Grant Agreement No.: 761802

D1.3: Legal validation report and system architecture

The goal of this task is to capture the regulatory requirements that are relevant for interactive radio with engagement, interaction and personalisation, in particular the new General Data Protection Regulation, Digital Internal Market rules etc. (digital services, IP law, media law etc.).. The legal assessment is concentrated on the general concept, use cases and requirements. The envisaged prototypes should comply with legal rules, in particular privacy. Means will be developed for transparency and for an appropriate privacy policy, in particular concerning consent.

Work package	WP 1
Task	Task Number 6
Due date	31/05/2018
Deliverable lead	UNIVIE
Version	0.4
Authors	Erich Schweighofer, Felix Schmautzer, Jakob Zanol (Partner UNIVIE)
Reviewers	
Keywords	data protection, personal data, social media monitoring, special categories of personal data

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	16/04/2018	1st version – data types	Erich Schweighofer (Partner UNIVIE), Felix Schmautzer (Partner UNIVIE), Jakob Zanol (Partner UNIVIE)
VO.2	24/05/2018	2nd version - legal basis for processing, general framework, jurisdiction	Erich Schweighofer (Partner UNIVIE), Felix Schmautzer (Partner UNIVIE), Jakob Zanol (Partner UNIVIE)
V0.3	29/05/2018	3rd version – privacy policy, transparency principles, collection of public data, declaration of consent, data sharing, DPIA	Erich Schweighofer (Partner UNIVIE), Felix Schmautzer (Partner UNIVIE), Jakob Zanol (Partner UNIVIE)
V0.4	31/05/2018	4th version; revision, comments	Erich Schweighofer (Partner UNIVIE), Felix Schmautzer (Partner UNIVIE), Jakob Zanol (Partner UNIVIE)

Co-funded by the Horizon 2020 Framework Programme of the European Union

Disclaimer

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 761802.

Project co-funded by the European Commission in the H2020 Programme	
Nature of the deliverable:	**R**
Dissemination Level	
PU	Public, fully open, e.g. web

Co-funded by the Horizon 2020 Framework Programme of the European Union

EXECUTIVE SUMMARY

UNIVIE has analysed architecture, data types and proposed services of MARCONI from a legal point of view, in particular taking into account the General Data Protection Regulation (GDPR). Each dataset is classified if it contains personal data falling under the scope of Articles 6, 9 and 10 GDPR. Further, it is evaluated under which conditions such data can be processed lawfully. The most important challenges are:

- The designation and classification of 'personal data' and 'data subject';
- Attaining informed, free and granular consent;
- Weighing of interests according to Article 6(1)(f) GDPR, in particular with regard to public data;
- Anonymisation and pseudonymisation of data;
- A guide to GDPR compliance, in particular concerning role allocation.

The respective data controller (radio stations) and their processors (aides such as PLUX, IN2, FXYZ) must conclude a written agreement. Both entities must have a register of processing activities.

Controllers may only process personal data under a lawful basis. In MARCONI, this shall either be consent (especially concerning sensitive data according to Article 9 GDPR), a necessity for the performance of a contract (smartphone app) or a necessity for the purpose of legitimate interests pursued by the controller.

Data protection principles should be respected. Only data absolutely necessary for the service shall be processed for legitimate purposes, kept accurate and deleted after the processing purposes are fulfilled. Before processing is being conducted, the data subject must be properly informed. The controller will be held responsible for demonstrating compliance to the aforementioned principles.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Table of Contents

Co-funded by the Horizon 2020 Framework Programme of the European Union

Co-funded by the Horizon 2020 Framework Programme of the European Union

Co-funded by the Horizon 2020
Framework Programme of the European Union

ABBREVIATIONS

DLNN	Deep Learning Neural Networks
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Council
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
Rec.	Recital
TCP	Transmission Control Protocol
WP29	Article 29 Data Protection Working Party

Co-funded by the Horizon 2020
Framework Programme of the European Union

1 Legal Framework on Data Protection

The legal framework on data protection consists of human rights, in particular right to privacy, international treaties, European legal instruments and national laws as well as relevant case law. In the EU, the General Data Protection Regulation (GDPR) is of particular importance.

1.1 Human Rights

Even if data protection is now regulated in European legal frameworks it is important to remember that data protection is not only a matter of national or European legislation but also a human right. As various inter-governmental organisations have developed an impressive normative framework regarding human rights in general[1], so too can the (human) right to data protection be found in various forms within this international network.

Aside from a specific right to data protection (see below) the right to privacy and the right to informational self-determination must be mentioned.

Article 8(1) European Convention on Human Rights[2] states that everyone has the right to respect for his private and family life, his home and his correspondence. If a public authority is interfering with someone's ability of his personal development it is interference into someone's right to respect for his private life.[3]

In the context of data protection, the most relevant part of the ECHR is Article 8 (respect for private and family life, home and correspondence) and also Article 10 (freedom of expression). This human right is, however, not protected absolutely, which means that necessary restrictions are possible. According to Article 6(3) TEU[4] fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) […], shall constitute general principles of the Union's law.

Article 17 of ICCPR[5] states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

[1] *Nowak/Januszewski/Hofstätter* (eds.), All Human Rights for All – Vienna Manual on Human Rights (2012) 63.

[2] Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, (last visited May 08 2018 on: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063765).

[3] *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung (2014) 23.

[4] Treaty on European Union and the Treaty on the Functioning of the European Union (TEU), Official Journal C 326 , 26/10/2012, 1 – 390.

[5] International Covenant on Civil and Political Rights, adopted by the United Nations General Assembly on December 16 1966 - resolution 2200A (XXI), which came into force March 23 1976.

Co-funded by the Horizon 2020 Framework Programme of the European Union

The German Federal Constitutional Court developed the right to informational self-determination as case-law during its famous decision concerning the collection of personal information during the 1983 census.[6] According to German Federal Constitutional Court:

"*in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the [German Constitution]. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest*".

In 2008, the German Federal Constitutional Court also developed the Right specifically to "IT-Privacy", within a ruling relating to an online investigation.[7]

The right to data protection results not only from the right to privacy and/or the right to Informational self-determination, it is also stated explicitly in Art. 8 of the **European Charter of Fundamental Rights**[8], wherein the EU reaffirmed the rights as they result from i.e. the constitutional traditions and international obligations common to the Member States[…], the European Convention for the Protection of Human Rights and Fundamental Freedoms[…] and the case-law of the Court of Justice of the European Communities and of the European Court of Human Rights.[9]

1.2 International Instruments

The **European Data Protection Convention**[10] is an international treaty of the Council of Europe with the aim to protect the "right to the respect for privacy of individuals, taking account of the increasing flow across frontiers of personal data undergoing automatic processing".[11] It was signed by the Member States of the Council of Europe on January 28, 1981. To secure respect for the rights and fundamental freedoms, and in particular the right to privacy with regard to automatic processing of personal data for every individual, whatever nationality or residence, in the territory of each Member State[12], the European Data Protection Convention provides a minimal level of data protection[13], that has to be provided by each party as well as a framework for transborder data flows[14] and mutual assistance between parties[15].

---

[6] German Federal Constitutional Court, BVerfGE 65, 1.

[7] German Federal Constitutional Court, 1 BvR 370/07, 1 BvR 595/07.

[8] Charter of Fundamental Rights of the European Union (Charter), OJ C 326, 26.10.2012, 391–407;
Also i.e. in Art. 1(1) of the Austrian Data Protection Act, BGBl. I Nr. 165/1999 idF BGBl. I Nr. 24/2018.

[9] Preamble of the Charter of Fundamental Rights of the European Union (Charter), OJ C 326, 26.10.2012.

[10] Convention for the protection of individuals with regard to automatic processing of personal data, Strasbourg 28.01.1981, ETS No. 108 (European Data Protection Convention).

[11] Preamble of the European Data Protection Convention.

[12] Art. 1 European Data Protection Convention.

[13] Art. 4 (f) European Data Protection Convention.

[14] Art. 12 European Data Protection Convention.

[15] Art. 13 (f) European Data Protection Convention.

