you use Spotify, personal information such as your name, address, gender and email address as well as technical information like your IP address are automatically collected. You only have the ability to choose whether to share more by adjusting the settings.

When an app collects data that is necessary for the functioning of the app, it means that it will be collected by default. This type of collection occurs regardless of your privacy options, as it is necessary for the performance of a contract. Therefore, information about this collection has to be made easily available and accessible by the controller. This is not the case if the user needs to search through multiple pages to find information about the processing.

[29] WP260 rev. 01, Guidelines on transparency under Regulation 2016/679, p. 8.

Information on the usage of SDKs in the app should also be available, and when this is not the case this is a clear violation of the transparency obligations under article 12 GDPR. For example, Spotify states in its privacy policy that it may share personal data with advertising partners or service providers without specifying them. Instead, they use a separate list "software by third parties" where all the SDKs are listed. In yet another document, the terms and conditions, Spotify states that you agree to comply with any third-party terms.[30] While it is clear that SDKs such as Firebase analytics by default collect data, this information is not shared in the privacy policy of the app, instead information is spread out over various documents.

Whereas Spotify does list some of the SDKs in the app, other apps do not mention SDKs at all. The app Perfect365 refers in its privacy policy[31] to "partners privacy policies" which shows two links to partners. However, Exodus discovered that the app contains 55 SDK trackers.[32] In this case the app grossly violates article 13(1)e which stipulates that a processor should inform data subjects about "the recipients or categories of recipients of the personal data".

This illustrates how apps do not comply with the transparency principle. While they are required to provide the most basic information regarding the receivers of data, privacy policy's neglect to do so. Either no information on the SDKs is available entirely (see the Perfect 365 example) or the information is stored apart from the privacy policy and the information is incomplete and too far away given the standard that information should never be more than "two taps away" in apps.[33]

Article 14 GDPR: SDKs violate transparency obligation

The SDKSs that receive data through the integration within the apps use the data they receive. For example, Google's Firebase SDK is used in almost all apps, including Spotify and Perfect 365 discussed before. In Google's privacy policy it is stated that "Apps use Google services (such as Google Analytics) ... when they integrate our services, these sites and apps share information with Google … Google uses the information shared by sites and apps".[34] It is thus undisputed that whenever an SDK developer itself uses the information obtained, they can be seen as a controller and therefore have to comply with the transparency requirements of article 14 GDPR. Because they receive the data indirectly, they are obliged to inform data subjects

[30] Terms and Conditions of Use - Spotify.

[31] Privacy Policy | Perfect365.

[32] εxodus (exodus-privacy.eu.org).

[33] WP260 rev. 01, Guidelines on transparency under Regulation 2016/679, p. 8.

[34] How Google uses information from sites or apps that use our services – Privacy & Terms – Google.

at the latest one month after the data are obtained when the data is not used for communication with the data subject or disclosed to another recipient.[35]

SDK developers consistently fail to do so. Whereas they are obliged to not only inform you that they are processing data, they should provide you with all the information listed in article 14 GDPR. SDK developers do not inform data subjects when they are using the data that they obtained through the SDK in an app that the subject uses, and therefore are in violation of the transparency requirements of article 14 GDPR.

Given the fact that there is no information at all, it is not even possible to assess whether the information provided meets the requirements set out by the GDPR. Thus, while it is likely that *when* SDKs would inform the subjects, they would fail to do so accordingly, because they do not inform data subjects at all.

4.2.3. The processing is unlawful because it is not limited in its purpose and the processing of data is not minimised

Personal data can only be collected with regard to an explicit, legitimate and specific purpose.[36] Any processing that is not compatible with this purpose is forbidden. The purposes pursued by SDKs and apps implementing SDK do not adhere to these required standards.[37]

The formulated purpose plays a central role in the processing, as the extent of many responsibilities and guarantees embedded in the GDPR depend on it. It is in the interest of the controller to formulate their purpose broadly so as to include as many types of processing as possible.

