General Data Protection Regulation and Intelligent Personal Assistants: A Study of Data Protection Obligations Governing the Principles for the Processing of Personal Data, its Transfer to Third Countries and its Utilisation for Marketing Purposes

Dr. Roland Steidle

ACKNOWLEDGEMENTS

I would like to thank my Tutor, Dr. Krzysztof Garstka, Centre for Intellectual Property and Information Law of the University of Cambridge, for the great support he offered me during the writing of my dissertation. His help and tips regarding content and structure of this work have been vital to finish this ambitious study at the interface of international laws and modern technologies in just a few months. My further thanks go to Ms Sally Frost, University of Cumbria, for the great help and hints regarding access to literature via the University’s online library.

ABSTRACT

Intelligent Personal Assistants (IPAs) such as Amazon's Alexa, Apple's Siri, Google's Assistant or Microsoft's Cortana are powerful tools that offer their users a wealth of functionality. For example, IPAs can assist in planning trips, navigating, ordering and paying for goods and services, handling search requests (sometimes depending on the user's location), processing text as well as converting between voice and text. In order to be able to offer this functionality, the providers must process a large amount of personal data. Some functions also require the processing of special categories of personal data such as voice data. Usually, the providers are based in the United States and process user data in data centres worldwide, that means in third countries outside the European Union. Most IPAs are offered free of charge to consumers. Instead, consumers often pay with their usage data which is sold to third parties for advertising purposes. This study examines the influence of data protection requirements – based on the EU General Data Protection Regulation (GDPR) – on the operation of modern IPAs, on data transfers to third countries and on the sale of data for marketing purposes. One focus of this study is to derive concrete requirements to fulfil general data protection principles arising under Article 5 GDPR. Another focus is placed on the analysis of the appropriate legal bases under Article 6 GDPR on which the various data processing operations can be performed in a legally secure way. It will be shown that IPA services that offer a typical range of functions including the processing of special categories of personal data as well as the sale of usage data for advertising purposes regularly require user’s consent.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
App	Software Application
art	article
Art 29 WP	Article 29 Data Protection Working Party
ch/chs	chapter/chapters
cmt	comment
DPA	Data Protection Supervisory Authority
DPD	Data Protection Directive 95/46/EC
ECJ	European Court of Justice
edn	edition
ed/eds	editor/editors
EEA	European Economic Area (Iceland, Liechtenstein, Norway)
eg	exempli gratia/for example
EPD	E-Privacy-Directive 2002/58/EC
EPR	E-Privacy-Regulation, Draft COM(2017) 10 final
et al	et alii/and other
EU	European Union
ff	and following
GDPR	General Data Protection Regulation (EU) 2016/679
ID	Identifier
ie	id est/that means
IPA	Intelligent Personal Assistant
IT	Information Technology
no	number
para	paragraph
PIM	Personal Information Manager
s/ss	section/sections
TC	Telecommunications
VoIP	Voice over IP

1. INTRODUCTION

Over the last 20 years, new information technologies (IT) have developed, offering great support to their users. Today, computers, tablets and smartphones can provide 'smart' and 'intelligent' services that are commonly known as Intelligent Personal Assistants (IPAs), sometimes called 'Digital Personal Assistants' or 'Virtual Personal Assistants', too.[1] For example, IPAs may be used for researching, scheduling, travel planning, navigating, paying for goods and services and for word processing.[2] They can also be used for controlling of other smart devices, eg in households or plants.[3] They can be controlled via voice input, keyboard or typing.[4] Typically, these IPA services are offered without demanding financial remuneration for the provider.[5] Instead, the user often pays with his usage data,[6] in many cases without having a concrete idea about how and to what extent his data is processed and utilised.

[1] Sanjay Mishra, *Wearable Android: Android Wear & Google Fit App Development* (Hoboken, New Jersey: Wiley 2015) 3ff., 24.; Michael McTear and Zoraida Callejas, *Voice Application Development for Android* (Birmingham: Packt Publishing, 2013) 9; Nicholas Negroponte, *Being Digital* (Alfred A. Knopf 1995) 101, 127ff.

[2] Apple, 'Hey Siri, wake me up at 7 AM tomorrow' <https://www.apple.com/ios/siri/> accessed 29 August 2018 and Google, 'Ready to help, wherever you are.' <https://assistant.google.com/intl/en_uk/#?modal_active=none> accessed 28 August 2018 show exemplarily typical areas where IPAs can be used.

[3] Mishra (n1) 19-23, 247ff.

[4] Mishra (n1) 6, 16f.; McTear et al (n1) 8f.; Negroponte (n1) 89ff., 127ff.

[5] ibid (n2).

[6] Yoan Hermstrüwer, 'Contracting Around Privacy. The (Behavioral) Law and Economics of Consent and Big Data' (2017) 8 JIPITEC 9f. <https://www.jipitec.eu/issues/jipitec-8-1-2017/4529> accessed 6 September 2018; Santiago López, 'Informing Consent. Giving Control Back to the Data Subject from a Behavioral Economics Perspective' (2018) 9 JIPITEC 35, 47f <https://www.jipitec.eu/issues/jipitec-9-1-2018/4678> accessed 6 September 2018; Gianclaudio Malgieri and Bart Custers, 'Pricing privacy – the right to know the value of your personal data' (2018) 34 C.L.S.Rev. ch 1.

In the past decade,[7] a reform of the European data protection law that was primarily based on the EU Data Protection Directive 95/46/EC (DPD) from 1995 was discussed. After years of negotiations and backlashes,[8] the Member States agreed on the EU General Data Protection Regulation (EU) 2016/679 (GDPR) that came into effect on 25th of May 2018. It contains new and, for some situations, stricter requirements as well as higher fines than the former DPD.[9]

Against this background, the requirements for providers of IPA services regarding the European data protection law shall be identified and concretised regarding IPA functionalities and purposes of processing. The aim of this study is to provide an answer to the question of what concrete requirements must be fulfilled by IPA providers who offer their services in the European Union (EU) with respect to the GDPR. The examination shall be focused on the following three requirements: first, concerning the fulfilment of general principles of data protection under the GDPR. Second, concerning the legal basis for providing IPA services focused on the international transfer of personal data from the European Union to third states where IPA providers are usually seated. Third, concerning the utilisation of personal data from data subjects by selling it for marketing purposes.

[7] J Kühling and J Raab, *DS-GVO und BDSG Kommentar* (GDPR and German Data Protection Act Commentary) (Jürgen Kühling and Benedikt Buchner eds, 2nd edn, C.H. Beck OHG 2018) introduction paras 1-9; Gerrit Hornung, 'A General Data Protection Regulation for Europe: Light and Shade in the Commission's Draft of 25 January 2012' (2012) 9 SCRIPTed 64ff.

[8] Jan Albrecht and Florian Jotzo (eds), *Das neue Datenschutzrecht der EU* (The new EU Data Protection Law) (NOMOS 2017) ch 1.C, paras 11ff.

[9] Lukas Feiler, Nikolaus Forgó and Michaela Weigl (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Globe Law and Business 2018) ch 1.

2. AN OVERVIEW OF LITERATURE REVIEW

A literature review with respect to the questions of this study shows a lot of peer-reviewed articles as well as several textbooks and a small number of legal commentaries regarding general data protection law in the European Union and its development over the last few years. A handful of articles can be found with respect to the new GDPR.

Besides, there are several technical and business-driven articles that explain how IPAs work and why the transfer and utilisation of personal data is such an enormous international business.

The literature review shows that there is a wide field of scientific material that provides a sound basis for further research and the development of answers to the questions above.

However, the missing piece is the connection between IPAs and the identification of concrete requirements for this technology that can be derived from Article 5 and Article 6 GDPR. Although many requirements from the substantive law of the GDPR are equal to the requirements of the former DPD, there are new principles under Article 5 GDPR as well as new details concerning the legal basis of data processing under Article 6(1) and (4) GDPR. As far as it can be seen after the literature review, there is no article or study that combines both, the new technology of IPAs as well as the new requirements for companies that offer IPA services under the GDPR. For this reason, the author concludes that answering the questions illustrated above could lead to new and enriching results for the legal discussion regarding the operation of IPAs, international data transfers and the sale of usage data for marketing purposes.

3. METHODOLOGY

In the following, the methodology of the examination will be described.

3.1 Focus of the Examination and Exclusions

The focus of this study will be placed on the GDPR requirements for the processing of personal data for the general operation of IPAs, the transfer to third countries and the re-use for marketing purposes excluding individual rights[10] of data subjects. Legal issues regarding the obligations towards a data protection supervisory authority (DPA), eg with respect to registration, cooperation, notification of data breaches or consultation, would exceed the scope of this work and will therefore be excluded. Moreover, issues regarding the internal compliance, for example obligations referring to proper documentation, undertaking of a data protection impact assessment, notifications in case of personal data breaches or mandating subcontractors,[11] will be excluded, too.

The E-Privacy-Directive 2002/58/EC (EPD)[12] will not be considered in detail. It shall be replaced by an E-Privacy-Regulation (EPR) in the future. In case any provisions of the EPD become relevant for the subject-matter of this study, they will be considered.

[10] For individual rights see Monika Kuschewsky (ed), *Data Protection & Privacy* (3rd edn, Sweet & Maxwell 2016) s 9 and W. Gregory Voss, 'European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting' (2017) 72 Business Lawyer 221, 225f.

[11] For all of this see Ardi Kolah, *The GDPR Handbook: A Guide to Implementing the EU General Data Protection Regulation* (Kogan Page 2018); Voss (n10) 228f.

[12] ibid (n10) s 4.4.

Furthermore, specific technical issues and challenges of artificial intelligence (AI) will not be in the focus. New requirements occurring from AI can concern the way personal data is being processed. However, this has no impact on the legal requirements of the GDPR for the operation of IPAs, international data transfers and the sale of personal data.

3.2 Proceeding of the Examination

First, there will be a short functional description of IPAs as the technical subject-matter. It will be shown what kind of services they provide, what data is required, collected, processed and transferred to the provider for the functioning of the services and for the further sale (section 4).

Second, the author examines and identifies the scope of the GDPR, the legal categories of personal data used by IPAs, the relevant principles for the processing of personal data regarding Article 5 GDPR and the legal bases under Article 6 GDPR that a provider can eventually rely on. General requirements that are not in particular important for IPAs and the subject-matter will be delimited (section 5).

Third, concrete obligations that apply especially for IPA providers will be derived from the general legal requirements that have been identified before (section 6). This will lead to the material results of this study. The author will critically analyse how the said requirements of the GDPR shall be fulfilled in concrete. It will be considered both, the obligations arising under the identified relevant principles of Article 5 GDPR as well as the obligations arising under the different legal bases of Article 6 GDPR.

Finally, the results of the examination will be summarised in a conclusion (section 7).

4. INTELLIGENT PERSONAL ASSISTANTS

In the following, a short functional description of the object of investigation will be provided.

4.1 Basic Functions and Data Processing of IPAs

As computing power and internet bandwidth have increased over the last 20 years and powerful mobile devices have been developed, interactive and autonomous computer systems have become increasingly popular.[13] These systems can now be described as intelligent.[14] Today, IPAs are mainly provided via mobile device platforms.[15] Apple's Siri, Amazon’s Alexa, the Google assistant ('Hey Google!') and Microsoft's Cortana are the best-known examples of IPAs. Future IPAs will probably be offered via ‘wearables’.[16]

IPAs include a variety of different functions. Typically, they are used for various research tasks. For example, inquiries using an internet search engine can be made by an assistant. More advanced assistants can also independently identify search sources, such as libraries and databases, and prepare research results for the user.[17]

[13] Mishra (n1) 3ff.; Negroponte (n1) 101ff. describes the first developments starting in the 1960ies.

[14] Mishra (n1) 4, 24; Negroponte (n1) 101.

[15] Mishra (n1) 4f.

[16] Mishra (n1) 4, 6. Thereafter, wearable means capable of being worn such as smart watches, eyeglasses or jewellery, and so on.

[17] ibid (n2).

Another typical field of application of IPAs is the conversion of text to speech,[18] for example to facilitate the operation of computers for people with visual impairments. Conversely, modern IPAs can convert speech to text, too.[19] Thus, they allow the instruction of software applications that were previously controlled by keyboard or typing movements solely.[20] They also allow the dictation of text, eg in situations where the user cannot operate a keyboard.[21] This can be helpful, for example, when a user drives a car, checks messages via his IPA and answers them verbally.[22]

Modern IPAs can analyse text in detail. They are capable of recognizing spelling errors as well as grammatically conspicuous sentences.[23] They can be used to produce text like contracts, eg in a legal-tech scenario.[24] Particularly challenging but more and more successful is the translation of text from and into different languages by IPAs.[25]

[18] McTear et al (n1) 14-16.

[19] Negroponte (n1) 91 describes first voice recognition developments in the 1970ies.

[20] Mishra (n1) 6, 16f.; Michael Veale, Reuben Binns and Jef Ausloos, 'When data protection by design and data subject rights clash' (2018) 8 IDPL 105, 122f. <https://doi.org/10.1093/idpl/ipy002> accessed 6 September 2018.

[21] ibid (n2); McTear et al (n1) 23ff.

[22] Daniel Herbig, 'Google Assistant funktioniert jetzt auch in Deutschland mit Android Auto' (Google Assistant now also works in Germany with Android Auto) Heise Online (Hannover, 19 September 2018) <https://www.heise.de/newsticker/meldung/Google-Assistant-funktioniert-jetzt-auch-in-Deutschland-mit-Android-Auto-4167890.html> accessed 19 September 2018; Nico Jurran, 'Sprachassistenz: Fahrzeuge von Audi künftig mit Alexa' (Language assistance: Audi vehicles to be equipped with Alexa in the future) Heise Online (Hannover, 19 September 2018) <https://www.heise.de/newsticker/meldung/Sprachassistenz-Fahrzeuge-von-Audi-kuenftig-mit-Alexa-4168022.html> accessed 19 September 2018.