Co-funded by the Horizon 2020
Framework Programme of the European Union

The Convention states basic principles for data protection. Each party was to take measures in its domestic law to give effect to these basic principles (Articles 4f European Data Protection Convention). Article 5 states principles that must be observed when personal data is undergoing automatic processing, which are almost identical to the Principles Relating to Data Quality stated in Article 6 of Data Protection Directive[16].

The European Data Protection Convention also includes a special provision (Article 6) regarding special categories of personal data (like racial origin or political opinions) and data relating to criminal convictions, prohibiting automatic processing of such data unless domestic law provides appropriate safeguards. It also states an obligation of each party to adopt appropriate measures for the protection of personal data against unauthorised tampering (Article 7) and a right to information for the data subject (Article 8).

In addition, the European Data Protection Convention addresses the issue of transborder data flows. According to Article 12(2), transborder flows of personal data from one party to another shall not be prohibited or subject to special authorisation. However, each party is entitled to derogate from this provision as long as equal protection is not provided.

With the Amendment to the European Data Protection Convention[17] the responsibility of each party to provide for one or more supervisory authorities[18] as well as a provision regulating transborder flows of personal data to third parties[19] were included.

The European Data Protection Convention is under ongoing modernisation to account for the technological developments since 1981 and to align this treaty with the Data Protection Reform Package, including the General Data Protection Regulation (Regulation 2016/679/EU) and the Directive 2016/680/EU.

To prevent disparities in national legislations that could hamper the free flow of personal data across frontiers and between the OECD[20] - Members, half of which had already introduced or would shortly be introducing privacy protection laws, the OECD developed **Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data** to help harmonize national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data.[21] These Guidelines have been revised in 2013.[22]

---

[16] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995, 31.

[17] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Strasbourg, 08/11/2001, ETS No.181 (Amendment to the European Data Protection Convention).

[18] Art. 1 Amendment to the European Data Protection Convention.

[19] Art. 2 Amendment to the European Data Protection Convention.

[20] Organisation for Economic Cooperation and Development (OECD).

[21] Preface of the OECD Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data 1980, C(80)58/FINAL.

[22] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013), C(80)58/FINAL, as amended on 11 July 2013 by C(2013) 79.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Addressing the fact, that the global economy is rapidly becoming digital and that digital technologies are transforming the lives of millions, the European Union aims to achieve a Digital Single Market, wherein the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection.[23]

In order to create the conditions and a level playing field for advanced networks and innovative services, part of achieving a digital single market is to generate trust in digital services by ensuring that individuals are protected in respect to processing of personal data.[24]

The **General Data Protection Regulation**, which replaced the **Data Protection Directive 95/46/EC** on May 25, 2018, as well as the **Directive 2016/680/EU**[25] are important steps toward EU-wide harmonisation of data protection laws.

Complementing the provisions regarding data protection as stated within the Directive 95/46/EC, the **Directive on Privacy and Electronic Communications**[26] includes additional provisions specifically for the telecommunications sector.[27]

A proposal for a **Regulation on Privacy and Electronic Communications**[28], that would replace the Directive on privacy and electronic communications, is currently being discussed in the Trilogue.

The Data Retention Directive[29] aimed to harmonize Member States provisions concerning the obligations of service providers with respect to the retention of certain data for the purpose of the

[23] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe, COM (2015) 192 final (Digital Single Market Strategy).

[24] Rec. 7 General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, 1–88).

[25] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, 89–131.

[26] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, 37–47.

[27] See also Rec. 4 Directive on privacy and electronic communications.

[28] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).

[29] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive), OJ L 105, 13.4.2006, 54–63.

Co-funded by the Horizon 2020 Framework Programme of the European Union

investigation, detection and prosecution of serious crime.[30] It was however annulled on April 8, 2014 by the European Court of Justice (ECJ), ruling that it would be in violation of fundamental rights.[31]

In addition to the above mentioned framework, **Regulation 45/2001/EC**[32] includes separate provisions regarding the processing of personal data by institutions of the European Union.

Since effective data protection also depends on data security, it is worth mentioning that the Council Decision 92/242/EEC as well as the **Directive (EU) 2016/1148** (NIS-Directive)[33], set out provisions on security of networks and information systems. The NIS-Directive was proposed by the European Commission as part of the EU Cybersecurity strategy with the goal to enhance cybersecurity across the European Union[34], including security measures that have to be taken by operators of essential services[35] and digital service providers[36].

1.3 General Data Protection Regulation (GDPR)

1.3.1 INTRODUCTION

The **General Data Protection Regulation** (GDPR) is the new framework for data protection law within the EU and replaces the Data Protection Directive 95/46/EC.[37] As the GDPR is not a directive but a regulation, it is directly applicable since May 25, 2018[38] Since the GDPR does not allow further transposition laws within each jurisdiction, a harmonisation of data protection law across the European Union will be achieved. There are, however, various "opening clauses" within the GDPR, giving each Member State some leeway in regulating certain topics.[39] The GDPR is part of the EU data

[30] Art. 1(1) Data Retention Directive.

[31] ECJ 8 April 2014, C-293/12 and C-594/12 ("Digital Rights Ireland and Seitlinger and Others") ECLI:EU:C:2014:238.

[32] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJ L 8, 12.1.2001, 1–22.*

[33] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Network and Information Security Directive – NIS-Directive), *OJ L 194, 19.7.2016, 1–30.*

[34] See also https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive.

[35] Art. 4(4), 5 and 14, as well as Annex II NIS-Directive.

[36] Art. 4(5)&(6), 16 and Annex III NIS-Directive, as well as Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, *OJ L 26, 31.1.2018, 48–51.*

[37] *Rücker* in *Rücker/Kugler* , New European General Data Protection Regulation (2018) point 4.

[38] *Rücker* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 9.

[39] For an overview, see: *Feiler*, Öffnungsklauseln in der Datenschutz-Grundverordnung – Regelungsspielraum des österreichischen Gesetzgebers, jusIT 2016/93, 210; *Rücker* in *Rücker/Kugler* (Eds.), New European General Data Protection Regulation (2018) 9f.

Co-funded by the Horizon 2020 Framework Programme of the European Union

protection reform package, along with the Data Protection Directive for Police and Criminal Justice Authorities[40].

1.3.2 SCOPE AND PERSONAL DATA

The GDPR applies to the processing of personal data (**material scope**) wholly or partly by automated means and also to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[41]

Since the GDPR is applicable only to processing of personal data, said term should be defined close and datasets reviewed accordingly.[42] The result of the evaluation can be found in Chapter 3.2. A prerequisite in for information being classified as personal data is the relation to an individual.

According to Article 4(1) GDPR, "*personal data*" means "*any information relating to an identified or identifiable natural person* ('data subject'). *An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".[43]

Recital 26 GDPR further states that "*to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*".[44]

It also states, that "[t]*o ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*".[45]

The ECJ already ruled that it is not required that all the information enabling the identification of the data subject must be in the hands of one person and that it must be determined whether the possibility to combine certain data (in that case a dynamic IP address) with additional data held by a third party (in that case the internet service provider) constitutes a means reasonably likely to be used to identify the data subject.[46] In this case the ECJ ruled that IP-Addresses are personal data since, in particular, in the event of cyber-attacks, legal channels exist enabling digital media services providers to contact the

[40] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, 89–131.

[41] Art. 2(1) GDPR.

[42] *Rücker* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 44f.

[43] Art. 4(1) GDPR.

[44] Rec. 26 GDPR.

[45] Rec. 26 GDPR.

[46] ECJ 19 October 2016, C-582/14 ("Breyer") ECLI:EU:C:2016:779 (with regard to Rec. 26 of Directive 95/46/EC, which is similar to Rec. 26 GDPR).

Co-funded by the Horizon 2020 Framework Programme of the European Union

competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and to initiate criminal proceedings.[47]

Regarding the **territorial scope**, the GDPR differentiates between processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union and by a controller or processor not established in the Union.[48]

Concerning processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, it is not relevant whether or not the processing takes place in the Union or not.[49] The key is to evaluate whether processing is in the context of the activities of an **establishment** of a controller or a processor that is situated within the EU. According to Recital 22 GDPR an "*establishment implies the effective and real exercise of activity through stable arrangements*", but also, that the legal form of such arrangements (whether through a branch or a subsidiary with a legal personality), should not be considered the determining factor in that respect.