Most relevant for the usage of SDKs is the requirement that a purpose is **specific**, which cannot be the case when purposes are formulated in a generic manner. On the basis of the provided purpose, it must be possible to determine its exact boundaries. Subjects are then able to ascertain what to expect from the processing, and it becomes evident for controllers which guarantees to implement. This aspect of purpose limitation is especially important as many controllers want to collect data for future use. They are sure personal data will be useful to them, but they do not know for what virtue at present. This attitude goes against the data

[35] Article 14(3) GDPR.
[36] Article 5(1)(b) GDPR.
[37] WP203, Opinion 03/2013 on purpose limitation.

minimisation and storage limitation principles. Purpose limitation seeks to be a solution to this threat. Examples of formulations that are not specific enough are *improving user experience*[38] and *securing the service*.[39]

As discussed, apps often send users' personal data to third parties, amongst which SDK developers. If SDK developers then want to use that data for their own benefit, they become controllers and must therefore define purposes themselves. These too must adhere to the standards set forth above. If controllers choose to pursue more than one purpose, they have to make sure each separate purpose is rooted in one of the lawful grounds of article 6 GDPR. Purposes must be announced before or at the latest at the time of the collection of personal data. Further processing is allowed, provided that such processing is compatible with the original purpose for which the data was collected.

The principles of purpose limitation and **data minimisation** are closely intertwined. One must not collect more or for a longer period of time than is necessary for the pursued goal. Anything beyond the minimum will be excessive, and therefore violate the minimisation principle. The amount of data collected and the period during which it is stored should be limited to what is necessary for the pursued purpose. With regard to SDKs, there is no evidence these principles are adhered to. The minimisation requirement has a number of benefits. It reduces the risk of the data leaking in a security breach. Moreover, more information about users often results in inference of additional information that is not explicitly present in the data. Negative consequences can arise when these inferences are incorrect. Lastly, as demonstrated elsewhere in this paper, lack of transparency is a problem that occurs frequently when it comes to SDK use. This causes data subjects to lose control over their data. To prevent the aggravation of such powerlessness, the amount of data must be limited to what is necessary.

A principle closely related to the aforementioned marriage is that of article 25 GDPR: privacy by design and default. The article aims to provide (very abstract) guidelines on how to implement privacy elements into a product or service in the developing stage.[40] For example, a system can be created to automatically delete information after a period of time. It will then actively intervene in the processing. A system can also be passive, for example when it is programmed to only collect certain types of information. When it is not programmed to collect more, it will not do so. Both approaches require prior contemplation by the developing team.

[38] As mentioned on the 23th of June 2021 in the privacy policy of second-hand clothing platform Vinted, paragraph 2.1 and 2.2.12.

[39] As mentioned on the 23th of June 2021 in the privacy policy of payroll human resource management app Kolibrie, paragraph 1.3 (Dutch).

[40] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

The rationale that SDK developers do not adhere to the principle of data minimisation is derived from the manner in which they conduct their business: they acquire their revenue (in large part) through the monetization of personal data. It is up to those with the appropriate technical expertise to research the factual accuracy of our statements. As we cannot factually confirm this hypothesis, we recommend that this topic be researched further by others who can.

4.3. In many instances, special categories of personal data (article 9 GDPR) are processed without controllers being able to base this on one of the grounds of exception, resulting in unlawful processing

Many SDKs collect special categories of personal data. It is prohibited to process special categories of data, unless it can be based on one of the grounds of exception that are set out in article 9 GDPR.

SDKs are present in the majority of apps, and will therefore collect many types of data, including data about political views, sexual orientation, religion and ethnic background. This data can be directly given by the data subject, for example by downloading and regularly using a Qur'an app. Additionally, it can be indirectly inferred, for example through location data, when the subject regularly uses a ride-sharing app to pick them up at a religious institution. Furthermore, the combination of several types of data from several sources - a practice in which advertising SDKs specialise - can yield special categories of data. For example, combining data such as contact lists, websites visited and podcasts listened to could produce conclusions about one's political preference. The processing of special categories of data by SDKs is often not based on one of the grounds of exception and is therefore unlawful.

The processing of special categories of data is in principle forbidden, because their use constitutes an exceptionally large threat to data subjects' fundamental rights, such as the right not to be discriminated against.[41] Last year VICE reported that the US Military has been buying location data collected by ordinary apps mainly targeted towards a Muslim audience.[42] One of the prayer apps alone has over 98 million downloads. Although VICE was unable to uncover what the data is being used for, in the past the US Military has been known to use this type of (meta)data to target drone strikes in their ongoing battle with Muslim terrorist groups. In

[41] EDPB, Guidelines 8/2020 on the targeting of social media users.

[42] J. Cox, 'How the U.S. Military Buys Location Data from Ordinary Apps'. Accessible through Vice.

essence, an SDK in a religious prayer app collects information about your location and sells it to data brokers who end up selling it to the US military. You might then run an increased risk of becoming the victim of a drone strike, solely because of your religious beliefs.