[23] McTear et al (n1) 62ff.

[24] StanfordLawSchool, 'Discover Legal Technology' <https://techindex.law.stanford.edu/> accessed 12 September 2018 contains a list of legal tech companies.

[25] ibid (n2); McTear et al (n1) 75ff.; see also the well-known Google translation website <https://translate.google.com>.

Furthermore, IPAs are used for various planning tasks. For example, an IPA can schedule appointments, plan trips, propose navigation for car journeys or travel on public transport and consider traffic disruptions in real time using location-based data of other mobile devices.[26]

Moreover, IPAs can also control other applications, eg applications on the user's devices such as e-mail clients, calendars or file storage. They can also control other devices such as machines in a factory or heating, light and kitchen appliances in a household.[27]

Finally, IPAs can also monitor users. They are used, for example, in the health sector to monitor certain parameters of their users, such as their heartbeat. If necessary, they communicate independently with doctors. In the automotive sector, for example, IPAs monitor users as to whether they are only partially fit for driving because of fatigue.[28]

The more powerful IPAs become and the more the evolution of autonomous systems towards AI progresses, the more powerful these personal assistants become and the more functions they will get in the future.[29]

[26] ibid (n2).

[27] Mishra (n1) 19-23, 247ff.; Nico Jurran, 'Alexa: Mikrowellen-Ofen und Wanduhr mit Sprachassistentin' (Alexa: Microwave oven and wall clock with language assistant) Heise Online (Hannover, 20 September 2018) <https://www.heise.de/newsticker/meldung/Alexa-Mikrowellen-Ofen-und-Wanduhr-mit-Sprachassistentin-4169442.html> accessed 20 September 2018.

[28] Mishra (n1) 5, 12, 15, 16, 20, 27 regarding the health sector.

[29] Mishra (n1) 25f.

4.2 Extensive Data Collection

IPAs often need to know a lot about their users. To fully realise their potential and to autonomously suggest information, they need an adequate amount of information about the user.[30] If an IPA search is to fulfil orders in a spatial context, it should know where the user is located. If an IPA wants to arrange appointments, it should get information about the calendar of the user and his or her contacts. If a trip is to be planned, the IPA should know which means of transport the user typically uses. If the IPA is to read emails, it should get access to the user's mailbox. To ensure the best possible speech recognition, the IPA should collect and process voice data to learn the user's pronunciation. In order to enable secure authentication of the user via his device, the IPA can have access to biometric data such as fingerprints or images of the iris.

These and similar features are enhanced as IPAs learns from historical data. For this reason, IPAs tend to store and evaluate a large amount of historical usage data.[31] This also results in a strong personalisation of IPAs to the respective user.

4.3 User Identification

In addition, IPAs regularly require an identification of the user by name through the provider of IPA services.[32] Theoretically, some functions could also be offered to a registered pseudonym of the user, such as 'John Doe'. However, this may no longer be sufficient

[30] Mishra (n1) 17f., 23f. describes this as the 'suggest paradigm': modern assistants are allowed to provide suggestions instead of only answering questions.

[31] Mishra (n1) 6, 23f.

[32] Mishra (n1) 30f.

if the IPA is to act on behalf of its user vis-à-vis third parties. If, for example, a ticket is to be booked for a trip or if the IPA is to send an email on behalf of its user, the user becomes identifiable to the provider of the IPA. Moreover, the IPA must also get access to payment data and bank details to be able to use payment services. Common payment services require an identification of the user by name, too.

Last but not least, users are usually identifiable because the providers of IPA services also provide other web-services[33] that require at least the use of a valid email address as an anchor date for identification, typically user's registration by name and other data like address and phone number and sometimes bank data. This applies, for example, but not only, for Apple regarding the use of their operating system iOS for Apple devices and the use of numerous applications, for Amazon with respect to the use of their marketplace, for Google regarding the use of their operating system Android and numerous other services as well as for Microsoft regarding their known operating system Windows and the use of their office applications and cloud services. They all require an identification of the user for several purposes such as the synchronisation of data and applications over several devices of the user,[34] the licensing of applications, the personalisation of their services and the providing of services against payment via app stores. By linking these data and services to IPA providers, they can easily identify their users.

[33] See for example the login areas under <www.google.com>, <www.microsoft.com> or <www.amazon.com>.

[34] Kristina Irion, 'Your digital home is no longer your castle: how cloud computing transforms the (legal) relationship between individuals and their personal records' (2015) 23 IJLIT ch 'Consumer-facing cloud services'.

4.4 Categories of Data Used by IPAs

Based on the considerations above, data that is typically used by an IPA, besides registration data, can be categorised as follows, whereby some of the categories may overlap.

4.4.1 Input Data

First of all, the IPA must be operated, for which various input data of the user is processed. For example, an IPA can be operated by entering text, by mouse, by the spoken word or by typing movements on a display with respect to tablets and smartphones with touch screen.[35]

4.4.2 Context-Dependent Data

To perform its functions, an IPA uses different context-dependent data.[36] These typically concern the location of the user, historically learned characteristics of the user, such as regularly used services or traffic routes that can be proposed by default, stored bank data and payment information, information about the user's contacts, telephone numbers, his messages such as emails, calendar entries, tasks notes – that is all the typical data of a typical personal information manager (PIM) in an office environment.[37]

4.4.3 Access Data

Furthermore, the IPA requires access to other applications, devices and networks.[38] If, for example, an email mailbox is to be

[35] Mishra (n1) 6, 16f.

[36] Mishra (n1) 4-6, 17f., 23f.

[37] ibid.

[38] Mishra (n1) 5, 6, 13, 23.

accessed, the IPA should know the credentials for accessing the mailbox. If calendar entries are to be made or changed, the IPA should get access to calendar applications. If the IPA is to read or send documents, it should get access to file storages and photo storages. In order to receive voice commands, the IPA should be allowed to activate the microphone of a device. If it is to be operated via touchscreen, it should get access to the control of the screen. If the IPA shall control the navigation and, for example, shall display it in an automobile, it should get access to the display system of the car.

The examples above show that the more powerful an IPA becomes, the more access rights it requires. The IPA tends to require access to almost all applications of the platform it is running on,[39] for example, to the cell phone's operating system and to selected other hardware, too.

4.4.4 Marketing-Related Data

Finally, regarding the marketing of usage data, data specifically required for marketing purposes is processed. This can be, for example, information about existing consent for advertising, a specific identifier (ID) to clearly identify users, although not by name then at least by an ID to be able to individually address them. Moreover, special settings of a user regarding the acceptance of marketing messages via the IPA must be taken into account.

[39] Mishra (n1) 23.

4.5 Need to Transfer Data to Data Centres

Most of the data analysed above is transferred to high-performance data centres of IPA service providers for the operation of the system. On the one hand, this is based due to the fact that providers' data centres are considerably more powerful than the devices of the users, for example, smartphones and tablets. In addition, the significant amounts of data, particularly the amount of context-related data, that needs to be processed to provide the functionality, requires large storage capacities.[40]

Central data processing in a data centre offers all the other benefits of a cloud service, too. Without going into details, these are, in particular, the possibility of being able to comprehensively recognize and use patterns and rules in large data sets using big data algorithms. Big data can be defined by the three 'Vs' volume, variety and velocity.[41] For example, user input behaviour can be better identified by comparing many similar users and situations.[42] This is important in the recognition of speech. Furthermore, services can be made available to all users based on the same technical configuration, standardised and up-to-date from a central data centre. The existing high bandwidths for data transmission make it possible to transfer large amounts of data quickly and cheaply, too.

As most providers of IPA services come from the United States, according to the companies Amazon, Apple, Google and Microsoft,

[40] Mishra (n1) 22-24, 28.

[41] See Dennis Broeders, Erik Schrijvers, Bart van der Sloot, Rosamunde van Brakel, Josta de Hoog and Ernst Hirsch Ballin, 'Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data' (2017) 33 C.L.S.Rev. 309, 310 for this and slightly other definitions; Kuschewsky (n10) s 4.10 for a list of Working Papers of the Art 29 WP regarding Big Data.

[42] Mishra (n1) 24.

these data centres are also located in third countries outside the EU or the European Economic Area (EEA). In practice, data processing takes place internationally across the globe, at least not exclusively in the Union. The same applies to the large marketing networks such as Google's DoubleClick, which are also internationally positioned and process marketing data worldwide.

4.6 Value of Personal Data for Marketing Purposes

The data processed by an IPA is not only processed to provide the functions but can also be used for advertising purposes and therefore transferred to international providers. The data of an IPA has a high financial value for marketing, too.[43] This is because IPAs, as described, process very large amounts of usage data, which are highly significant and from which many characteristics of the users are readable or can be calculated. The more characteristics of a user are known, the more extensive and in a larger context he can be advertised. The more characteristics of a user are known, the more targeted and therefore more valuable he can be advertised.[44] If it is known via an IPA which device the user uses and how old it is, then he can be advertised purposefully by his telecommunications (TC) provider for buying a new device. If the car is known that he drives, he can be offered new cars in the appropriate category. If the location is known where the user likes to eat Italian, he can be recommended Italian restaurants in his area.

[43] Tobias Enders, 'Exploring the Value of Data – A Research Agenda' [2018] LNBIP 1ff.; Malgieri (n6) 289ff.

[44] Chunlei Tang, *The Data Industry: the Business and Economics of Information and Big Data* (Hoboken, New Jersey: Wiley 2016); Enders (n43) 12.

Furthermore, data are particularly valuable because they are constantly updated and therefore of good quality.[45] IPAs are used regularly, often daily, and are constantly active on mobile devices such as smartphones.[46] In contrast to classic marketing databases, where data is collected and stored at a historical point in time, IPAs constantly transfer up-to-date data to the providers.

Finally, the usage data of an IPA is personalised and can be assigned to individual, known users.[47] This enables the exploitation and sale of the data for a personalised direct marketing.[48]

5. REQUIREMENTS UNDER THE GDPR

The GDPR is in effect since May 25th, 2018. It contains partially similar but also much stricter substantive rules than the former DPD which was replaced by the GDPR.[49] The GDPR also brings several new requirements that must be considered.

5.1 Legal Framework and Scope of the GDPR

According to Article 1(1) GDPR, the processing of personal data[50] of natural persons through controllers and processors is still the link to the application of European data protection law.[51] Besides the objective of free movement of personal data in the Union, Article 1(1) GDPR says that the GDPR 'lays down rules relating to

[45] Enders (n43) 12.

[46] Mishra (n1) 4.

[47] Mishra (n1) 23.

[48] Philipp Hacker, 'Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things' (2017) 7 IDPL chs I, III.A; Malgieri (n6) ch 4.1.

[49] Voss (n10) 223.

[50] See s 5.2; Feiler et al (n9) ch 4.1.

[51] Feiler et al (n9) ch 3.

the protection of natural persons with regard to the processing of personal data'.

The material scope[52] of the GDPR covers mainly the processing of personal data by automated means as regulated under Article 2(1) GDPR. Because of the automated processing of personal data through IPAs, the GDPR applies.

With respect to the territorial scope[53] of the GDPR, Article 3(2)(a) GDPR regulates the application of the GDPR to the processing of personal data of natural persons in the EU by companies that are not seated in the EU in case of processing activities that are related to 'the offering of goods or services, irrespective of whether a payment of the data subject is required'. Moreover, Article 3(2)(b) GDPR stipulates the application in case of activities that are related to 'the monitoring of' the data subjects 'behaviour as far as their behaviour takes place within the Union'. Finally, the EEA Joint Committee decided on 6 July 2018 to implement the GDPR into the EEA Agreement.[54] For this reason, the GDPR applies to the processing and selling of personal data even if IPA providers are seated in third countries if they offer their services to data subjects in the Union or the EEA.[55]

As any regulation in the Union, the GDPR will apply directly and without the need to transpose it in all the Member States.[56] Older national data protection laws will be superseded by the GDPR.[57]

[52] Feiler et al (n9) ch 4.1.

[53] Feiler et al (n9) ch 4.3; Kuschewsky (n10) s 1.3.5.; Voss (n10) 222f.

[54] The EEA Joint Committee, no 154/2018 (Commission Decision, 6 July 2018), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:22018D1022&from=EN> accessed 28 August 2018.

[55] Case C-131/12 *Google Spain v AEPD and Mario Costeja González* [2014] OJ C 165, 9.6.2012 regarding the former DPD if a controller sets up a branch or subsidiary in a Member State.

[56] Feiler et al (n9) ch 5.

[57] ibid.

However, there are several fields where the GDPR contains opening clauses that allow the Member States to enact own national laws.[58] In case of such a situation that becomes relevant for this study, the author will give the reader a hint.

5.2 Personal Data

The term 'personal data' is defined in Article 4(1) GDPR.[59] Thus, personal data means 'any information relating to an identified or identifiable natural person ('data subject')'. According to Article 4(1) GDPR, the data subject can be identified 'directly or indirectly, in particular by reference to an identifier [...] or to one or more factors specific to the [...] identity of that natural person.' Furthermore, the Regulation lists some typical identifiers for a direct identification, namely 'the name, an identification number, location data' and 'an online identifier'. Such online identifiers can be all unique numbers that are capable to be used to identify a user, even though third-party knowledge is needed, such as IP addresses,[60] numbers in cookies, fingerprints[61] or other unique numbers that are related to a natural person.[62] In contrast, it follows, that anonymised data are basically not subject of the provisions of the GDPR.[63]

[58] ibid.