The ECJ[50] ruled that the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement[51] if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question. The ECJ also stated that these provisions (regarding territorial scope) cannot be interpreted restrictively, since the European legislature sought to prevent individuals from being deprived of the protection.[52]

Without such an establishment, the GDPR still applies, if the processing activities are related to the **offering of goods or services to data subjects in the Union**, irrespective of whether a payment of the data subject is required[53] or if they are related to the monitoring of their behaviour, as far as their behaviour takes place within the Union[54]. Also the GDPR applies to the processing of personal data by a controller not established in the Union, if Member State law applies by virtue of public international law, such as in a Member State's diplomatic mission or consular post.[55]

[47] ECJ 19 October 2016, C-582/14 ("Breyer") Rec. 47.

[48] Art. 3 GDPR.

[49] Art. 3(1) GDPR; *Schumacher* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 189.

[50] ECJ 1 October 2015, C-230/14 ("Weltimmo") ECLI:EU:C:2015:639.

[51] This ruling concerned Rec. 19 and Art. 4(1)(a) Data Protection Directive (Directive 95/46), wherein the establishment was defined as "the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect" (see Rec. 19 Directive 95/46).

[52] ECJ 13 May 2014, C-131/12 ("Google Spain und Google") ECLI:EU:C:2014:317.

[53] Art. 3(2)(a) GDPR.

[54] Art. 3(2)(b) GDPR.

[55] Rec. 25 and Art. 3(3) GDPR.

Co-funded by the Horizon 2020
Framework Programme of the European Union

1.3.3 LAWFUL PROCESSING

Since the right to protection of personal data is not an absolute right, it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.[56]

This means that the lawfulness of processing of personal data under the GDPR is based on the aim to respect all fundamental rights and to observe the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.[57]

To achieve this goal, the processing of personal data is generally prohibited unless a legal ground of processing exists.[58] Such legal ground may be consent or some other legitimate basis[59]. Furthermore, processing must also adhere to certain principles, like transparency, purpose limitation and confidentiality.[60]

It is possible that more than one ground of justification applies to certain processing activities.[61]

When determining grounds of justification to process personal data in a lawful manner, differentiation has to be made whether **special categories of personal data**[62] are processed, which merit higher and more specific protection, as the context of their processing could create significant risks to the fundamental rights and freedoms, **or other personal data**.[63]

Regarding **("normal") personal data Article 6(1) GDPR** states that processing shall be unlawful only if and to the extent that at least one of the following applies:

a. the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes

b. processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

c. processing is **necessary for compliance with a legal obligation** to which the controller is subject

[56] Rec. 4 GDPR.

[57] Ibidem.

[58] See *Schantz* in *Wolff/Brink*, BeckOK DatenschutzR[23] (2017) Art. 5 point 5.

[59] Rec. 40 GDPR.

[60] Rec. 39 GDPR.

[61] Art. 6(1) GDPR (arg: "**at least one** of the following"); see also *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 4 point 7.

[62] Art. 9(1) GDPR.

[63] Rec. 53 GDPR; *Weichert* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) Art. 9 point 4.

Co-funded by the Horizon 2020 Framework Programme of the European Union

d. processing is **necessary in order to protect the vital interests of the data subject** or of another natural person

e. processing is **necessary for the performance of a task carried out in the public interest** or in the **exercise of official authority** vested in the controller

f. processing is **necessary for the purposes of the legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[64]

Special categories of personal data, which consist (exclusively[65]) of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation require specific grounds of justification and are to be distinguished from Article 6(1) GDPR which are not applicable to processing of special categories of personal data.[66]

Regarding the processing of special categories of personal data**, Article 9(2) GDPR** states that even though processing of such categories is generally prohibited (Article 9(1) GDPR) unless one of the following justifications apply:

a. the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in Article 9(1) GDPR may not be lifted by the data subject;

b. processing is necessary for the purposes of carrying out the **obligations and exercising specific rights** of the controller or of the data subject **in the field of employment and social security** and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. processing is **necessary to protect the vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a **foundation, association or any other not-for-profit body** with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. processing relates to personal data which are **manifestly made public by the data subject;**[67]

[64] Art. 6(1) GDPR.

[65] *Albers* in *Wolff/Brink,* BeckOK Datenschutzrecht[23] (2017) DS-GVO Art. 9 point 13.

[66] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 9 point 18.

[67] Refer to Chapter 5.4 for a detailed description.

Co-funded by the Horizon 2020 Framework Programme of the European Union

f. processing is necessary for the establishment, exercise or defence of **legal claims** or whenever courts are acting in their judicial capacity;

g. processing is necessary for reasons of **substantial public interest, on the basis of Union or Member State law** which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of **health or social care** systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Article 9(3) GDPR;

i. processing is necessary for reasons of **public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. processing is necessary for **archiving purposes** in the public interest, **scientific or historical research** purposes or **statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[68]

These specific grounds of justification must be kept in mind when generating data through profiling, since even though it is not likely that a user will share that data within the intended purpose of the app, these data could be generated from data that has been shared by the user or shared via Social Media.[69]

Regarding **processing of photographs** it should be noted that even though, according to Recital 51 GDPR, "[sensitive] *personal data should include personal data revealing racial or ethnic origin*"[70], it does not mean that every photograph is to be considered of a special category of personal data. Recital 51 therefore states that "[t]*he processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person*" as additional data such as the mapping of facial structures would only then create such data.[71]

[68] Art. 9(2) GDPR.

[69] *Buchner* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) Art. 4 Nr. 4 point 7; *Wille* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 1151.

[70] "[...] whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races" as Recital 51 further states.

[71] See Recital 51 GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Also, data about the appearance are not in general "genetic data"[72] if such data cannot be established "uniquely" from such photographs.[73] However, photographs may contain personal data concerning health[74] in some cases, for example, if the person on the photograph is wearing glasses.[75] Other data that refers only to one's lifestyle and not to one's health, is not generally to be considered data concerning health, even though such data could be extracted from such data.[76] Applying the reasoning of the ECJ in the Breyer case regarding personal data this would depend on the means reasonably likely to be used by the controller to extract such data.

This means that photographs can, in some circumstances be sensitive personal data. However, if photographs are processed after they have been manifestly made public[77] or the data subject has given explicit consent[78], these photographs may be processed lawfully, even if they represent special categories of personal data.[79] If processing of photographs includes sharing them with the audience, the ground of justification should be that of explicit consent[80], since this would also be a matter of intellectual property law.[81]

Regarding processing of **personal data relating to criminal convictions and offences** or related security measures Article 10 GDPR states that these "*shall be carried out only under the control of official authority or when processing is authorised by Union or Member State law*."[82] In addition, "any comprehensive register of criminal convictions shall be kept only under the control of official authority", which means that the establishment of such a register would not be allowed within MARCONI. However, processing of such data is not envisaged. From all the possible grounds of justification of processing, the primary one will most likely be that of consent[83]. However, other grounds of justification, like the necessity for the performance of a contract to which the data subject is party[84], for compliance with a legal obligation to which the controller is subject[85] or for the purpose of legitimate interests pursued by the controller of by a third party[86] or even if processing relates to

[72] Art. 4(13) GDPR; Rec. 34 GDPR.

[73] See also *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 9 point 14.

[74] Rec. 35, Art. 4(15) GDPR.

[75] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 9 point 15.

[76] Also *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 9 point 15.

[77] Art. 9(2)(e) GDPR.

[78] Art. 9(2)(a) GDPR.

[79] *Weichert* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) Art.9 point 72.

[80] Art. 9(2)(a) GDPR.

[81] Refer to Chapter 9.

[82] "[P]roviding for appropriate safeguards for the rights and freedoms of data subjects"; Art. 10 GDPR.

[83] Art. 6(1)(a) or Art. 9(2)(a) GDPR.

[84] Art. 6(1)(b) GDPR.

[85] Art. 6(1)(c) GDPR.

[86] Art. 6(1)(f) GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

personal data which are manifestly made public by the data subject[87] may be relevant, in particular if consent to the processing cannot be achieved.