4.4. The transfer of personal data obtained through SDKs to third countries is not based on GDPR mechanisms and is therefore unlawful

In principle, any transfer of personal data to third countries or international organisations is prohibited, unless the exceptions in articles 45 up and until 49 GDPR are met. In the case of SDKs, they are not met. Especially transfers to the United States rely heavily on invalid adequacy decisions.

A controller must verify the transfer exception they wish to rely on.[43] The starting point in this process is usually checking if there is an adequacy decision, as enshrined in article 45 GDPR. These decisions are made by the EC, when they've determined that the level of protection in a third country is up to GDPR standards. In absence of such a decision, controllers can rely on the standard contractual clauses mentioned in article 46 GDPR. These too are determined by the EC, but it remains up to the controller to regularly check and guarantee the level of protection. Binding corporate rules, as can be found in article 47 GDPR, and article 49 GDPR for incidental transfers are not of use to the relevant businesses. Many SDK providers are stationed in third countries. For example, SDK developer AppsFlyer is located in the United States, South Korea, India and Thailand, all of which are not subject to an EC adequacy decision. Ditto for SDK developer AppLovin, based in the United States. Both developers' products are present in over 5000 apps.[44] Neither business has received an approval to implement binding corporate rules.[45]

Data transfers to the US are especially problematic, considering the Court of Justice of the European Union has ruled adequacy decisions illegitimate twice (both Safe Harbour and Privacy Shield) and has expressed its concern about the level of protection possible through standard contractual clauses when taking the Snowden leaks into consideration.[46] However, many developers still arrange their transfer practices on the basis of these invalid adequacy

[43] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

[44] According to Exodus Privacy: AppsFlyer and Applovin.

[45] The EC has published a list with BCR approvals current until the 25th of May 2018 here.

[46] CJEU Case C-362/14 (*Schrems I*) and CJEU Case C-311/18 (*Schrems II*).

decisions. For example, AppsFlyer legitimizes its data transfers to the US based on Privacy Shield certifications.[47] Not only are these transfers illegitimate as the Privacy Shield is illegitimate, such statements also create a false sense of security for the average end user that is not up to date with GDPR ins-and-outs. Other examples include SDK developers InMobi[48] (located worldwide, including in the US and reaching over 1 billion unique devices), OneSignal[49] (located in the US and present in +750.000 apps) and Vungle[50] (located in the US and present in +4000 apps).

[47] As can be found in the privacy policy on their website.
[48] As can be found in the privacy policy on their website.
[49] As can be found in the privacy policy on their website.
[50] As can be found in the privacy policy on their website.

5. CONCLUSION

SDKs, or software development kits, are software tools which contain pre-written sets of codes that help apps function by offering functionalities for apps that are time consuming to build from scratch. The underexposed problem of SDKs is the potential illegitimate use of them in apps by app creators, turning these apps into spies. By adding certain codes in the SDK that not only add functionalities, but facilitate the collecting personal data of the smartphone, SDKs are being used to track smartphone users through the apps that they use. This practice is carried out on a very large scale and without the smartphone user being aware. After all, almost everyone possesses a smartphone nowadays which contains apps with these evil SDKs, making it an issue that touches the interest of almost every individual on earth. The illegitimately collected personal data are subsequently sold or transferred to third parties which use the data for example for advertising purposes or even worse for actual spying. These activities regarding SDKs are illegal and in violation of existing privacy laws.

Examples in this report illustrate how SDK developers and app developers violate the obligations set out in the ePD, since the requirements of valid consent are not met. The same holds true for a violation of the consent ground as well as the legitimate interest ground under the GDPR. Additionally, the report showed how the general principles of the GDPR are not complied with, along with the requirements regarding the transfer of data to third countries. We have seen that the privacy policies of the major apps we looked at, fail to mention the information that is required regarding the use of SDKs. This harms the transparency requirements, but also deprives users from an effective enforcement of their own rights, which could be an interesting topic for further research. Furthermore, the lack of information gives the impression that the principle of data minimisation has not been adhered to. The overall difficulty to find the relevant information, leads us to believe that there are more violations to be found. Therefore, we recommend that a technical specialist researches this topic.

This report tried to give an overview and by means of examples show how SDKs and app developers violate provisions in both the ePD and the GDPR. The fact that we found violations for all developers and creators in these examples, suggests that this is common practice and the violations amongst SDK developers and app creators are widespread. We have tried to give an overview of the practice of SDKs and how this practice can violate European data protection legislation. We hope that this report can contribute to the knowledge that exists about the legal issues surrounding SDKs. Ideally, more research is conducted in the future, possibly leading to concrete complaints to data protection authorities that would help to stop the current illegal practice carried out by SDK developers and app creators.