[59] Feiler et al (n9) ch 4.1 and art 4 cmt 1ff.

[60] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] OJ C 89, 16.3.2015.

[61] Art 29 WP, 'Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting' (2014) WP224 3 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf> accessed 28 August 2018.

[62] Feiler et al (n9) art 4 cmts 4, 34.

[63] See ss 5.4.3 and 6.1.5.1; Feiler et al (n9) art 4 cmt 3.; Art 29 WP, 'Opinion 05/2014 on Anonymisation Techniques' (2014) WP216 3 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 28 August 2018.

When using IPAs, users are typically identified directly by the IPA providers because of a prior registration and by means of identifiers. Indirect identification by using one or more features is usually not required although theoretically thinkable because of the huge amount of processed data. An IPA provider not only has access to registration data, identifiers and location data but also to many different types of personal data. The input data may include biometric voice data, contextual usage data, e-mail addresses and payment data that are directly personal.[64] Access data to other applications and hardware also contain unique credentials and marketing identifiers are unique and thus by definition personal.[65]

As an interim conclusion, it follows that IPAs use personal data. The IPA provider can directly identify users with the data he processes. The same applies to marketing providers if they use unique identifiers.

5.3 Special Categories of Personal Data

Furthermore, the GDPR also deals with special categories of personal data under Article 9 GDPR.[66] Article 9(1) GDPR regulates the general prohibition of the use of special categories of personal data and defines them at the same time. Thereunder, special categories of personal data relate to the race or ethnic origin of a natural person, to political opinions, to religious or philosophical beliefs, to a trade union membership, to genetic data, to biometric data, to health data or to data relating to a person’s sex life or sexual orientation.

[64] See ss 4.2-4.4.
[65] See s 5.2.
[66] Feiler et al (n9) art 9 cmts 1ff.

With respect to IPAs, especially a processing of biometric data and possibly of health data and data on the race or the sex life of a person could be considered.

The term biometric data is defined in Article 4(14) GDPR.[67] According to this, biometric data are data obtained with special technical methods relating to the 'physical, physiological or behavioural characteristics of a natural person' and, in particular, 'which allow or confirm the unique identification'. Among other things, the regulation explicitly mentions facial images that can be qualified as biometric data only when, pursuant to recital 51, processed with 'technical means' that allow 'unique identification or authentication'. Furthermore, it is recognized that a person's voice is classified as biometric data that allows for unambiguous identification.[68] If an IPA processes voice data or facial images of the user, for example, to control the IPA or to authenticate the user, processing of special categories of personal data takes place.

Besides, biometric data could eventually be collected by IPAs with respect to instructions through typing, zooming and swiping. In several contexts, zooming, swiping and rhythm of typing could also be suitable for identification. However, today's known IPAs can usually not identify users by these data without other means.[69]

[67] See Catherine Jasserand, 'Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data' (2016) 2 EDPL 297ff.; Feiler et al (n9) art 4 cmts 32ff.

[68] Art 29 WP, 'Opinion 3/2012 on developments in biometric technologies' (2012) WP193 4, 24 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf> accessed 28 August 2018; Omer Tene, 'Privacy: The new generations' (2011) 1 IDPL 15, 21 <https://doi.org/10.1093/idpl/ipq003> accessed 6 September 2018; Veale et al (n20) 123; Jasserand (n67) 297, 299, 303.

[69] Art 29 WP (n68) speaks of 'soft biometrics, 16f, 27; Lehmbruck L, 'Neues System erkennt PC-Nutzer am Tippverhalten. Biometrie-Software ersetzt das Passwort' (New system recognizes PC user by typing behaviour. Biometrics Software replaces Password) *Handelsblatt*

Finally, data processed by IPAs could eventually contain health information. Article 4(15) GDPR defines health data as 'personal data related to the physical or mental health of a natural person [...] which reveal information about his or her health status'. Such data could be processed if it would be possible to derive excess information from biometric input data, for example, if conclusions could be drawn from the user's voice regarding his health. Excessive information might also arise as part of an authentication via facial images or iris scans of the eye.[70]

Finally, it is conceivable that an IPA processes in special situations information about a person's race and sexual orientation, for example when communicating with dating services or hospitals or when conducting searches with certain keywords.

As an interim conclusion, it should be noted that IPAs usually process special categories of personal data, too.[71]

5.4 The Principles of Article 5 GDPR

The following section presents principles of data processing set out by Article 5 GDPR. The study identifies those principles that should be taken into account when operating IPAs. The focus is on those

(Düsseldorf, 26 March 2006) <https://www.handelsblatt.com/technik/it-internet/neues-system-erkennt-pc-nutzer-am-tippverhalten-biometrie-software-ersetzt-das-passwort/2633532.html?ticket=ST-5775102-BWSlJKh50bXXpHAbYFey-ap4> accessed 8 September 2018.

[70] Art 29 WP (n68) 15, 17, 21, 23; see Jasserand (n67) 297, 299f.; 305f. to the term authentication as uses by the GDPR vs identity verification.

[71] A more futuristic, but with respect to the abilities future IPAs imaginable, special category could be digital memories, see Krzysztof Garstka, 'From Cyberpunk to Regulation – Digitised Memories as Personal and Sensitive Data within the EU Data Protection Law' (2017) 8ff. JIPITEC 293ff. <https://www.jipitec.eu/issues/jipitec-8-4-2017/ 4637> accessed 6 September 2018.

essential principles that are relevant to the subject matter of the study as described in section 3.

5.4.1 Lawfulness, Fairness, Transparency

Article 5(1)(a) GDPR contains three principles that are not necessarily related.[72] First of all, personal data must be lawfully processed. A narrow understanding of the term 'lawfully' means that there must be a sufficient legal basis for processing personal data. This would be the case if there is a legal basis within the meaning of Article 6(1) GDPR.[73] If, on the other hand, a broad understanding of the concept of lawfulness is accepted, this would require the fulfilment of all the requirements of the GDPR.[74] This would include, for example, the fulfilment of the information requirements under this principle. However, against such a broad understanding speaks the lack of contour of the term lawfulness. If the concept of lawfulness were to include all requirements, this would mean that the infringement of any of the conceivable requirements would be fined under Article 83(5)(a) GDPR.[75] A differentiated consideration as made under the GDPR would no longer be possible. In addition, the other principles of Article 5 GDPR would lose their independent regulatory content, for example, the principle of transparency.[76] Moreover, recital 40 only considers a 'legitimate basis' for a lawful processing. In this respect, it can be assumed that the principle of lawfulness is based on a narrow understanding, which states that it requires only the existence of a sufficient legal basis for data processing. Therefore,

[72] T Herbst, *DS-GVO und BDSG Kommentar* (GDPR and German Data Protection Act Commentary) (Jürgen Kühling and Benedikt Buchner eds, 2nd edn, C.H. Beck OHG 2018) art 5 para 7.

[73] Feiler et al (n9) ch 6 and art 5 cmt 1; Voss (n10) 224f.

[74] Feiler et al (n9) ch 6 and art 5 cmt 6 regarding legitimacy of the purposes; Herbst (n72) art 5 para 9.

[75] Herbst (n72) art 5 para 10.

[76] ibid.

only a legal basis is required for the fulfilment of the principle. This will be considered under section 6.2.

The principle of fairness of the data processing is difficult to grasp. Concrete evidence for what is fair is not given by the GDPR. Recital 38 of the former DPD required that the data subject should know the existence of a processing and be properly and fully informed of the conditions of the data collection. All in all, the principle of fairness, against the background of the other principles, is a catchall element that relates to other principles and applies only if no other, detailed principle applies.[77] Therefore, it is not further focused in this study.

In contrast, the principle of transparency plays a vital role in data processing using modern technologies such as IPAs.[78] In particular, secret data processing should be forbidden and data subjects should be fully informed. This is relevant because IPAs are typically always on and listen to their environment, ie to the spoken word of data subjects (and third persons).[79] These requirements have been assigned under the principle of fairness under the former DPD.[80] The principle of transparency is specified in Articles 12 to 15 GDPR[81] and also plays a role for the regulations concerning data protection by means of technology, in particular regarding the provisions of privacy by design[82] and privacy by

[77] Feiler et al (n9) ch 6 and art 5 cmt 2.

[78] With respect to location data see Caitlin Cottrill and Piyushimita Thakuriah, 'Privacy in context: An evaluation of policy-based approaches to location privacy protection' (2014) 22 IJLIT 178ff.

[79] Heise Online, 'Amazons Smart-Home-Chef: Sprach-Assistenten werden immer in Hörweite sein' (Amazon's Smart-Home boss: "Speech assistants will always be within earshot) <https://www.heise.de/newsticker/meldung/Amazons-Smart-Home-Chef-Sprach-Assistenten-werden-immer-in-Hoerweite-sein-4154044.html> accessed 28 August 2018.

[80] Herbst (n72) art 5 paras 18f.

[81] Feiler et al (n9) ch 6 and art 5 cmt 3.

[82] Veale et al (n20) 105ff.

default under Article 25 GDPR.[83] Therefore, the principle of transparency is particularly taken into account when deriving specific requirements for the design of data processing by IPAs.

5.4.2 Purpose Limitation

Article 5(1)(b) GDPR regulates the principle of purpose limitation. Thereafter, personal data must be collected for 'specified, explicit and legitimate purposes' and must not be processed in a way 'that is incompatible with those purposes'. The purposes for which data shall be processed must be determined before the collection and processing of personal data begin.[84] This determination also sets the framework in which personal data may be processed in the future.

The term 'explicit' requires that purposes are determined in a manner that is understandable to the data subject and the DPAs. If the processing is to be done for multiple purposes, each purpose must be sufficiently determined. According to the Article 29 Data Protection Working Party (Art 29 WP), it is not sufficient to provide only blanket information such as 'marketing purposes' or 'improving user's experience' as a purpose.[85]

Furthermore, the processing must be for legitimate purposes and within the limits set.[86] Therefore, according to the principle of purpose limitation, further processing and onward transfers, ie processing for an originally undetermined purpose, is only

[83] Kolah (n11) s 14.

[84] Feiler et al (n9) ch 6 and art 5 cmt 7; Art 29 WP, 'Opinion 3/2013 on purpose limitation' (2013) WP203 15 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 28 August 2018; Herbst (n72) art 5 para 31.

[85] Art 29 WP ibid (n84) 16, 52-54; Feiler et al (n9) ch 6 and art 5 cmt 4; Herbst (n72) art 5 para 35.

[86] Feiler et al (n9) ch 6 and art 5 cmt 6.

accepted by the Art 29 WP when a legitimate change of the purpose takes place. Such change of the purposes is not per se forbidden but must meet the requirements under Article 6(4) GDPR.[87]

The principle of purpose limitation has particular relevance in the context of this study as data, originally collected for the purposes of operating IPAs, shall be sold for marketing purposes in the future. The requirements for such change of the purpose will be examined later.

5.4.3 Data Minimisation

The principle of data minimisation is regulated in Article 5(1)(c) GDPR. According to this, personal data must be 'adequate, relevant and limited to what is necessary' for the purpose of the processing.[88] Thus, the principle goes beyond the mere principle of necessity, which requires that data are processed only to the extent necessary to achieve a certain purpose and that data are no longer necessary if the purpose pursued can be achieved without their processing. It contains the conceptual requirement to actively minimise the scope of a personal data processing.[89] From the principle of data minimisation, it may also follow to choose the purposes and means of data processing in such a way that processing with aggregated or anonymised data is sufficient and personal data processing is therefore inadmissible.[90] It also

[87] See s 5.5.5.

[88] Feiler et al (n9) ch 6.

[89] Herbst (n72) art 5 paras 56ff.; against the background of big data Broeders et al (n41) 316f. emphasise the need to shift regulation from the collection to analysis and use.

[90] ibid.

follows from this principle to design systems in such a way that as little personal data as possible is processed.[91]

The principle is relevant in connection with data processing by IPAs, since these assistants tend to collect and process a huge amount of data, especially a huge amount of contextual data, to be able to map detailed information on the characteristics of the user and to be able to give the best possible answers and forecasts in the communication with the user.

5.4.4 Accuracy

According to the principle of accuracy of personal data pursuant to Article 5(1)(d) GDPR, personal data must be factually correct and 'up to date'. This is accompanied by an obligation of data controllers under the said provision to take 'every reasonable step' to delete or correct personal data that are inaccurate 'without delay'.[92]

Since the data processed by an IPA is continuously updated, a lot of data tend to be up-to-date and correct. Of course, this is no guarantee to fulfil the principle since a provider of IPA services can store and process data equally inaccurately as other data processors do. It should therefore be noted that the principle is relevant for IPA providers, too. If the principle concerns the handling of the rights of data subjects, eg the right to erasure or the right to be forgotten,[93] it will not be further elaborated at this point, as these rights are not in the focus of this study due to its scope.

[91] ibid.

[92] Herbst (n72) art 5 para 60ff.

[93] Case C-131/12 *Google Spain v AEPD and Mario Costeja González* [2014] OJ C 165, 9.6.2012.