1.3.3.1 PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

Complementing the aforementioned grounds of justification, the principles relating to processing of personal data, as stated in Article 5 GDPR, must be adhered to.[88] The controller is responsible for, and has to be able to demonstrate compliance with these principles.[89] These principles are in a close relationship to Article 16 TFEU[90] and Article 8 of the Charter[91], meaning that they have to be interpreted in a manner that allows appropriate protection of personal data.[92]

According to the principles relating to processing of personal data (Article 5 GDPR), personal data shall be

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**');

b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) GDPR, not be considered to be incompatible with the initial purposes (**'purpose limitation'**);

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);

d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without undue delay (**'accuracy'**);

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**).[93]

---

[87] Art. 9(2)(e) GDPR.

[88] *Dienst* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 241.

[89] Art. 5(2) GDPR; *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) Art. 5 point 77f.

[90] Treaty on the Functioning of the European Union, OJ C 202 (2016).

[91] Charter of Fundamental Rights of the European Union (Charter), OJ C 326, 26.10.2012, 391–407.

[92] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 5 point 4.

[93] Art. 5(1) GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

In the Context of MARCONI, aside from the principle of lawfulness, which concerns the aforementioned grounds of justification of processing of personal data, the principles purpose limitation, data minimisation and storage limitation should also be kept in mind when building the architecture.[94]

1.3.4 RIGHTS OF THE DATA SUBJECT

Assuming that processing of personal data by the controller or processor is in accordance with the GDPR, Chapter III of the Regulation, which contains various rights of the data subject, will also have to be observed as well.[95] As part of the transparency principle, the controller shall inform the data subject of the existence of these rights.[96]

1.3.4.1 INFORMATIONAL DUTIES AND ACCESS TO PERSONAL DATA

It should be transparent to natural persons that personal data concerning them are collected, used, consulted and to what extent the personal data are or will be processed.[97] To "*ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed*"[98], various informational duties of the controller can be found within Chapter III (Section 1 & 2) of the GDPR.[99]

Articles 13 and 14 GDPR state that certain information has to be provided by the controller, at the time when personal data are collected.[100] The information the controller is obligated to provide differs, depending on whether personal data is collected from the data subject[101] or from sources other than the data subject[102].[103]

However, there are exceptions to these informational duties[104]:

- if the data subject already has the information[105] or
- if the data is not collected from the data subject itself:

---

[94] *Dienst* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 241f.

[95] *Schrey* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 602.

[96] See immediately below.

[97] Art. 5(1)(a) GDPR.

[98] Rec. 39 GDPR.

[99] Art. 12f GDPR.

[100] *Schrey* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 619.

[101] Art. 13 GDPR.

[102] Art. 14 GDPR.

[103] *Schrey* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) points 621 & 622.

[104] *Bäcker* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) Art. 12 point 19f.

[105] Art. 13(4) and 14(5)(a) GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- if the provision of such information proves impossible or would involve a disproportionate effort[106] or
- if obtaining or disclosure is expressly laid down by Union or Member State law[107] or
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.[108]

To provide the necessary information, standardised icons that will be determined by the Commission in accordance with Articles 12(8) and 92 GDPR, should be used when providing the necessary information of Article 13 or 14 GDPR.

In addition to the information the controller has to provide at the time when personal data is obtained (Articles 13 or 14 GDPR), the data subject also has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the certain information, specifically:

a. the purposes of the processing;
b. the categories of personal data concerned;
c. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f. the right to lodge a complaint with a supervisory authority;
g. where the personal data are not collected from the data subject, any available information as to their source;
h. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[109]

[106] Art. 14(5)(b) GDPR.

[107] Art. 14(5)(c) GDPR.

[108] Art. 14(5)(d) GDPR.

[109] Art. 15(1) GDPR; *Schrey* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 631f ("Right of access by the data subject").

Co-funded by the Horizon 2020 Framework Programme of the European Union

These informational duties stated in Articles 13, 14 and 15 GDPR should provide the data subject with the means to exercise their rights to rectification, erasure or data portability.[110] For further information as well as a template please refer to Chapter **Error! Reference source not found.**.

1.3.4.2 RECTIFICATION, ERASURE AND PORTABILITY

A significant right granted to data subjects by the GDPR is the **right of erasure** (Article 17 GDPR) according to which the controller has the obligation to erase personal data without undue delay where one of the following grounds applies[111]:

a. the personal data are **no longer necessary** in relation to the purposes for which they were collected or otherwise processed[112];

b. the data subject **withdraws consent** on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is **no other legal ground** for the processing;

c. the **data subject objects to the processing** pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);[113]

d. the personal data have been **unlawfully processed**;

e. the personal data have to be **erased for compliance with a legal obligation** in Union or Member State law to which the controller is subject;

f. the personal data have been collected in relation to the **offer of information society services referred to in Article 8(1)**.

In addition, according to Article 17(2) GDPR, where the controller has made the personal data public and is obliged pursuant to Article 17(1) to erase personal data, the controller, *"taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data*".[114]

---

[110] *Bäcker* in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 13 point 8.

[111] Art. 17(1) GDPR; Peuker in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 17 point 1f.

[112] This correlates with the Principles of „purpose limitation" and „storage limitation" as stated in Art. 5(1)(b)&(e) GDPR (*Peuker* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 17 point 16); regarding the Principles of Processing refer to Chapter 1.3.3.

[113] This concerns data that is processed on the ground of legitimate interests according to Art. 6(1)(f) (or on a task carried out in the public interest/in exercise of official authority Art. 6(1)(e)) Art. 21(1). In case of processing for marketing purposes (including profiling), this right to object cannot be overridden by legitimate interests of the controller; see *Peuker* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 17 point 21f.

[114] Art. 17(2) GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

The term "right to be forgotten" originates from the ECJ ruling in the case Google Spain,[115] wherein the right to erasure has been empowered in the sense, that even search engines would be required to delete indices of websites containing personal data, that would appear to be, "*having regard to all the circumstances of the case, […] inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing, even if published lawfully*".[116] Article 17(2) GDPR now includes an obligation of the controller, which originally published the personal data in question, to inform other controllers, which again are obligated to erase said data if Article 17(1) GDPR applies.[117] However, considering the wording of Article 17(2) GDPR, this obligation will only be applicable to the controller if the data subject expressly claims his right.[118]

Article 17(3) GDPR states exceptions to the right to erasure, which apply to the extent the processing is necessary:

a. for exercising the right of freedom of expression and information;

b. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in Article 17(1) GDPR is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e. for the establishment, exercise or defence of legal claims.[119]

According to Article 16 GDPR, data subjects may obtain from the controller without undue delay the **rectification** of inaccurate personal data concerning him or her, or to have incomplete personal data completed.[120]

Also, Article 20 GDPR now grants the data subject the right (if the data subject has provided personal data concerning him or her to a controller), to receive said data in a structured, commonly used and

[115] ECJ 13 May 2014, C-131/12 ("Google Spain und Google") ECLI:EU:C:2014:317.

[116] ECJ 13 May 2014, C-131/12 ("Google Spain und Google") ECLI:EU:C:2014:317, Rec. 94.

[117] *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 17 point 67f.

[118] *Haidinger*, Die Rechte auf Löschung, Berichtigung, Einschränkung und Datenübertragbarkeit nach der DSGVO (Teil XI), Dako 2017/34, 56(57); Herbst in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 17 point 50.

[119] Art. 17(3) GDPR; *Herbst* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) Art. 17 point 70.

[120] Art. 16 GDPR; which is less detailed than the similar Art. 12(b) Data Protection Directive (*Peuker* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art.16 point 3).

Co-funded by the Horizon 2020 Framework Programme of the European Union

machine-readable format or to have it transmitted to another controller where technically feasible ("**data portability**").[121]

1.3.4.3 RIGHT TO OBJECT

According to Article 21, the data subject has the right "to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions."[122]

If the data subject objects to these processing activities, the controller may no longer process the personal data unless the controller demonstrates

- either legitimate grounds for processing that override the interests, rights and freedoms of the data subject
- or that the processed data are used for the establishment, exercise or defence of legal claims.