5.4.5 Storage Limitation

The principle of storage limitation in accordance with Article 5(1)(e) GDPR requires that personal data are only stored in a form that allows the identification of data subjects 'for no longer than is necessary for the purposes for which the personal data are processed'. Conversely, it follows that data storage in a form that does not allow identification is permitted without limitation, ie in particular in an anonymised form which prevents re-identification.[94]

Because of the described personalisation of IPAs, it makes no sense to store user data in a way that forbids identification of a user. For the functioning of an IPA, data will be stored in a way that allows identification. There are many registration and context data which allow the provider an identification and the IPA uses those data to work properly. Therefore, anonymisation makes no sense at this stage. After the functionality has been provided, identification is no longer mandatory, and it is no longer necessary to keep the data in a form that permits identification. However, this could be different with respect to certain marketing measures. Therefore, this principle is relevant for the further examination.

5.4.6 Integrity and Confidentiality

The principle of integrity and confidentiality of personal data, as set out in Article 5(1)(f) GDPR, requires 'appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage'. Adequate security shall be guaranteed by appropriate

[94] Feiler et al (n9) ch 6; Herbst (n72) art 5 para 66.

technical and organisational safeguards. The principle therefore refers to the principle of lawfulness and the necessary measures according to Article 32 GDPR and regulates the material protection goals of technical data security.[95] Article 32 GDPR addresses all the classic IT security protection goals, even if they do not rely directly on data protection goals like the availability and authenticity of data.[96] However, confidentiality and integrity of data are explicitly required.

With respect to IPAs, this principle is important to especially protect the huge amount of personal data and the access credentials to other applications. Insofar as the confidentiality of personal data must be considered, this goal of protection must also be considered in the context of the secrecy of telecommunications. This applies to all transferred data like emails or Voice over IP (VoIP) data, especially to the spoken word.

5.4.7 Accountability

The principle of accountability under Article 5(2) GDPR has two components. On the one hand, data controllers are responsible for the compliance with the said principles of paragraph 1. On the other hand - and this is particularly new - they must be able to demonstrate this compliance under the second paragraph.[97] This could lead to a factual duty of proof to relieve the burden.[98] This principle leads to a considerable tightening of the compliance and documentation requirements for controllers and must therefore be considered for IPA providers, too.

[95] Kolah (n11) s 13.

[96] Feiler et al (n9) ch 6 and art 5 cmt 11.

[97] Feiler et al (n9) ch 6 and art 5 cmts 12-14.

[98] Feiler et al (n9) ch 6 and art 5 cmts 12-14 say that shifting the burden would not be compliant with the presumption of innocence.

5.5 Legal Basis under Article 6 GDPR

In addition to the principles of data protection law under Article 5 GDPR as discussed before, the legal bases for the operation of an IPA, the international data transfer to a third country and the sale of personal data for marketing purposes must be identified. The need for a legal basis arises from the principle of lawfulness set out in Article 5(1) GDPR.[99] Even more clearly, this follows from Article 6(1) GDPR, according to which the processing of personal data is forbidden and only legal if at least one of the paragraphs regulated in Article 6(1) GDPR applies.

For the data processing by IPAs within the framework discussed, the following legal bases come particularly into consideration.

5.5.1 Consent

Processing of personal data is permitted as a direct consequence of self-determination[100] if the data subject has consented thereto in accordance with Article 6(1)(a) GDPR. The consent must refer to one or more specific purposes. Blanket consent to all possible purposes that cannot be clearly determined at the time of the consent is inadmissible.[101]

[99] Feiler et al (n9) ch 6 and art 5 cmts 1; Kuschewsky (n10) s 3.

[100] Albrecht et al (n8) ch 3.C, para 37; critical of a consent in today's distributed IT environment López (n6) 35ff.; for the history of consent and its dogmatic background see Eleni Kosta, *Consent in European Data Protection Law* (Leiden, Boston: Martinus Nijhoff, 2013).

[101] Art 29 WP, 'Guidelines on Consent under Regulation 2016/679' (2018) WP259 rev.01 4, 10f. <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed 28 August 2018; Feiler et al (n9) ch 7.2 and art 5 cmt 3; B Buchner and T Petri, *DS-GVO und BDSG Kommentar* (GDPR and German Data Protection Act Commentary) (Jürgen Kühling and Benedikt Buchner eds, 2nd edn, C.H. Beck OHG 2018) art 6 para 20; B Buchner and J Kühling, *DS-GVO und BDSG Kommentar* (GDPR and German Data Protection Act Commentary)

Further conditions of consent are set out in Article 7 GDPR. According to Article 7(1) GDPR, the controller must prove that he has received the consent of the data subject.[102]

If consent is to be given in written declaration that also covers other issues, the request must be made in ‘in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language’ in accordance with Article 7(2) GDPR. If this is not the case, the parts of the consent affected by it are not binding.

In accordance with Article 7(3) GDPR, the data subject has the right to withdraw his or her consent at any time with future effect. The data subject must be informed of this before giving consent.[103]

Of particular importance is the strict prohibition of making a contract conditional on the data subject's consent to the processing of personal data, which was introduced by Article 7(4) GDPR.[104] To answer the question of whether consent has been given voluntarily, the controller must take the greatest possible account of whether, amongst others, the fulfilment of a contract has been made ‘conditional on consent to the processing of personal data that is not necessary’ to fulfil said contract. Therefore, personal data that is not required for the fulfilment of a contract may not be linked to a mandatory consent. This raises the question of whether and to what extent a business model in

(Jürgen Kühling and Benedikt Buchner eds, 2nd edn, C.H. Beck OHG 2018) art 7 paras 61ff.; Kuschewsky (n10) s 3.1.

[102] Feiler et al (n9) art 5 cmt 2.

[103] Feiler et al (n9) ch 7.2 and art 5 cmt 5.

[104] Feiler et al (n9) ch 7.2 and art 5 cmts 7-11.

which personal data is paid against receipt of a service will remain permissible in the future. This is particularly relevant for free IT services like IPA services where the user pays with his data.

While it is sometimes assumed that the processing of unnecessary personal data based on consent in such situations is generally no longer allowed,[105] others rely on the extent to which the voluntariness of consent by such a business model is affected.[106] Based on the wording of Article 7(4) GDPR ('utmost account'), it is to be assumed that the legislature intended to protect the voluntary nature of consent by the provision but did not want to totally undermine the self-determination of the data subjects. In this respect, a voluntary consent to the processing of unnecessary data can be achieved, inter alia, by giving a data subject the right to freely choose whether to pay with his or her data or, alternatively, to pay a certain fee.[107] The value of the data and the alternative remuneration should be essentially the same, so that the data subject has a genuine freedom of choice without being forced, for financial reasons, to consent to the disclosure of personal data.[108]

In addition, the processing of special categories of personal data, such as biometric voice data or facial images, may require consent to be given.[109] In principle, Article 9(1) GDPR prohibits the processing of special categories of personal data but allows

[105] Malgieri (n6) ch 6.

[106] Albrecht et al (n8) ch 3.C, paras 40-44.

[107] Feiler et al (n9) ch 7.2 and art 5 cmts 9-11; Albrecht et al (n8) ch 3.C, para 44; R Steidle, *Datenschutz im Internet, Rechtshandbuch zu DSGVO und BDSG* (Legal Handbook on GDPR and German Data Protection Act) (Silke Jandt and Roland Steidle eds, NOMOS 2018) ch B.III, para 176.

[108] Albrecht et al (n8) ch 3.C, para 44 demands such an adequate exchange rate without saying how to calculate in practice.

[109] Art 29 WP, 'Opinion 02/2012 on facial recognition in online and mobile services' (2012) WP192 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf> accessed 28 August 2018; Art 29 WP (n68) 10.

processing on the basis of, among others, explicit consent in accordance with paragraph 2(a).[110] It should be noted, however, that the Member States may maintain the prohibition under their national laws or make processing subject to further conditions in accordance with paragraph 4, including further restrictions. Apart from consent, no other legal basis is plausible which permit the processing of special categories of personal data within the scope of the subject-matter of this study. In particular, it will generally not be possible to assume that data processed by IPAs has obviously been made public by a user before, which would permit processing in accordance with Article 9(2)(e) GDPR.

5.5.2 Performance of a Contract

Pursuant to Article 6(1)(b) GDPR, the necessary processing of personal data is permitted for the 'performance of a contract to which the data subject is party'. Processing is also necessary for the implementation of pre-contractual measures if the data subject has requested them.[111]

Within the framework of this provision, necessary data processing between a controller and its users is permissible, but not a further processing that is not necessary to fulfil the contract or an unnecessary processing between a controller and its other business partners, eg for newly introduced marketing purposes. However, data processing is strictly limited to the extent necessary for contract performance. This means that data processing which, for example, is just practical or wise from the point of view of the provider, but which is not necessary for the fulfilment of the contract, cannot be based on this legal basis.[112]

[110] Feiler et al (n9) ch 7.1.

[111] Feiler et al (n9) ch 7.1.

[112] See s 5.4.3.

5.5.3 Legitimate Interests

However, such and other data processing may be permitted based on Article 6(1)(f) GDPR. According to this provision, processing may be permitted to the extent necessary to follow the 'legitimate interests' of the data controller, but also of a third party, eg one to whom data are transmitted, provided that the conflicting 'interests or fundamental rights and freedoms of the data subject which require protection of personal data' do not prevail.[113] Consequently, it is not sufficient that the processing of data serves a legitimate interest alone. Moreover, it is necessary to weigh up the interests of the data subject against those of the controller or a third party.

In particular, the interests of the data subject predominate according to this regulation, if the data subject is a child. In principle, a child is defined as any person up to the age of 18, as stated in the proposal of the commission for a GDPR in Article 4(18),[114] based on the definition of Article 1 of the UN Convention on the Rights of the Child.[115] However, the age of the child can be considered in the context of the concrete weighing of interests with respect to the use of an IPA. Regarding Article 8(1) GDPR, the age limit of 16 years is of high importance because below this limit there is a special need for protection. It can be assumed, that personal data of a child of 16 years that consented in an IPA service can be processed under this provision, too.[116] However,

[113] Feiler et al (n9) ch 7.1 and art 6 cmts 7-9.

[114] Proposal of the European Commission for a GDPR, Draft COM(2012) 11 final.

[115] Convention on the Rights of the Child of 20 November 1989; Buchner et al (n101) art 6 para 155.

[116] Feiler et al (n9) ch 7.1 and art 6 cmt 9.

Article 8(1) GDPR allows the Member States to provide by law for lower age not below 13 years.

Furthermore, recital 47, which, unlike the articles of the GDPR, does not constitute binding law but, according to the case-law of the European Court of Justice (ECJ), can be used as an indication for the interpretation of statutory provisions, provides indications as to whether the controller has a legitimate interest or not.[117] Recital 47, first sentence, also says that the legitimate interests may be those of a controller to whom personal data is disclosed as well as the interests of third parties. This means that, unlike under Article 6(1)(b) GDPR, Article 6(1)(f) GDPR could eventually be a basis for the transfer of data by an IPA provider to its advertising third-party business partners.

In addition, the reasonable expectations of the data subject, based on his or her relationship with the data controller, must be taken into account when weighing up interests pursuant to recital 47.[118] The recital further states that a legitimate interest may exist, for example, if there is a 'relevant and appropriate relationship between the data subject and the controller', eg if the data subject 'is a client or in the service of the controller'. Therefore, in the context of a customer relationship, assuming a reasonable expectation, more data processing based on legitimate interests tends to be permissible than in the relationship of the data subject to third parties unknown to the data subject.

In this context, the question arises as to what criterion should be set for the existence of 'reasonable expectations'. Starting from the wording, an objectification must be made by the fact that the

[117] Case C-461/13 *Bund für Umwelt und Naturschutz Deutschland e.V. v Bundesrepublik Deutschland* [2015] ECR I-433.

[118] Feiler et al (n9) ch 7.1 and art 6 cmt 8.

expectations must be 'reasonable'.[119] Independent of the subjective perception of the data subject, the expectations must be impartial and reasonable. Furthermore, the recital refers to the concrete situation in which data are processed, ie sentence 3 to the expectations ‘at the time and in the context of the collection’ and sentence 4 to the ‘circumstances’ of data collection. This makes it clear that an assessment on an individual basis must be carried out.[120]

In addition, the recital contains a dynamic component, as users' expectations change over time.[121] Changes in living conditions and existing technologies change users' expectations. This raises the question of whether and if so, how the reasonable expectations of a data subject can be influenced, for example by providing transparent information by the controller. In fact, expectations are influenced by information and, based on the dynamic component of expectations; it should also be possible to influence them to a certain extent with legal effect. Thus, this should not be understood as a free ticket to raise expectations through extensive information on all possible data processing with the result that every data processing becomes legitimate.[122] Against this background, the objective criterion of ‘reasonability’ has a restrictive meaning. However, it should be noted that the reasonable expectations of the user of an internet technology depend on each individual case but can be influenced to some extent.

Furthermore, recital 47 mentions in sentence 7 direct marketing as a possible legitimate interest for the processing of personal

[119] ibid.

[120] Buchner et al (n101) art 6 para 147; Steidle (n107) ch B.III, para 361.

[121] Tene (n68) 15ff.; Steidle (n107) ch B.III, para 362.

[122] ibid.

data. Direct marketing means any form of advertising in which the recipient of the advertising is addressed individually and directly.[123]

Finally, data subjects may object such processing pursuant to Article 21 No. 2 GDPR at any time.[124]

5.5.4 Compliance with a Legal Obligation

Another legal basis that can be relevant in connection with the fulfilment of data protection obligations by IPA providers can arise under Article 6(1)(c) GDPR. It states that the processing of personal data is legal if it is necessary for the fulfilment of a legal duty of the controller. The provision that contains this duty can then be regarded as the legal basis.[125]

Regarding the principles of integrity and confidentiality discussed above, the IPA provider is subject to such a duty which results from Article 32 GDPR.[126] Article 32 GDPR obliges the responsible controller regulating a risk-based approach to implement appropriate technical and organisational safeguards to secure data processing.[127]

5.5.5 Change of the Purpose

Where personal data collected for a particular purpose are to be processed and used for another purpose, Article 6(4) GDPR stipulates that this must be done either on the basis of consent, a provision of a Member State law or that the processing for the new

[123] Buchner et al (n101) art 6 para 175; Steidle (n107) ch B.III, para 162.

[124] Kuschewsky (n10) s 4.9.

[125] Feiler et al (n9) ch 7.1 and art 6 cmt 3.

[126] Steidle (n107) ch B.III, para 306.

[127] Feiler et al (n9) art 32 cmt 2; Kolah (n11) s 13, 15.

purpose must be 'compatible' with the original purpose.[128] In the last context, paragraph 4(a)-(e) of Article 6 GDPR establishes five requirements which the data processor must consider when determining whether the purposes can be assumed compatible. It states, inter alia, that the 'link between the purposes' must be taken into account, the 'context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller', the 'nature of the personal data', the 'consequences of the intended further processing for data subjects' and the 'existence of appropriate safeguards which may include encryption or pseudonymisation'. Moreover, data subjects must be informed before regarding Article 13(3) GDPR. On this basis and within narrow limits, constellations might be conceivable in a customer relationship between a user and an IPA provider, in which data collected by the provider could also be processed for other compatible purposes.

5.5.6 Data Transfers to Third Countries

The processing of personal data by IPAs does not end at the borders of the European Union but takes place in third countries such as the United States, too.[129] While the GDPR has led to further harmonisation of data protection law within the Union, which only permits minor national derogations and specifications based on opening clauses in the regulation, there is – a priori – no adequate level of data protection as defined by the GDPR in most third countries.[130]

[128] Feiler et al (n9) ch 7.1 and art 6 cmts 12-18.

[129] See s 4.5; Lingjie Kong, 'Data Protection and Transborder Data Flow in the European and Global Context' (2010) 21 EJIL 441f. <https://doi.org/10.1093/ejil/chq025> accessed 2 May 2018.

[130] Feiler et al (n9) art 45 cmt 13, Kolah (n11) s 19 and Kuschewsky (n10) s 7.1 contain a list of countries with an adequacy decision.

However, according to the marketplace principle of Art 3(2) GDPR, the GDPR also applies if IPA providers just offer their services to data subjects in the Union or the EEA. As described earlier, a separate branch in the Union is not required for the application of the GDPR.[131] Whether the transfer of data to a third country is permissible or not, is determined within the framework of a two-stage examination. The first step is to check whether a substantive legal basis within the meaning of Articles 5 and 6 GDPR permits the processing.[132]

The second stage is to check whether the data transfer to a third country is permitted. The data exporter in the Union must fulfil all the additional requirements of the fifth chapter of the GDPR, as stipulated in the first sentence of Article 44 GDPR.[133] Moreover, sentence 1 says that the requirements of the GDPR also apply if the data importer in the third country further outsources the data, so-called onward transfers.[134] On the second stage, permissible data transmissions to a third country require that there is an adequate level of data protection at the data importer. This can result from various regulations and safeguards.

First, there are third countries for which the European Commission has generally recognised an adequate level of data protection pursuant to Article 45 GDPR.[135] These adequacy decisions of the Commission will continue to apply in the future pursuant to paragraph 9 of this provision. The decisions include, among others, the countries of the EEA.[136] There are a number of other third countries with an adequate level of data protection that has

[131] See s 5.1.

[132] Feiler et al (n9) ch 18 and art 44 cmt 5; Kolah (n11) s 19.

[133] ibid; Kuschewsky (n10) s 7.2.

[134] Kuschewsky (n10) s 7.1.

[135] ibid (n130).

[136] ibid (n130).

been recognised by the Commission, too.[137] For some of them, the appropriate level of data protection has just been recognised for special sectors in the country concerned, such as for the private sector in Canada.

Another possibility, especially for transfers to the USA, is that the data importer has joined the EU-US Privacy Shield as part of a voluntary commitment.[138] However, an action is pending before the ECJ against the adequacy decision of the Commission regarding the EU-US Privacy Shield.[139]

A further possibility for legalising third country transfers is to establish an adequate level of data protection through appropriate guarantees in accordance with Article 46(2) GDPR.[140] Around modern cloud technologies, this is, in particular, the possibility of achieving an appropriate level of data protection by concluding the EU standard contractual clauses[141] with the data importer. These clauses contain both obligations of the data importer, which do not exist according to his state law, as well as certain rights for the data subjects and the DPAs of the Union. Other possibilities, such as binding corporate rules or approved rules of conduct, are, however, not relevant in the context of the subject-matter of this study.

[137] ibid (n130).

[138] Feiler et al (n9) ch 18.1 and art 45 cmt 13; Martin Weiss and Kristin Archick, 'U.S. - EU Data Privacy: From Safe Harbor to Privacy Shield' (2016) Congressional Research Service 1ff. <https://fas.org/sgp/crs/misc/R44257.pdf> accessed 2 May 2018; Voss (n10) 231f.

[139] Case T-670/16 *Digital Rights Ireland v Commission* [2016] ECLI:EU:T:2017:838; the previous Safe Harbour Agreement was held invalid in 2015, see Case C-362/14 *Schrems v Data Protection Commissioner* [2015] 2 CMLR 2; for further criticism see Weiss et al (n138) 12-14.

[140] Feiler et al (n9) ch 18.1 and art 46 cmts 6-18.

[141] Feiler et al (n9) ch 18.1 and art 46 cmts 10-14.

In addition, there are some exceptions for which the existence of the consent of the data subject pursuant to Article 49(1)(a) GDPR must be particularly considered. If a data subject consents to transfers in a third country and has been informed of the specific risks of the lack of an adequacy decision of the Commission and the lack of appropriate safeguards, his or her consent may justify the transfer of data, too.[142]

6. DERIVING CONCRETE OBLIGATIONS FOR PROVIDERS

Based on the requirements of the previous section 5 that were identified as relevant within the scope of the subject-matter of this study, concrete implementation proposals and regulatory proposals for providers of IPA services can be derived to comply with the respective GDPR requirements.

6.1 Obligations Arising under the Principles of Article 5 GDPR

First, concrete implementation proposals based on the relevant data protection principles will be derived.

6.1.1 Transparency

The information that must be provided based on the transparency principle[143] of Article 5(1)(a) GDPR can be found in Articles 13 and 14 GDPR. These Articles specify the content that must be disclosed to the data subject when data is collected.[144] Since the IPA Provider collects data directly from the data subjects using their devices, Article 13 GDPR is relevant. For the provision of

[142] Feiler et al (n9) ch 18.1 and art 49 cmts 6-8.

[143] See s 5.4.1.

[144] Feiler et al (n9) ch 8 and art 13 cmts 1ff. and art 14 cmts 1ff.

information outside the scope of Article 13 GDPR, for example in the context of a self-disclosure under Article 15 GDPR, the following proposals on the implementation could apply accordingly.

6.1.1.1 Time and Form of the Information

Article 13 requires the information to be provided at the time it is collected.[145] Therefore, the IPA providers must inform the users before the service begins, for example in the registration process. If new functions are introduced, the data subject must be informed before the operation, too.

Moreover, the user must be informed compliant to Article 12 GDPR in 'a concise, transparent, intelligible and easily accessible form, using clear and plain language'. There is a conflict of objectives in conveying the information in a concise, intelligible form as well as through plain language but at the same time transparent regarding the whole processing.[146] However, these conflicting requirements must not result in a lack of the obligatory content pursuant to Article 13 GDPR.

When collecting data via IPAs, it is difficult to explain the technical complexity of the system, the international data transmission and the subsequent marketing of some usage data in an understandable manner and transparent at the time of the data collection. In addition, IPAs are often used via mobile devices[147] that only have small displays or even via devices that are only

[145] Feiler et al (n9) ch 8 and art 13 cmt 3; Art. 10(2) EPR contains a similar obligation that requires early information when software is installed.

[146] M Bäcker, *DS-GVO und BDSG Kommentar* (GDPR and German Data Protection Act Commentary) (Jürgen Kühling and Benedikt Buchner eds, 2nd edn, C.H. Beck OHG 2018) art 12 para 12.

[147] See s 4.1.

operated via voice. In these cases, the question arises as to how the extensive information obligations under Article 13 GDPR are to be fulfilled at the time of the data collection. Thus, the complexity of a technology or a business model must not lead to a reduction in the legal transparency requirements. Therefore, all requirements of the transparency principle must be fulfilled for the processing of personal data by IPAs.[148] These can be implemented as follows.

6.1.1.2 Layered Information Model

One possibility for the implementation is to point out less but fundamental and important information to the data subjects in a first step and to link the complete information to a website. Such a media discontinuity between the information given by the IPA and a website that displays the information in a web browser is permitted following the Art 29 WP. In its working paper WP260 the Working Party stresses that in a first step it may be sufficient to provide information on the 'identity of controller', 'details of the purposes of processing', a 'description of the data subject's rights' and information on those things which have the greatest influence on the data subject.[149] The Working Party understands this in a way that the data subject can understand the consequences of the data processing and to 'avoid information fatigue'.[150] As a result, IPA providers can offer only this important information in a first step and link the full information on a website or another text that is implemented in the IPA application.

[148] Feiler et al (n9) ch 8.

[149] Art 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260 rev.01 paras 8, 11, 17, 24, 35-37 <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id= 622227> accessed 28 August 2018; Feiler et al (n9) ch 8 and art 12 cmt 1.

[150] Art 29 WP (n149) para 35.

6.1.1.3 Providing Detailed Information only on Request

The requirements of giving the information in an intelligible form and plain language can also be fulfilled by providing the user at an upper level with initial, simple information in the form of headings and brief texts, maybe read by the IPA, which he can deepen by clicking, typing or by asking for further information. It is possible to provide the data subject with 'tailored information'[151] and more information than required in Article 13 GDPR through such additional tools.

6.1.1.4 Voice Control and Push Messages

Using voice control, it is also possible to read out parts of the information to the data subject and to link for the full information to a website or to make the link available by means of a short message. The Art 29 WP also assumes that information can be made available to the data subject by means of a push message.[152]

6.1.1.5 Using Standardised Icons

Furthermore, Article 12(7) GDPR allows providing the information according to Article 13 GDPR 'in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing'.[153] Moreover, it requires that electronically presented icons are machine-readable. Although such standardised icons do not exist by now because the process of standardisation requires

[151] Art 29 WP (n149) para 37.

[152] Art 29 WP (n149) para 39.

[153] Feiler et al (n9) ch 8 and art 12 cmts 11, 12.

delegated acts of the Commission under Article 12(8) GDPR that also do not exist, IPA providers could add such symbols in the future to provide an intelligible and clearly legible overview on an upper level instead of written headings like proposed above.

6.1.1.6 Privacy Dashboard

A further possibility to provide the data subject with comprehensive transparency is to offer a special user area in the backend in which the information stored can be viewed, explained, rectified and deleted. For example, Microsoft’s Cortana assistant pursues this approach and allows that certain usage data can be viewed and deleted in the backend system.[154] In a corresponding manner, IPA providers can offer privacy dashboards for registered users to provide all the information required under Article 13 GDPR as well as further information that is not obligatory.[155]

6.1.1.7 Traceable Switch-Off of Sensors

Transparency is also important regarding other natural persons whose data might be collected, eg friends or colleagues of a user who talk beneath a listening IPA. To avoid secret data collection, it must be possible to switch off the sensors.[156] This should be made traceable to other persons, eg by standardised symbols or by emitting a signal to other devices that cannot be forged.

[154] See Microsoft, ‘Cortana and Privacy - How to Control Cortana’s Collection and Use of Your Data‘ (2018) <https://privacy. microsoft.com/en-us/windows-10-cortana-and-privacy> accessed 10 September 2018.

[155] Art 29 WP (n149) para 39; Mishra (n1) 30; Veale et al (n20) 105, 115ff.

[156] See s 5.4.1; Art 29 WP (n149) para 39; Mishra (n1) 30.

6.1.2 Purpose Limitation

The principle of purpose limitation[157] under Article 5(1)(b) GDPR prohibits the provider from using data collected to operate the IPA for marketing purposes. It could be implemented as follows:

6.1.2.1 Separate Legal Basis for Marketing Purposes

If the IPA provider plans to sell usage data for marketing purposes, he must consider a legal basis at an early stage. This can be done best at the time of the data collection, as otherwise only a retroactive consent could legitimise a change of purpose.[158]

6.1.2.2 Separate Data Storage

Data that is only used to operate the IPA should be able to be separated from other data for future marketing purposes. It could be marked to be able to differentiate stored data regarding the purposes of its processing. This ensures that data that are subject to different purposes are not mixed by IPA providers and can be treated separately.

6.1.3 Data Minimisation

The principle of data minimisation[159] of Article 5(1)(c) GDPR, according to which personal data must be 'appropriate, relevant and limited' to the necessary extent for processing, could be implemented in IPA systems as follows:

[157] See s 5.4.2.

[158] See ss 5.5.1 and 5.5.5 whether a legal basis or compatible purposes under Article 6(4) GDPR are available.

[159] See s 5.4.3.