In case of processing for direct marketing purposes, the personal data shall no longer be processed if the data subject objects to processing for such purposes, regardless of legitimate interests on the controller's side.[123]

The right to object also exists in regard to processing for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) GDPR. However in this case, processing may continue, if the processing is necessary for the performance of a task carried out for reasons of public interest.[124]

1.3.5 ORGANISATIONAL AND OTHER REQUIREMENTS

The GDPR can also be seen as a reaction to the challenges for the protection of personal data resulting from rapid technological developments and globalisation, like the scale of the collection and sharing of personal data and the technology to make use of personal data on an unprecedented scale.[125]

The controller as well as the processor shall maintain a **record of processing activities** (Article 30 GDPR) which serves as a form of self-check and re-emphasizes the importance of responsibility the controller or the processor must bear.[126] It should also permit towards Supervisory Authorities compliance with the GDPR.[127] Each controller shall maintain records of all processing activities[128], each processor shall

[121] Art. 20 GDPR; *Sydow* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 20 point 5.

[122] Art. 21(1) GDPR; this includes processing activities on the grounds of legitimate interests (Art. 6(1)(f); refer to Chapter 5.3 and 5.4).

[123] Art. 21(2)&(3) GDPR; *Feiler/Forgo*, EU-DSGVO (2017) Art. 21 point 6.

[124] Art. 21(6) GDPR; *Feiler/Forgo*, EU-DSGVO (2017) Art. 21 point 6.

[125] Rec. 6 GDPR; see also: *Mantz* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 32, point 1.

[126] *Ingold* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 30 point 1.

[127] *Voigt*, *von dem Bussche*, The EU General Data Protection Regulation (GDPR) (2017) 3.

[128] Article 30(1) GDPR; *Ingold* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 30 point 10f.

Co-funded by the Horizon 2020 Framework Programme of the European Union

maintain records of all categories of processing activities[129]. In turn, most of the notification obligations have been removed.[130] For more information concerning the record of processing activities please refer to Chapter **Error! Reference source not found.**.

In order to comply with GDPR frameworks it is important to procure an impact assessment, thereby listing all processing steps alongside with the individual purpose and how personal rights of data subjects might be infringed or discriminated.[131] According to Art. 32 GDPR, controller and processor should implement "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".[132] For more information refer to Chapter 8.

Where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller has to carry out a **data protection impact assessment**[133] to evaluate, in particular, the origin, nature, particularity and severity of that risk, prior to the processing.[134] If this impact assessment indicates a high risk, which cannot be mitigated, the supervisory authority should be consulted.[135] To clarify what processing activities will require a Data Protection Impact Assessment, Supervisory Authorities might issue black- and whitelists.[136] Please refer to Privacy by Design in Chapter 8.1 for more information.

Public authorities, as well as a controllers (or processors) whose core activities[137] either require regular and systematic monitoring of the data subjects on a large scale, or the processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, shall designate a **data protection officer**.[138] This should be a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation.[139]

Additionally each controller should – taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing – implement appropriate technical and organisational measures to integrate the necessary safeguards into the processing and that, by default, only personal data which are necessary for each specific

[129] Article 30(2) GDPR; *Ingold* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 30 point 19f.

[130] See also Rec. 89 GDPR.

[131] See *Sassenberg/Schwendemann* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 35 point 40.

[132] Art. 32(1) GDPR; see Chapter 8 (Privacy by Design and Default Measures).

[133] See Chapter 8.4.

[134] Rec. 84, 89 and 90 as well as Article 35 GDPR.

[135] Art. 36 GDPR.

[136] *Voigt/von dem Bussche*, The EU General Data Protection Regulation (GDPR) (2017) 3.

[137] Processing of personal data must be the „core activity". It is not necessary, however, that such processing is the business purpose itself, but a necessary precondition. (*Helfrich* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 37 point 63).

[138] Rec. 97 and Art. 37 GDPR; *Bergt* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) Art. 37 point 18.

[139] Rec. 97 GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

purpose of the processing are processed (principles of "**Privacy-by-Design**" and "**Privacy-by-Default**").[140] Refer to Chapter 8.

The right of the data subject to gain knowledge of **data breaches**, if they are likely to result in a high risk to the rights and freedoms of natural persons[141] (Article), also is an application of the principle of transparency.[142]

1.3.6 SUPERVISORY AUTHORITIES AND PENALTIES

According to Article 52 GDPR, supervisory authorities shall act with complete independence[143] in performing its tasks and exercising its powers in accordance with this Regulation[144], which is important, since the fines, these supervisory authorities may issue, are up to 4% of the global annual turnover or up to 20 million Euros, depending on which amount is higher[145]. In terms of privacy, supervisory authorities are also known as Data Protection Authorities (DPAs).

Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.[146]

Similarly[147] to the Data Protection Directive[148], when processing concerns different supervisory authorities, i.e. where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority[149]. This lead authority should, cooperate with the other supervisory authorities concerned.[150]

Other supervisory authorities may handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only

---

[140] Rec. 78 and Art. 25 GDPR; see Chapter 8 (Privacy by Design and Default Measures).

[141] Art. 34(1) GDPR; provided that none of the conditions of Art. 34(3) GDPR are met, in which case the data subject does not need to be informed of the data breach.

[142] *Schrey* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 736.

[143] Which is not in conflict with national principles of democracy; *Ziehbarth* in *Sydow,* Europäische Datenschutzgrundverordung (2017) Art. 52, point 2; ECJ 09.03.2010, C-518/07 ("Commission v Germany") ECLI:EU:C:2010:125.

[144] Art. 52(1) GDPR.

[145] Art. 79f GDPR.

[146] Art. 55(1) GDPR.

[147] *Ziehbarth* in *Sydow,* Europäische Datenschutzgrundverordnung (2017) Art. 55, point 2.

[148] Art. 28(6) Data Protection Directive.

[149] Art. 56(1) GDPR.

[150] Rec. 124 GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

processing carried out in a single Member State and involves only data subjects in that single Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter, after which the lead supervisory authority should decide, whether it will handle the on cooperation between the lead supervisory authority and other supervisory authorities concerned ('**one-stop-shop mechanism**'[151]), or whether the supervisory authority which informed it should handle the case at a local level. [152]

[151] *Dix* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) Art. 56 point 17.

[152] Rec. 127 GDPR.

Co-funded by the Horizon 2020
Framework Programme of the European Union

2 Architecture, Data Collection and Structures

2.1 Architecture

The MARCONI consortium consists of three radio stations being VRT[153], NPO[154], and Stadtfilter[155] as well as PLUXBOX[156], JRS[157], IN2[158] and Faction XYZ[159] as technical partners including the University of Hasselt[160] and the University of Vienna.[161] While the project remains a work in progress while MARCONI is being developed, partners will each process and share personal data for testing and development purposes between each other. In the following section, data flow will be elaborated and explained by reference to flowcharts and diagrams.

Data will be **collected** through three major applications, two of which are now compiled into a minimum viable product. Users will have the opportunity to engage with a radio station of their choice through a webpage, a smartphone application or a chatbot implementation designed for the Facebook Messenger.[162]

Data will be **processed** by the consortium partners with the exception of the University of Vienna. Personal data will be saved in databases which are controlled by their respective owners; datasets are being shared between them. While PLUXBOX provides the modalities for an audience and artist database, IN2 stores chatlogs to create an index providing metadata analysis in order for search queries to be performed. Faction XYZ as well as JRS handle message logs and multimedia items in order to train DLNNs as well as other algorithms to assure good performance of the chatbot.

In order to ensure compliance with data protection frameworks it must be identified **which data** will be used for **which purpose** and under **which legitimate basis**. Data must be classified through a risk-based approach as outlined in Chapter 8. Security measures must be taken where natural persons must be specifically protected from negative impacts by a potential **data breach**. Concerning data protection and role allocation please refer to Chapters 1.3.5 and 4.

Radio stations will be able to query and retrieve related data from the audience database of MARCONI in order to complete their own registries and databases. Users will be informed about where their data will be saved and who will remain in control of it.

---

[153] Vlaamse Radio- en Televisieomroeporganisatie (https://www.vrt.be/en/contact/).