6.1.3.1 Considering the Need of Personal Data

It may seem reasonable or desirable to collect a huge amount of personal data for a future processing, for example for big data analysis or an extensive marketing of usage data; however, this does not justify collecting unnecessary data in stock without an existing legal basis just to have it available later. Though, against the background of big data technologies, it becomes more and more difficult to draw the line between an unnecessary and a necessary data collection. IPAs need a lot of context data to improve functions like recognition of speech or recommendations to the user.[160] Sometimes providers find correlations between data that can be used to develop new functions that have not been thought about at the time of the data collection. Although anti-discrimination of algorithms[161] could have been a better answer of the law to the challenges of such analysis than the well-known requirement of data minimisation, IPA providers must respect data minimisation. They should implement a company process for the development of IPAs to clearly justify the purposes of collecting data and to use as less data as possible to achieve these purposes. The line towards an unnecessary data collection would be data retention, ie collecting data without any concrete purpose.

6.1.3.2 Privacy by Design and Pseudonymisation

A corresponding design requirement for the product development arises directly from Article 25 GDPR, which regulates the requirements of privacy by design and privacy by default.[162] According to paragraph 1, appropriate technical and

[160] See s 4.4.

[161] Broeders et al (n41) 317f.; Hacker (n48) ch V.C.; Hermstrüwer (n6) 12-16.

[162] See s 5.4.1.

organisational measures must be taken to comply, explicitly, with the principle of data minimisation. Paragraph 1 relates in particular to measures of pseudonymisation. As a result, IPA providers should check whether personal data is required or whether certain purposes can be achieved with data that has been pseudonymised. Pseudonymised data could be, for example, sufficient to recognise[163] a device or user for sending marketing messages that rely on the user's interests without the need for identification by name.

6.1.3.3 Privacy by Default

An IPA system should be preconfigured in such a way that data processing that is not absolutely necessary for the operation is deactivated. According to Article 25(2) GDPR, the principle of privacy by default[164] includes the amount of personal data that is collected, the scope of its processing, the storage time and the possibility to access data. This is in contrast to the usual procedure of the developers to activate functions so that the users use them and get familiar with them immediately.[165] With respect to this, IPA providers should consider means to make new functions and data processing both interesting and transparent to users so that they understand and activate them if desired.

Moreover, Article 25(2) GDPR requires in particular that 'personal data are not made accessible without the individual's intervention to an indefinite number of natural persons'. This would be the case, for example, if an on-off switch in an IPA's privacy dashboard would be activated from the beginning that allows usage data to

[163] See s 6.1.5.1.

[164] See s 5.4.1.

[165] J Hartung, *DS-GVO und BDSG Kommentar* (GDPR and German Data Protection Act Commentary) (Jürgen Kühling and Benedikt Buchner eds, 2nd edn, C.H. Beck OHG 2018) art 25 paras 24-26.

be transferred to a third country for purposes of selling them to marketing networks. Other bad examples would be activated on-off switches for the collection of location-based user data or the permanent listening of an IPA's microphone or photo lenses to collect context data and to receive instructions.

6.1.4 Accuracy

The principle of the accuracy of personal data[166] under of Article 5(1)(d) GDPR could be implemented by the providers of IPA Services as follows:

6.1.4.1 User Area for an Own Data Management

The providers of IPA services could make a user area available, for example in a privacy dashboard as described above,[167] in which users can check, rectify and delete some data themselves - provided it does not prevent the IPA from functioning if termination of the user contract is not desired. Since users typically have to register by name as described above, there is usually a backend for authorised users with various configuration options anyway. Similar technologies are known, for example, for the management of cookies in a web browser,[168] which a user can display and delete if necessary, or for the control and enrolment of fingerprints for authentication on a device.[169] As a result, IPA providers should check whether they can give their users control

[166] See s 5.4.4.

[167] See s 6.1.1.6.

[168] Microsoft, 'Delete and Manage Cookies' (2017) <https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies> accessed 10 September 2018.

[169] Microsoft, 'Enrolling a Fingerprint' (2018) <https://docs.microsoft.com/en-us/xamarin/android/platform/fingerprint-authentication/enrolling-fingerprint> accessed 10 September 2018.

over certain usage data in a special user area and in a user-friendly manner.

6.1.4.2 Easy Way to Contact the Provider, Information Refresh

In addition, IPA providers should provide users with a simple possibility to contact them to apply for updating, rectification or deletion of personal data. In this context, an 'information refresh' as described by the Art 29 WP[170] should also be borne in mind, for example, a refresh from time to time regarding stored data of the user by means of a push message to give the user control over his data. In this context, IPA providers should also ask data subjects at regular intervals to check their data whether they are correct or must be updated.

6.1.5 Storage Limitation

The principle of storage limitation of Article 5(1)(e) GDPR could be implemented by IPA providers as follows:

6.1.5.1 Early Anonymisation and Pseudonymisation

With a view to marketing measures, a differentiation between the types of marketing measures could be made.

For some marketing measures, it is sufficient if user data is anonymised, ie that the personal reference is removed irrevocably.[171] Anonymised data could be sufficient, for example, for a statistical evaluation of which user groups are interested in

[170] Art 29 WP (n149) para 32.

[171] Art 29 WP, 'Opinion 05/2014 on Anonymisation Techniques' (2014) WP216 3, 5ff. <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 28 August 2018.

what advertising prior to a marketing campaign. It is also sufficient if all IPA users get the same advertising without any customising, comparable to banner advertisement on websites.

Other marketing measures can be carried out by advertisers, ie buyers of usage data, if data is pseudonymised. For example, it might be sufficient to address the advertised IPA user in a targeted manner if the user can be assigned to certain interests via a unique ID without further, name-identifying characteristics being used in addition. Depending on whether or not such pseudonymised data is considered personal data, a legal basis is required or not.[172]

However, in view of the requirements of a future EPR, which cannot be addressed in detail in the context of this study and which is only available in various draft versions at the time of this study, it can be assumed that marketing identifiers to be used for third party marketing measures, such as cookies, shall require a specific legal basis following Articles 8, 16 EPR. Nevertheless, pseudonymisation serves to fulfil the principle of data minimisation and, therefore, makes sense any way.

In the event of a personal contact with the IPA user, as often occurs in the field of direct marketing, data must be stored for as long as the purpose of direct marketing shall be achieved. In this case, however, it is necessary to legitimise a long-term storage and use for advertising purposes on a legal basis. This is dealt with separately below.[173]

[172] The question of whether pseudonymized data is personal under the GDPR is highly controversial and leads too far in the conduct of this study. See for example Feiler et al (n9) art 4 cmts 3, 4, 7, 8.

[173] See s 6.2.

6.1.5.2 Rules for Deletion of Data

Similarly and in connection with the principles of data minimisation and accuracy, it follows from the principle of storage limitation that personal data that is no longer required for the operation of the IPA must no longer be stored as personal data. This is accompanied by the obligation of the IPA providers to delete or anonymise personal data as described above.[174] This presumes that it is known when certain data is no longer needed to be processed appropriately. Therefore, IPA providers are required to categorise different data types regarding the purpose of processing and to implement a concept of deletion rules based on each category of data.[175]

6.1.6 Integrity and Confidentiality

The data protection principle of integrity and confidentiality[176] under Article 5(1)(f) GDPR is important because of the amount of used data, the use of special categories of personal data and the access rights of the IPA to other applications, hardware and networks. It could be implemented by IPA providers as follows:

6.1.6.1 Use of Electronic Signatures

The Integrity of user's electronic data and their usage data could be achieved by implementing electronic signatures.[177] To create

[174] Feiler et al (n9) ch 6 and art 5 cmt 10.

[175] V Hammer, *Datenschutz im Internet, Rechtshandbuch zu DSGVO und BDSG* (Legal Handbook on GDPR and German Data Protection Act) (Silke Jandt and Roland Steidle eds, NOMOS 2018) ch B.IV, paras 180, 190ff.

[176] See s 5.4.6.

[177] Kolah (n11) s 15; S Jandt, *DS-GVO und BDSG Kommentar* (GDPR and German Data Protection Act Commentary) (Jürgen Kühling and Benedikt Buchner eds, 2nd edn, C.H. Beck OHG 2018) art 32 para 19.

an electronic signature, a compressed hash-value, a so-called fingerprint, is generated from an electronic file, which is thereafter encrypted with a user's private key. This private key is linked with a public key that is generally known, so anyone who can open a hash-value encrypted in such a way knows that it is authentic and originates from the holder of the private key. If the decrypted hash-value then corresponds to the hash-value that the recipient can create from the original electronic file itself using the known and public hash function, it is clear that the original file has not been changed.[178] For this reason, IPA providers should implement electronic signatures to protect the integrity of important user data as well as of several usage data, at least of usage data that is stored for a longer time.

6.1.6.2 Secure Storage and Limited Access Rights

Another way to protect such data is a secure data storage that prevents unauthorised third persons from access.[179] IPA providers should implement well-known measures of data security considering the state of the art as required by Article 32(1) GDPR to protect stored personal data like all other controllers.

Furthermore, they should limit access rights following the need to know approach that arises from the principle of data minimisation, too. This prevents from too many persons of the IPA provider being capable of accessing personal data and eventually violating their integrity.

[178] DocuSign, 'Understanding digital signatures. What is a digital signature, and how can you create one?' (2018) <https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq> accessed 14 August 2018.

[179] Kolah (n11) s 15.

6.1.6.3 Transmission Encryption

Confidentiality could be achieved by means of encryption.[180] The GDPR addresses the encryption on several occasions.[181] The confidentiality of data transmission, for example from the user's device to the servers of the IPA provider and in particular during a login or authentication process, can be ensured by means of encryption. Transmission is usually encrypted using SSL or TLS encrypted connections.[182] In a web browser, such encryption would be recognizable by the fact that it displays 'https' in the address line and possibly an icon of a lock. The IPA should also encrypt data transmissions by default and make this transparent to the user, for example using a symbol. It could also offer several options for an encryption in the privacy dashboard.

6.1.6.4 Encrypted Data Storage

Not only the data transmission but also the storage of personal data should be encrypted by the IPA provider for reasons of confidentiality in case of other persons' access, eg through maintenance companies or hackers. This can be done in various ways, for example by encrypting the personal data at the database level or by encrypting individual data records in an unencrypted

[180] Art 29 WP, 'Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU' <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229> accessed 10 September 2018.

[181] See arts 6(4), 32(1)(a), 34(3)a) GDPR.

[182] Gerald Spindler and Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 JIPITEC paras 64ff. give an overview of encryption technologies <https://www.jipitec.eu/issues/jipitec-7-2-2016/4440> accessed 6 September 2018; U Aßmus, *Datenschutz im Internet, Rechtshandbuch zu DSGVO und BDSG* (Legal Handbook on GDPR and German Data Protection Act) (Silke Jandt and Roland Steidle eds, NOMOS 2018) ch B.III, para 287.

database.[183] In all these cases, however, confidentiality is only protected against others than the user and the IPA provider.

An even more extensive confidentiality protection also towards the IPA provider can be achieved by an end-to-end encryption,[184] where only the user has access to the private keys for decryption but not the provider himself. The IPA provider should think about implementing such encryption with respect to data he does not need for the operation of the IPA, for example for stored messages or for personal data storages that are administrated by the IPA for its user. In some cases, such systems are already offered in connection with cloud storage.[185] They offer a maximum protection regarding confidentiality. However, they also challenge the user to take care of a backup of his private keys, because if he loses them, the IPA provider cannot recover data.

6.1.7 Accountability

Accountability[186] under Article 5(2) GDPR is one of the GDPR's key innovation principles. It covers all the principles of Article 5 GDPR and puts high challenges to controllers for the data processing. In connection with providing IPA services, the following possibilities for implementation should be considered by IPA providers:

[183] Art 29 WP (n149) para 39; Mishra (n1) 30; Spindler et al (n182) paras 64ff.; Kolah (n11) s 15; Jason Buffington, *Data Protection for Virtual Data Centers* (Hoboken, New Jersey: Wiley 2010); Aßmus (n182) ch B.III, para 289.

[184] Art 29 WP (n180) 1; Aßmus (n182) ch B.III, para 288.

[185] OwnCloud, 'End-to-End Encryption for ownCloud Enterprise' (2018), <https://owncloud.com/end-to-end-encryption/> accessed 10 September 2018.

[186] See s 5.4.7.

6.1.7.1 Data Protection Management System

For IPA providers, as for all other processors of personal data, the internal data processing processes should be clearly defined, following a data protection management system.[187] This concerns, for example, the development of new functions of an IPA, its documentation and the use of new categories of data. If a high risk to the rights and freedoms of the data subject is likely under Article 35(1) GDPR, a data protection impact assessment is to be carried out.[188]

Clear processes must also exist for the involvement of the company's data protection officer in such processes.[189] The same applies to the implementation of the fulfilment of the rights of data subjects which, however, are not the focus of this study.

6.1.7.2 Policies

An IPA provider can legitimise his internal organisation and compliance with the principles of the data protection law by, among other things, writing these principles down in policies for both employees and customers.[190] This makes the data protection principles understandable and data subjects can demand actions based on those principles. For example, an IPA provider should set out its compliance with the data protection principles towards users in a policy.

[187] Feiler et al (n9) art 5 cmts 13-14; J Hartung, *DS-GVO und BDSG Kommentar* (GDPR and German Data Protection Act Commentary) (Jürgen Kühling and Benedikt Buchner eds, 2nd edn, C.H. Beck OHG 2018) art 24 para 21.

[188] Herbst (n72) art 5 para 80.

[189] Feiler et al (n9) art 5 cmts 13-14.

[190] Hartung (n187) art 24 para21.

6.1.7.3 Training and Awareness Measures

In addition, accountability can be met by training relevant employees on data protection law and raising awareness through certain measures like web-based training or newsletters with respect to data protection issues.[191] This should be considered by IPA providers, too.