[154] Nederlandse Publieke Omroep (https://over.npo.nl/).

[155] Radio Stadtfilter (http://stadtfilter.ch/kontakt/).

[156] Pluxbox (https://pluxbox.com/about).

[157] Joanneum Research (https://www.joanneum.at/joanneum/impressum/).

[158] IN2 Digital Innovations (https://in-two.com/imprint).

[159] Faction XYZ (https://www.faction.xyz/about/).

[160] Universiteit Hasselt (https://www.uhasselt.be/OverUHasselt).

[161] University of Vienna (https://www.univie.ac.at/en/imprint/).

[162] Facebook Messenger (https://www.messenger.com/).

Co-funded by the Horizon 2020 Framework Programme of the European Union

MARCONI currently consists of several services which are composed of:

- A profiling service and audience database
- A communication service
- A radio station interface
- A chatbot and related algorithm training
- A service to like and remember music
- Artist database for referencing
- An analytics database
- Visual location matching and classification
- Face detection and recognition
- Sentiment analysis
- Social media analysis
- Named entity recognition
- Topic detection
- Content filtering and clustering

These processing operations are being performed by the responsible consortium partner as highlighted in Figure 1 as it provides an overview on the architecture of MARCONI, in particular concerning data collection, data types and dissemination. The dataflow will be further outlined below.

Co-funded by the Horizon 2020
Framework Programme of the European Union

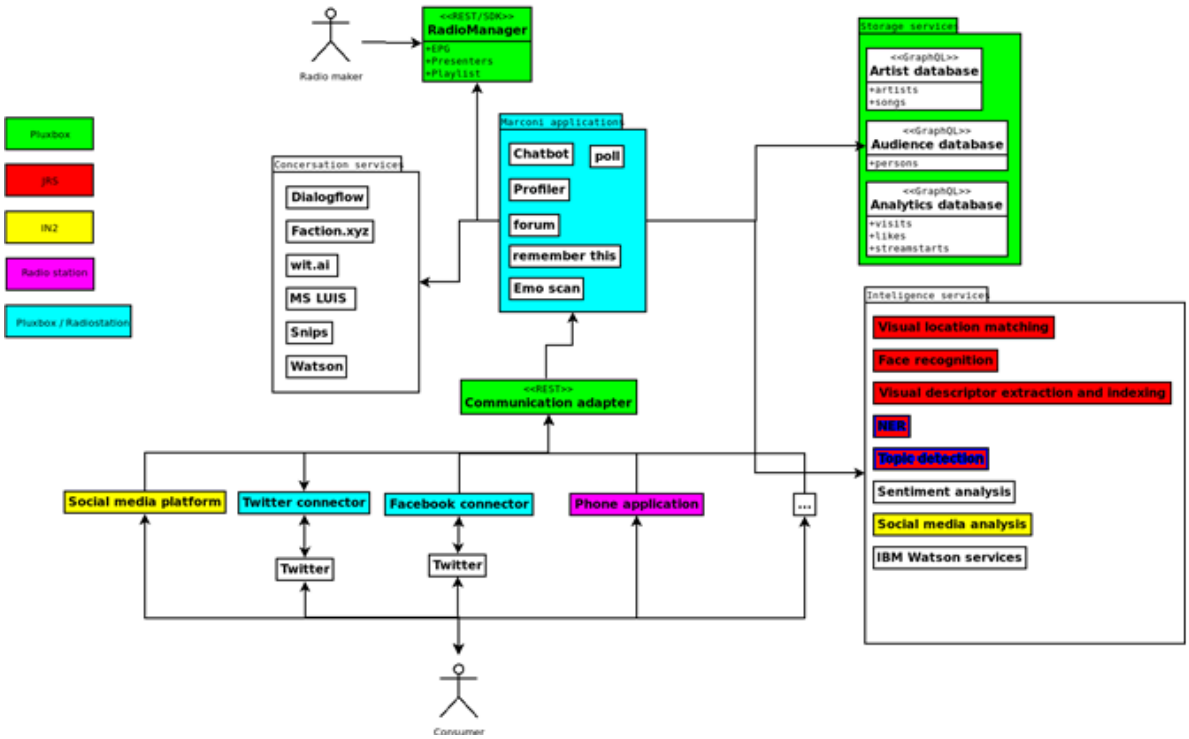

Figure 1: Architecture of MARCONI

MARCONI, when deploying its services to the end user, pays special attention to respect the data subject's rights and will, without a voluntary registration of the user through the web interface (Figure 2), only collect the necessary data to stay in contact with him or her. This means, that in the event the data subject enters text in the chatbot interface on a MARCONI website, an anonymous user profile will be generated to map individual interaction with the system in a single user session. Should a user choose to register, a permanent profile will be created with the optional possibility to add further information about her- or himself in order to personalise the user experience.

This can happen either by providing a name, an email address, locations or associated social media presence such as Facebook or Twitter.

When the subject interacts with MARCONI, information containing personal data about him will be saved in the audience database via a query language (GraphQL). From there, user data will be shared with other consortium members in order to fulfil their respective needs such as algorithm training and metadata extraction in order to provide radio stations with necessary information for future use. This information can be related to current events, market analysis and music preferences to provide feedback to radio editors.