6.1.7.4 Contracts in Conformity with the Law

IPA providers should adapt their contracts with users, hosting providers and marketers to the new situation under the GDPR.[192] New possibilities resulting from the GDPR must be taken into account without going into details on the drafting of contracts at this point. For example, a joint data protection responsibility between different companies in accordance with Article 26 GDPR could now be thought about. Except for that, it remains with the known fundamental differentiation between a processing on behalf between a processor and a controller under Article 28 GDPR or, in contrast, a processing between two controllers that requires a legal basis under Article 6 GDPR.

6.1.7.5 Comprehensible Documentation

Finally, not least with regard to document requests by DPAs, there should be a clean and comprehensible document situation at the IPA provider. This includes structured documentation of possible data protection impact assessments.[193] It also includes decisions concerning weighing up of legitimate interests of the IPA provider

[191] This can be part of a Data Protection Management System ibid (n187); see also Article 39(1)(b) GDPR that rules awareness-raising and training as tasks of the data protection officer.

[192] In particular regarding contracts under art 28(3)(a)-(h) GDPR.

[193] Feiler et al (n9) art 5 cmts 13-14.

against conflicting interests of users under Article 6(1)(f) GDPR, for example concerning the operation of an IPA, or decisions regarding the likelihood and severity of risks of a certain processing to implement appropriate technical and organisational security measures under Article 32 GDPR. In addition, the communication with DPAs should be properly documented as well as the appointment of a data protection officer or, in the case of IPA providers from a third country, the appointment of a representative in the Union under Article 27 GDPR.

6.2 Obligations Arising Under the Legal Bases of Article 6 GDPR

Based on the previously identified legal bases of Article 6 GDPR[194] that can be considered for the operation of an IPA, the data transfer to a third country and the marketing of such data, concrete requirements shall be derived below with respect to which legal basis the provider can rely on in order to make his offering legitimate.

6.2.1 Performance of IPA Services

First, it must be analysed on which legal basis the operation of an IPA service can be carried out in a legally secure manner.

6.2.1.1 Processing of Personal Data

To the extent necessary, personal data in accordance with Article 6(1)(b) GDPR may be processed in order to fulfil the contract between the data subject and the provider of the IPA

[194] See s 5.2.

service.[195] Therefore, the legal basis can be derived directly under the statutory law of the GDPR. Consent of the data subject is not required in such case. However, the data subject must be sufficiently informed about the data processing within the scope of Article 13 GDPR.

6.2.1.2 Special Categories of Personal Data

Since a modern IPA typically processes special categories of personal data too,[196] in particular voice data to control the IPA or to transform it into text as well as certain biometric data for authentication, a further legal basis for the processing is required under Article 9 GDPR.[197] As discussed, explicit consent is therefore required under Article 9(2)(a) GDPR. However, paragraph 2 also mentions other legally admissible circumstances to process special categories of personal data, for example if the processing is necessary to protect the vital interests of a data subject according to (2)(c) – whereby one could think of certain SOS functions of an IPA service – or if data were obviously made public according to (2)(e). Though, such special processing situations are not the focus of this study. Moreover, Member States could implement further conditions and limitations concerning the processing of genetic data, biometric data or health data. Therefore, IPA providers must check the legal situation in each Member State when processing such data.

Consequently, the operation of an IPA with a typical functional scope requires, due to the collection and processing of special categories of personal data, at least for this part of data processing an explicit consent of the data subject in addition to the legal basis

[195] See s 5.5.2.
[196] See s 4.4.
[197] See s 5.5.1.

of Article 6(1)(b) GDPR. As a result, two different legal bases for the operation of a typical IPA are possible. Consent is not mandatory for every processing, but usually, consent will be mandatory in case of a typical processing of special categories of personal data.

6.2.1.3 Transfer of Personal Data to Third Countries

For the transfer of personal data as well as of special categories of personal data in data centres of IPA providers in a third country, the requirements of Article 44ff. GDPR must be observed in addition to the legal bases described above.[198]

Often, providers from the USA justify data transfers from Europe on joining the EU-US Privacy Shield. A voluntary commitment under the Privacy Shield offers sufficient guarantees to ensure an adequate level of data protection on the basis of a decision of the EU Commission.[199]

In addition, IPA providers often base data transfers in parallel on the conclusion of EU standard data protection clauses. One reason for this is that the Privacy Shield is subject of legal proceedings[200] and that it is criticised by, among others, the DPAs as insufficient,[201] so that its future existence or form is not foreseeable.

Furthermore, exceptions from the obligation to meet the requirements of Article 44 GDPR are conceivable. In accordance

[198] See s 5.5.6.

[199] ibid.

[200] ibid.

[201] Art 29 WP, 'EU-U.S. Privacy Shield – First annual Joint Review' (2017) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619> accessed 28 August 2018.

with Article 49(1)(a) GDPR, a consent of the data subject may be considered, provided that the data subject has been informed in advance of the risks of such a third country transfer.

Furthermore, in the absence of an adequacy decision and appropriate guarantees, a data transfer to a third country may be permitted under Article 49(1)(b) GDPR if the data transfer is necessary to fulfil a contract between the provider and the data subject which the data subject has requested. As an exception, the provision is to be interpreted narrowly, so that a data transfer that serves only the interests of the IPA provider is not sufficient.[202] Necessity exists if there is no reasonable and appropriate alternative to the data transfer. This may be the case in e-commerce constellations, for example, if the provider is only based in a third country.[203] Accordingly, a transfer to IPA providers in a third country could also be permitted if they maintain the technical infrastructure only there, in particular, their data centres.

As a result, explicit consent for the third country transfer is not mandatory in every situation, especially not with IPA providers from the United States who have joined the EU-US Privacy Shield, but also not with IPA providers from other third countries who have either concluded the EU standard data protection clauses or if the data transfer to IPA providers is necessary for the fulfilment of a contract the user has requested and if he has been sufficiently informed.

[202] C Schröder, *DS-GVO und BDSG Kommentar* (GDPR and German Data Protection Act Commentary) (Jürgen Kühling and Benedikt Buchner eds, 2nd edn, C.H. Beck OHG 2018) art 49 para 19.

[203] Schröder (n202) para 18.

6.2.2 Sale of Data for Marketing Purposes

If the data has legally arrived at the provider for the operation of the IPA, the question arises whether and how he can further utilise it, in particular by selling it for marketing purposes. However, as described above, anonymised data that could be sufficient for certain marketing measures do not require a legal basis.[204]

6.2.2.1 Compatible Purposes

As discussed before, the GDPR allows changing the purpose of data collected under Article 6(4) GDPR.[205] This could eventually apply for the sale and utilisation of data for marketing purposes that have been collected to enable the functioning of an IPA. This would require 'compatible purposes'. Of the criteria described above which an IPA provider must consider when assessing whether there are compatible purposes, paragraph 4(a) refers to a 'link between the purposes for which the data have been collected and the purposes of the intended further processing'. Such a substantive connection between the original purpose of the data collection to provide functions to the sale of these data in third countries for marketing purposes is not recognisable. Since Article 6(4) GDPR is an exceptional provision which undermines the principle of purpose limitation, it must be interpreted narrowly.[206] In addition, the consequences of the change of purpose for the data subject must be assessed in accordance with paragraph 4(d). These consequences are a loss of control due to the transfer of the data to a third country and the sale to third-party advertising networks and companies that are unknown to the data subjects. Unlike advertising by the IPA provider itself, the

[204] See s 6.1.5.1.

[205] See s 5.5.5.

[206] Buchner et al (n101) art 6 para 186.

data subject cannot understand who receives and uses his data for marketing purposes. This is particularly serious against the background of the considerable amount and the categories of usage data that are collected by IPAs. As a result, it can be assumed that there are two different and incompatible purposes regarding the providing of services and the marketing of personal data. Each purpose requires an own legal basis under the principle of lawfulness.

6.2.2.2 Legitimate Interests

As also discussed earlier, an IPA provider may have legitimate interests under Article 6(1)(f) GDPR to use personal data for direct marketing purposes.[207] Direct marketing purposes ‘may be regarded as carried out for a legitimate interest’ under recital 47 sentence 7. In this context, 'reasonable expectations of data subjects' have to be considered according to sentence 1 of recital 47, especially if, according to sentence 2, there is a suitable relationship between the controller and the data subject, for example, because the user is a customer of the provider.

In this respect, the question of what ‘reasonable’ expectations the user of an IPA service has of his or her usage data being sold for advertising purposes is of particular importance. In principle, it could be assumed that a consumer who is offered a typical web service without a financial obligation will assume that services are financed by advertising and that he must therefore, to a certain extent, expect his data to be used for advertising purposes. This utilisation may also include the disclosure of certain personal data to several third parties if it has been made transparent.[208] This

[207] See s 5.5.3.

[208] Steidle (n107) ch B.III, paras 179-181; Feiler et al (n9) art 6 cmt 7 are speaking of ‚conventional direct marketing‘.

could apply as long as the user has no reasonable indications that the service is financed elsewhere. For example, this could be the case, if, in a recognisable way, the IPA service advertises donations or is offered as a funded research project that is supported by the public sector.[209]

However, it is more than questionable whether the above legal interpretation is also possible for IPA systems and a marketing of personal data via onward transfers to international companies in third countries. The utilisation of usage data via onward transfers, ie the resale of the data by the provider in the third country to advertisers and advertising networks, which in turn may resell to other advertisers, is likely to regularly fall outside the reasonable expectations of an average user. In particular, the data subject will have no reasonable expectation of the legal systems that apply in the third countries and which rights he has with respect to the international marketing.

To what extent this reasonable expectation can be influenced by detailed information[210] has not yet been conclusively clarified by the DPAs. But even if, as described, one assumes that information can influence expectations in a small amount, this must always be in line with the reasonability. This means that a certain objectification[211] is necessary although expectations change over time in a dynamic environment. However, the protective nature of the GDPR with regard to third country transfers would be abolished if information alone would be sufficient to legitimise any data processing as by IPA providers within the framework of reasonable expectations.

[209] Steidle (n107) ch B.III, para 181.

[210] See s 5.5.3.

[211] See s 5.5.3 for the meaning of the term 'reasonable'.

In this respect, it cannot be assumed that comprehensive marketing of usage data including international onward transfers can be legally secure implemented by IPA providers in third countries on the basis of legitimate interests. Therefore, consent will be necessary for most situations of utilisation of user's data abroad.

6.2.2.3 Consent

As a result, in most cases of marketing personal usage data by an IPA provider in a third country, explicit consent is already required for reasons of legal certainty under the GDPR.[212] If special categories of personal data are also to be marketed, this is mandatory according to Article 9(2)(a) GDPR.

However, it should be borne in mind that even within the scope of consent no unlimited marketing of usage data is permitted. On the one hand, blanket consents without a concrete purpose are not permissible, for example, consent in a processing 'for utilisation' without further differentiating forms of advertising.[213] On the other hand, data processing must always be made transparent to the user who consents. Thus, it is not possible to legitimise completely unforeseeable and indefinite data sales for marketing purposes over consent of the data subject.[214] Furthermore, the IPA provider must check the age of his users.[215]

[212] This might become different regarding usage data of data subjects from the US, see Alex Johnson, 'Trump Signs Measure to Let ISPs Sell Your Data Without Consent' *NBC News Digital* (New York, 4 April 2017) <https://www.nbcnews.com/news/us-news/trump-signs-measure-let-isps-sell-your-data-without-consent-n742316> accessed 21 August 2018.

[213] ibid (n101).

[214] ibid (n101).

[215] See s 5.5.3.

Finally, he must note that the advertising consent is given voluntarily under Article 7(4) GDPR and is not linked to the processing of data not required for the operation. If the advertising consent is refused, other ways for a financial compensation of the provider are to be considered. As shown, this can be, for example, a paid offer that the user can choose voluntarily instead of paying with his personal data.[216]

6.2.3 Comprehensive Consent

The GDPR allows various legal bases of Article 6(1) GDPR to be applied side by side.[217] Considering that the typical processing of special categories of personal data already requires explicit consent for the operation of the IPA and that extensive marketing of usage data via the sale to international advertising networks requires consent, too, it is conceivable that the difficult distinction between the various legal basis will be dispensed with and that an IPA provider will ask his users to consent to all data processing. In this case, users should be fully informed during registration and asked to give their individual consent to each of the various processing purposes under Article 7(2). Recital 32 Sentence 5 requires explicit and unconditional consent for each purpose, for the performance of the services as well as for the utilisation of personal data.

6.2.4 Compliance with Security Obligations

Finally, the processing to secure personal data and the processing itself constitutes a further purpose. It may be necessary for the provider to process personal usage data with the aim of protecting

[216] See c 5.5.1; Feiler et al (n9) art 7 cmt 9.

[217] Buchner et al (n101) art 6 para 22.

its services, inter alia to guarantee the confidentiality and integrity of personal data. This requires, for example, access to IP addresses, login data and certain device data such as certificates.

If these measures are within the scope of the obligations of Article 32 GDPR to provide adequate technical and organisational security measures, the IPA Provider thus only fulfils its legal obligation under Article 6(1)(c) GDPR.[218] Besides, it does not require any other legal basis or user consent to process data for this purpose. Moreover, it would not make sense to include such processing in an overarching consent, since the IPA provider remains obliged, irrespective of the user's consent, to maintain appropriate security measures which protect all other users.[219]

Although, it is conceivable that an IPA provider may additionally rely on a legitimate interest under Article 6(1)(f) GDPR in conjunction with Recital 49 in order to achieve a 'given level of confidence'. Such security measures are not required by the obligation under Article 32 GDPR to consider the state of the art and to implement adequate safeguards. However, such cases of data processing with regard to special IT security measures are not the focus of this study.

7. CONCLUSIONS

Intelligent personal assistants are a modern technology that is becoming more and more popular. Against the background of new possibilities of artificial intelligence, its range of functions is increasingly expanding and the assistants are now able to perform sophisticated services that were previously only available to

[218] See s 5.5.4.

[219] Buchner et al (n101) art 6 para 23.

qualified people. This applies in particular to services in which biometric data such as voice data is analysed and processed, and in which the actions of the assistant are placed in context with the current situation of a user and other IPAs.

The well-known assistants from Amazon, Apple, Google and Microsoft, which have been widely used up to now, are offers from providers seated in a third country. Typically, usage data as well as special categories of personal data are transferred to and processed in the United States and worldwide for the operation of the services.

Furthermore, the offers are typically aimed at consumers. Usually, they do not have to pay a separate financial fee to receive the extensive services of an assistant. Instead, they pay with their usage data and its marketing, although users, in most cases, do not understand this in detail. Thus, usage data is sold to international advertising networks and is used for direct marketing purposes regarding users as part of a business worth billions.

The GDPR, which came into force at the end of May 2018, poses special challenges for providers of such services. The GDPR forces, not least through a substantially increased fine framework and the principle of accountability, the providers to comply with numerous data protection principles. Special challenges arise in particular from the data protection principles of transparency, purpose limitation, data minimisation, accuracy, storage limitation and the integrity and confidentiality of the processed personal data.

In addition, there are new requirements regarding the legal bases on which providers can offer their services in the future. Although there is only one central framework regulation under Article 6

GDPR, it is difficult to identify the applicable provisions under paragraph 1 that can be used for the various processing purposes. However, it could be conceivable to base the operation of an IPA without using special categories of personal data but including the transfer to a third country on a statutory legal basis. Though, common assistants process biometric data and special categories of personal data, which is why consent is typically required. If one considers that an extensive marketing also requires consent, it is obvious that the providers could place their business model on an overarching consent and ask for an explicit consent for both the operation and the marketing.

Though, if a user refuses to consent to the marketing of his data, he is entitled to do so. Due to the new provision of Article 7(4) GDPR that requires unconditional consent with respect to a processing that is not necessary for the performance of a contract, the user cannot be forced to agree to advertising measures. Providers are therefore faced with the challenge of finding new business models and opportunities to be remunerated for their services. One possibility may be to offer paid alternatives to the marketing of usage data in parallel to models financed by advertising.

Solely for the implementation of appropriate technical and organisational security measures, taking the state of the art into account, consent is neither meaningful nor permissible, since the implementation is a legal obligation of the provider.

The GDPR thus poses considerable challenges to providers of IPA services, although the substantive legal regulations at first glance suggest little new obligations in comparison to the former DPD. Despite these challenges, the present study shows that an implementation is possible which takes into account both, the interests of the data subjects in a comprehensive and effective data protection as well as the possibilities of IPA providers to offer modern technologies in the European Union and making a profit. It is possible to operate IPAs in a way that personal usage data is processed in third countries and may be sold by the providers abroad for advertising purposes. The GDPR thus does not represent an inadequate obstacle to innovation, as some feared during the legislative process, but rather an opportunity to continue to guarantee users an effective data protection in an increasingly digital world.

BIBLIOGRAPHY

1. Primary Sources

Legislation

EU Directives

European Data Protection Directive 95/46/EC

E-Privacy-Directive 2002/58/EC

EU Regulations

Proposal of the European Commission for a GDPR, Draft COM(2012) 11 final

General Data Protection Regulation (EU) 2016/679

E-Privacy-Regulation, Draft COM(2017) 10 final

Conventions

Convention on the Rights of the Child 1989

Cases

Bund für Umwelt und Naturschutz Deutschland e.V. v Bundesrepublik Deutschland [2015] Case C-461/13 ECR I-433

Digital Rights Ireland v Commission [2016] Case T-670/16 ECLI:EU:T:2017:838

Google Spain v AEPD and Mario Costeja González [2014] Case C-131/12 OJ C 165, 9.6.2012

Patrick Breyer v Bundesrepublik Deutschland [2016] Case C-582/14 OJ C 89, 16.3.2015

Maximilian Schrems v Data Protection Commissioner Case [2015] C-362/14 2 CMLR 2

2. Secondary Sources

Commission Decisions

The EEA Joint Committee, no 154/2018 (Commission Decision, 6 July 2018), <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:22018D1022&from=EN> accessed 28 August 2018

Administrative Opinions and Working Papers

Article 29 Data Protection Working Party, Opinion 02/2012 on facial recognition in online and mobile services (2012) WP192 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf> accessed 28 August 2018

Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies (2012) WP193 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf> accessed 28 August 2018

Article 29 Data Protection Working Party, *Opinion 3/2013 on purpose limitation* (2013) WP203 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 28 August 2018

Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques* (2014) WP216 <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 28 August 2018

Article 29 Data Protection Working Party, *Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting* (2014) WP224

<http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf> accessed 28 August 2018

Article 29 Data Protection Working Party, *EU–U.S. Privacy Shield – First annual Joint Review* (2017) <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619> accessed 28 August 2018.

Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (2018) WP259 rev.01 <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051> accessed 28 August 2018

Article 29 Data Protection Working Party, *Guidelines on Transparency under Regulation 2016/679* (2018) WP260 rev.01 <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227> accessed 28 August 2018

Article 29 Data Protection Working Party, *Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU* (2018) <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622229> accessed 10 September 2018

Books

Albrecht J and Jotzo F, *Das neue Datenschutzrecht der EU* (The new EU Data Protection Law) (NOMOS 2017)

Buffington J, *Data Protection for Virtual Data Centers* (Hoboken, New Jersey: Wiley 2010)

Feiler L, Forgó N and Weigl M, *The EU General Data Protection Regulation (GDPR): A Commentary* (Globe Law and Business 2018)

Jandt S and Steidle R, *Datenschutz im Internet, Rechtshandbuch zu DSGVO und BDSG* (Legal Handbook on GDPR and German Data Protection Act) (NOMOS 2018)

Kolah A, *The GDPR Handbook: A Guide to Implementing the EU General Data Protection Regulation* (Kogan Page 2018)

Kosta E, *Consent in European Data Protection Law* (Leiden, Boston: Martinus Nijhoff, 2013)

Kuschewsky M (ed), *Data Protection & Privacy* (3rd edn, Sweet & Maxwell 2016)

Kühling J and Buchner B (eds), *DS-GVO, BDSG Kommentar* (GDPR and German Data Protection Act Commentary) (2nd edn, C.H. Beck OHG 2018)

McTear M and Callejas Z, *Voice Application Development for Android* (Packt Publishing 2013)

Mishra S, *Wearable Android: Android Wear & Google Fit App Development* (Wiley 2015)

Negroponte N, *Being Digital* (Alfred A. Knopf 1995)

Tang C, *The Data Industry: the Business and Economics of Information and Big Data* (Hoboken, New Jersey: Wiley 2016)

Journals

Broeders D, Schrijvers E, van der Sloot B, van Brakel R, de Hoog J and Ballin E, 'Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data' (2017) 33 C.L.S.Rev. 309

Cottrill C and Thakuriah P, 'Privacy in context: An evaluation of policy-based approaches to location privacy protection' (2014) 22 IJLIT 178

Enders T, 'Exploring the Value of Data – A Research Agenda' [2018] LNBIP 1

Garstka K, ‘From Cyberpunk to Regulation – Digitised Memories as Personal and Sensitive Data within the EU Data Protection Law’ (2017) 8 JIPITEC 293 <https://www.jipitec.eu/issues/jipitec-8-4-2017/4637> accessed 6 September 2018

Hacker P, ‘Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things’ (2017) 7 IDPL 266

Hermstrüwer Y, ‘Contracting Around Privacy. The (Behavioral) Law and Economics of Consent and Big Data’ (2017) 8 JIPITEC 9 <https://www.jipitec.eu/issues/jipitec-8-1-2017/4529> accessed 6 September 2018

Hornung G, ‘A General Data Protection Regulation for Europe: Light and Shade in the Commission's Draft of 25 January 2012’ (2012) 9 SCRIPTed 64

Irion K, ‘Your digital home is no longer your castle: how cloud computing transforms the (legal) relationship between individuals and their personal records’ (2015) 23 IJLIT 348

Jasserand C, ‘Legal Nature of Biometric Data: From ‘Generic’ Personal Data to Sensitive Data’ (2016) 2 EDPL 297

Kong L, ‘Data Protection and Transborder Data Flow in the European and Global Context’ (2010) 21 European Journal of International Law 441 <https://doi.org/10.1093/ejil/chq025> accessed 2 May 2018

López S, ‘Informing Consent. Giving Control Back to the Data Subject from a Behavioral Economics Perspective’ (2018) 9 JIPITEC 35 <https://www.jipitec.eu/issues/jipitec-9-1-2018/4678> accessed 6 September 2018

Malgieri G and Custers B, ‘Pricing privacy – the right to know the value of your personal data’ (2018) 34 C.L.S.Rev. 289

Spindler G and Schmechel P, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 JIPITEC 163 <https://www.jipitec.eu/issues/jipitec-7-2-2016/4440> accessed 6 September 2018

Tene O, 'Privacy: The new generations' (2011) 1 IDPL 15 <https://doi.org/10.1093/idpl/ipq003> accessed 6 September 2018

Veale M, Binns R and Ausloos J, 'When data protection by design and data subject rights clash' (2018) 8 IDPL 105 <https://doi.org/10.1093/idpl/ipy002> accessed 6 September 2018

Voss W, 'European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting' (2017) 72 Business Lawyer 221

Weiss M and Archick K, 'U.S. - EU Data Privacy: From Safe Harbor to Privacy Shield' (2016) Congressional Research Service <https://fas.org/sgp/crs/misc/R44257.pdf> accessed 2 May 2018

Articles

Herbig D, 'Google Assistant funktioniert jetzt auch in Deutschland mit Android Auto' (Google Assistant now also works in Germany with Android Auto) *Heise Online* (Hannover, 19 September 2018) <https://www.heise.de/newsticker/meldung/Google-Assistant-funktioniert-jetzt-auch-in-Deutschland-mit-Android-Auto-4167890.html> accessed 19 September 2018

Johnson A, 'Trump Signs Measure to Let ISPs Sell Your Data Without Consent' *NBC News Digital* (New York, 4 April 2017) <https://www.nbcnews.com/news/us-news/trump-signs-measure-let-isps-sell-your-data-without-consent-n742316> accessed 21 August 2018

Jurran N, 'Sprachassistenz: Fahrzeuge von Audi künftig mit Alexa' (Language assistance: Audi vehicles to be equipped with Alexa in the future)

Heise Online (Hannover, 19 September 2018) <https://www.heise.de/newsticker/meldung/Sprachassistenz-Fahrzeuge-von-Audi-kuenftig-mit-Alexa-4168022.html> accessed 19 September 2018

Jurran N, 'Alexa: Mikrowellen-Ofen und Wanduhr mit Sprachassistentin' (Alexa: Microwave oven and wall clock with language assistant) *Heise Online* (Hannover, 20 September 2018) <https://www.heise.de/newsticker/meldung/Alexa-Mikrowellen-Ofen-und-Wanduhr-mit-Sprachassistentin-4169442.html> accessed 20 September 2018

Lehmbruck L, 'Neues System erkennt PC-Nutzer am Tippverhalten. Biometrie-Software ersetzt das Passwort' (New system recognizes PC user by typing behaviour. Biometrics Software replaces Password) *Handelsblatt* (Düsseldorf, 26 March 2006) <https://www.handelsblatt.com/technik/it-internet/neues-system-erkennt-pc-nutzer-am-tippverhalten-biometrie-software-ersetzt-das-passwort/2633532.html?ticket=ST-5775102-BWSlJKh50bXXpHAbYFey-ap4> accessed 8 September 2018

Web Sites

Apple, 'Hey Siri, wake me up at 7 AM tomorrow' <https://www.apple.com /ios/siri/> accessed 29 August 2018

DocuSign, 'Understanding digital signatures. What is a digital signature, and how can you create one?' (2018) <https://www.docusign.com/how-it-works/electronic-signature/digital-signature/digital-signature-faq> accessed 14 August 2018

Google, 'Ready to help, wherever you are.' <https://assistant.google.com /intl/en_uk/#?modal_active=none> accessed 28 August 2018

Heise Online/ DPA, 'Amazons Smart-Home-Chef: Sprach-Assistenten werden immer in Hörweite sein' (Amazon's Smart-Home boss: "Speech assistants will always be within earshot) <https://www.heise.de/newsticker/meldung/Amazons-Smart-Home-Chef-Sprach-Assistenten-

werden-immer-in-Hoerweite-sein-4154044.html> accessed 28 August 2018

Microsoft, ‘Delete and Manage Cookies‘ (2017) <https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies> accessed 10 September 2018

Microsoft, ‘Cortana and Privacy - How to Control Cortana’s Collection and Use of Your Data‘ (2018) <https://privacy.microsoft.com/en-us/windows-10-cortana-and-privacy> accessed 10 September 2018

Microsoft, ‘Enrolling a Fingerprint’ (2018) <https://docs.microsoft.com/en-us/xamarin/android/platform/fingerprint-authentication/enrolling-fingerprint> accessed 10 September 2018

OwnCloud, ’End-to-End Encryption for ownCloud Enterprise’ (2018), <https://owncloud.com/end-to-end-encryption/> accessed 10 September 2018

StanfordLawSchool, ‘Discover Legal Technology’ <https://techindex.law.stanford.edu/> accessed 12 September 2018