Co-funded by the Horizon 2020
Framework Programme of the European Union

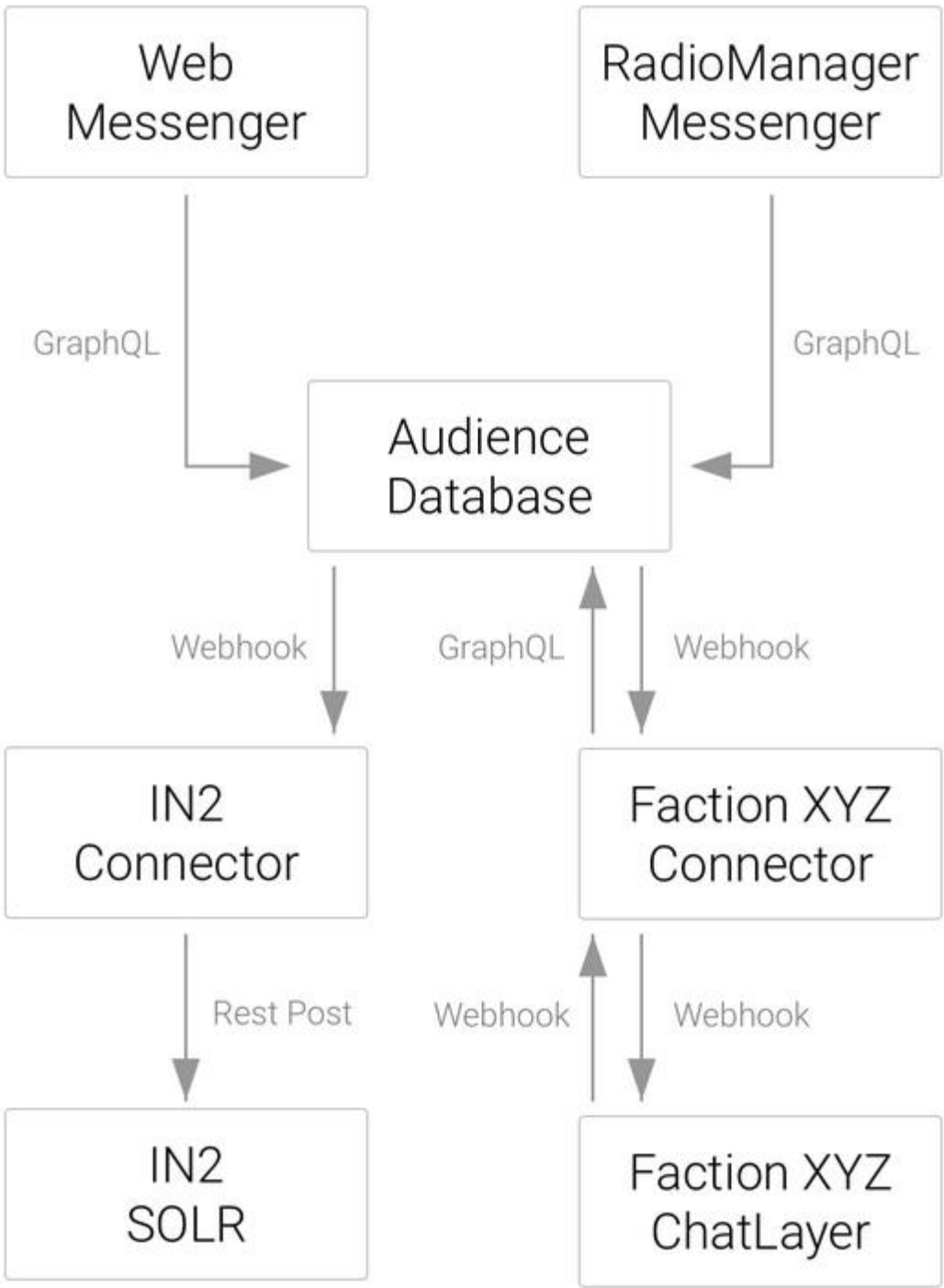

Figure 2: Sprint 2 architecture

Co-funded by the Horizon 2020 Framework Programme of the European Union

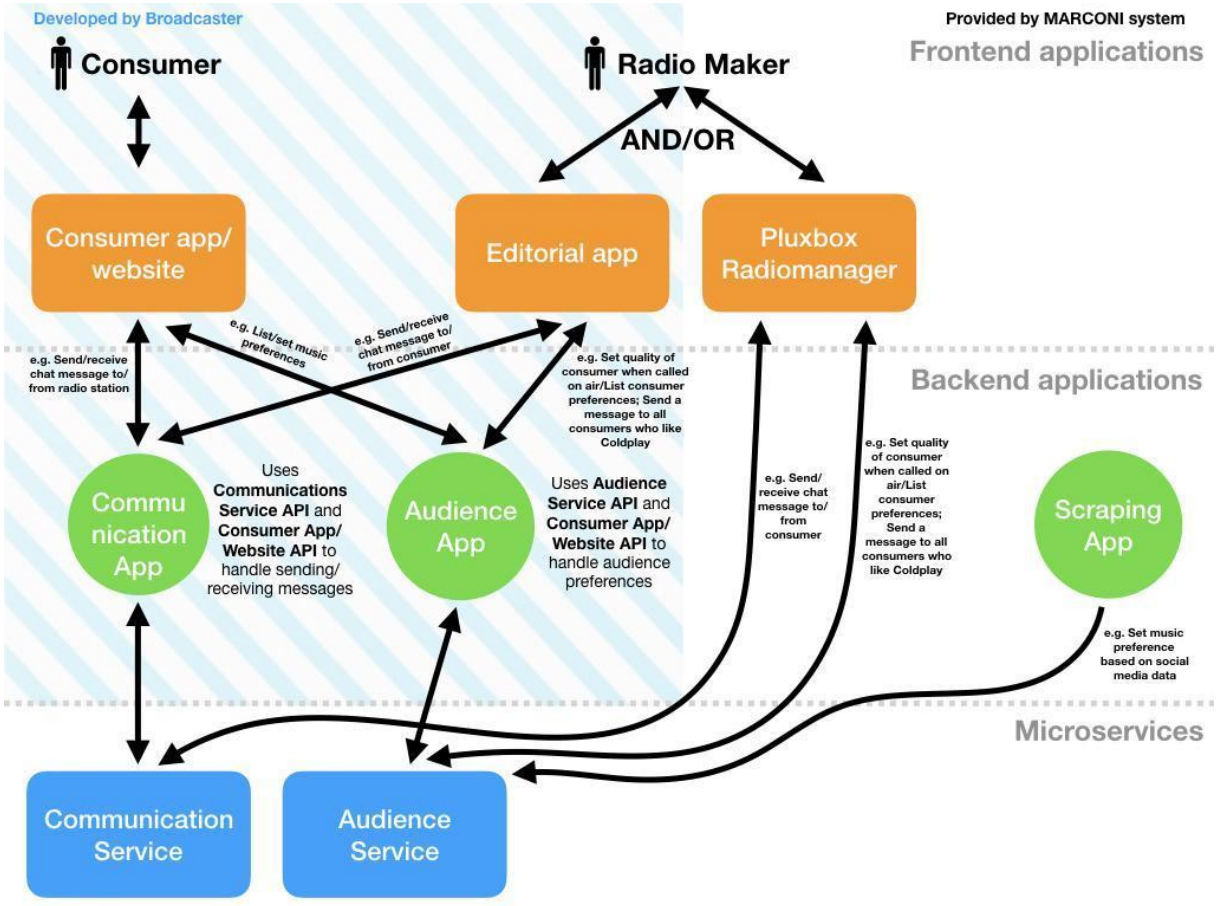

Figure 3 – MARCONI Backend

Figure 3 shows an example communication between the consumer and the radio station, showing that the radio station will be able to provide their own apps as well as the backend of MARCONI, the only frontend application being the PLUXBOX radio manager and a "scraping app" being responsible for collecting information off traffic and necessary packets from the dataflow between consumer and broadcaster in order to provide its necessary services.

2.2 MARCONI – Data Collection Policy

- MARCONI will process the subject's preferences regarding music and social events for the purpose of designing a personal radio broadcast.
- MARCONI will conduct market analysis in terms of getting to know its audience on an individual basis for the purpose of employing user content into the show and to gain relevant feedback for the broadcaster.
- MARCONI indexes texts posted by social media accounts for topic detection in order to make them searchable for relevant content. This also includes contacting the user via automated means to inform him of broadcasts of interest as well as invitations to contribute with personal content.
- MARCONI will classify social media accounts and markers such as "hashtags" in order to observe how they impact the audience.

Co-funded by the Horizon 2020 Framework Programme of the European Union

The main reason for justification is consent by the user (Article 6(1) (a) GDPR). In some cases, a weighing of interest (Article 6(1) (f) GDPR) may be necessary, in particular, when consent has been withdrawn. In addition, the fact that data has been made available to the public will be very relevant for the justification of processing.

In some cases, a privacy impact assessment according to Article 35 GDPR is recommended by some opinions in current literature.[163]

2.3 Data Types and Structures

The following tables present a technical presentation of the data types and structures of MARCONI. A detailed evaluation in terms of data protection and personal data can be found in Data Types in Detail.

[163] Refer to Chapter 8 (Privacy by Design and Default Measures) for a more detailed description.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Table 1: Data Types and Structures

Data item	Type	Notes	Cardi-nality	External references/links	Uses	Storage duration	Anonymisable
User	ID /URI	User who registered with a MARCONI service	1				no
Name	Text		1+		Identification	while registered	no
Age / DoB	Integer / Date		0-1		Content customisation, Notifications	while registered	when aggregated
Gender	controlled value		0-1		Content customisation, Notifications	while registered	when aggregated
Place	Place		0+		Content customisation, Notifications	while registered	when aggregated
(additional user data)							
User social media account	ID		0+	ID/URI of external service	Link to other communication channels, Access to profile metadata	when provided and not revoked	no
Relation	ID /URI		0+		Sharing content with groups, Content customisation	while registered	Target of relation can be anonymised
type	controlled vocabulary		1				
target	Person		1				
Client	Client	Client devices known to be used by the user	0+		Adapt content to device, Interaction possibilities offered	while registered	when aggregated
Preference	ID / URI	Like, rating, derived from other info	0+	Target may be external entity (song, artist, place, …)	Content customisation, Notifications	while registered	when aggregated

Co-funded by the Horizon 2020 Framework Programme of the European Union

		target	URI	the object of the preference expression					
		score	double [-1;+1]						
	Content consumption		ID / URI	Content item consumed	0+		Content customisation, Notifications	Few months, raw data can be discarded when aggregate or preferences have been mined	when aggregated
		Target	URI		1+	Target may be external entity (song, video)			when aggregated/classified
		Date	Date		0+			Days to months	
		Client	Client	client device(s) used for the content consumption	1+			Days to months	
Person			ID/URI	not a user – probably user can be modelled as specialisation of person		Could be pointing to database/vocabulary of artists, etc.		When used a target of relation of a user, or a certain max. time after last interaction with the system	May be anonymised (e.g. only an ID may be known)
	User social media account		ID		0+	ID/URI of external service		max. time after last interaction with the system	May be only a handle

Co-funded by the Horizon 2020 Framework Programme of the European Union

Content item		URI			URL of social media content		Unlimited (if station/professional, rights explicitly granted), while user is registered	yes
	Type	Controlled value (Text, image, video, audio)		1				n/a
	Provenance	Controlled value (radio station, UGC, other professional)						n/a
	Location	Place		0+				If contributor is decoupled
	Date			0+				If contributor is decoupled
	Contributor	URI		1+			While user is registered with system	Can be stored separately (but should be kept for copyright record)
	other technical media item properties			0+				n/a
Place		URI	Known location		vocabulary such as Geonames, TGN, etc.		unlimited	n/a
	Geo-coordinates	long/lat/alt tuple	possible multiple to represent polygon	0+			unlimited	n/a
	Name	string [+language id]		0+			unlimited	n/a

Co-funded by the Horizon 2020 Framework Programme of the European Union

Event		ID / URI	real-world event related to the programme or interactions				unlimited	n/a
	editorial item	ID/URI	reference to related programme item(s)/campaign in RadioManager	0+			unlimited	n/a
	Person	Person	involved persons	0+			unlimited	No, but concerns only published information
	location	Place	involved locations	0+			unlimited	n/a
	Date	date, date range, list of dates, recurring date		0+			unlimited	n/a
Interaction		ID/URI	assumption is that all incoming and outgoing action or content items that involve consumers are modelled using interactions		URL of social media interaction		Day to months (until aggregated or preferences have been inferred)	when aggregated
	Involved users	ID		1+				when aggregated
	action		part of an interactions that is not a content item, but a button click, service call, content consumption, …					when aggregated

Co-funded by the Horizon 2020 Framework Programme of the European Union

		type	ID/URI		1				
		content	key/value list	describing details of the action, contains identifiers of preferences, content consumptions, relations, etc. expressed through the action	0+				when aggregated
	content items		ID		0+				when aggregated
		ordering/threading of items in interaction	ref. to predecessor / follower/ parent + qualification of link		0+				
	channel		ID (controlled set of communication channels)		1+				when aggregated
	editorial item		ID/URI	reference to related programme item(s)/campaign in RadioManager	0+				n/a

Co-funded by the Horizon 2020 Framework Programme of the European Union

Client device			ID (maybe with type, e.g. IMEI)	HW or SW client	1+	could point to an external database of HW devices/SW environments		While device type is still in use	n/a
	Name		String		0+				
	Manufacturer		ID / URI		0+				
	Type		controlled vocabulary	e.g., mobile phone, tablet, browser	1				
	Related client		Client device	e.g., HW on which SW is running	0+				
Analysis			ID / URI	description of content analysis job				As long as results are used in order to document provenance	n/a
	profile		ID/URI	analysis profile/set of modules being applied	1+				n/a
		setting	key/value list of settings		0+				
	content		Content item	item(s) being analysed (at least one content item or interaction must be specified)	0+				n/a
	interaction		Interaction	Interaction(s) being analysed (at least one content item or interaction must be specified)	0+				If processing sufficiently aggregates
	results		JSON structure,		1+				Depends on whether input

Co-funded by the Horizon 2020 Framework Programme of the European Union

		see separate proposal						contained personal data, and processing sufficiently aggregates
	date	date	time/date of analysis	1+				n/a
	machine	ID /URI	ID of machine(s) where analysis has been performed	1+				n/a
Inference		ID /URI	inference of information				As long as results are used in order to document provenance	n/a
	profile	ID/URI	inference profile/set of modules being applied	1+				n/a
	setting	key/value list of settings		0+				
	source	ID/URI	any stored data item or analysis result	1+	may include external data (note that persistence of external sources may be beyond control of the system)			n/a
	result	ID / URI	data item created/modified as a result	0+				Depends on whether input contained personal data, and processing sufficiently aggregates

Co-funded by the Horizon 2020 Framework Programme of the European Union

		type	controlled set of values (created, modified, invalidated)		1				
	date		date	time/date of inference	1+				n/a
	machine		ID /URI	ID of machine(s) where inference has been performed	1+				n/a
Training			ID /URI	training/customisation of analysis or inference modules				While retraining is needed, or while user owning data is registered with the system	n/a
	profile		ID/URI	inference profile/set of modules being affected	1+				n/a
		setting	key/value list of settings		0+				
	source		ID/URI	any stored data item or analysis result	1+	may include external data (note that persistence of external sources may be beyond control of the system)			No, as long as source data shall be available for retraining
	date		date	time/date of training	1+				n/a
	machine		ID /URI	ID of machine(s) where training has been performed	1+				n/a

Co-funded by the Horizon 2020 Framework Programme of the European Union

3 Evaluation of Data Types and Structures

Each data type of MARCONI will be assessed according to its particular legal status, e.g. in respect to data protection rights or IP rights. Depending on the category, special legal provisions apply.

To determine whether a natural person is identifiable, all means should be considered which would be reasonably likely to be used by the controller or any other person to identify the natural person directly or indirectly.[164] According to Article 4(1) GDPR a person can be identified directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This means that movement profiles through geo-information can constitute personal data[165].

It has been controversially discussed whether relative or absolute criteria had to be used to establish reasonable likeliness of identifiability.[166] Using absolute criteria would mean that the definition of 'personal data' is being met as soon as anyone would have the possibility to connect the processed data to an individual. Within the famous "Breyer" case, the ECJ applied a relative approach to determine whether a person is identifiable.[167] According to the ECJ, a data subject is identifiable not only if the controller can gain access to additional information without **disproportionate effort** in terms of time, cost and manpower[168] but also if a legal channel exists that would allow third parties to identify the data subject.[169] Regarding "tools" for extracting personal data out of aggregated data: if only specialised software that is usually employed by intelligence agencies are up to this task, the effort would almost always be disproportionate.[170] However, if sufficient background knowledge is available, an attacker may conduct successful re-identification through the means provided by the use of auxiliary information.[171] For more information see Chapter 1.3.2.

3.1 Overview of Data Types

- Personal data according to Article 4(1) GDPR

[164] *Schild* in BeckOK DatenschutzR DS-GVO (2018) Article 4, points 14-21.

[165] *Bergauer* in *Knyrim*, Datenschutz-Grundverordnung (GDPR) – das neue Datanschutzre4cht in Österreich und der EU (2016), 54.

[166] *Voigt*, Datenschutz bei Google, MMR 2009, 377; *Bergt*, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, 365.

[167] ECJ 19 October 2016, C-582/14 ("Breyer") ECLI:EU:C:2016:779.

[168] ECJ 19 October 2016, C-582/14 ("Breyer") ECLI:EU:C:2016:779; Rec. 26 GDPR.

[169] ECJ 19 October 2016, C-582/14 ("Breyer").

[170] *Marzi/Pallwein-Prettner*, Datenschutzrecht auf Basis der DS-GVO (2018) 22.

[171] *Narayanan/Shmatikov*, Robust De-anonymization of Large Sparse Datasets, 2008 IEEE Symposium on Security and Privacy, (2008) 113.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Data according to Article 4(1) GDPR ("normal personal data") can be processed on the basis of various grounds according to Article 6(1) GDPR. It can, for example, be based either on consent[172] or weighing of interests[173] under Article 6(1)(f).[174]

- Special categories of personal data according to Article 9 GDPR

Processing data according to Article 9 and 10 GDPR requires the compliance with the processing requirements of Article 9(2) GDPR. Of particular interest are the justifications in Article 9(2)(a) and (e), e.g. consent of the user or data made public by the data subject (such as public posts on social media platforms). Consent must be explicit when concerning sensitive data, which is a higher threshold than in Article 6(1) GDPR.[175]

The condition 'made public' by the data subjects applies if the data subject releases data into a public space.[176] Therefore, if such special categories of data are processed without consent, Article 9(2)(e) GDPR could be applicable. An analogy of this clause regarding non-sensitive data should be used.[177] An *argumentum a maiore ad minus* is possible since processing data that is not encompassed by the categories of Article 9 is not even in need of said special grounds of justifications. Refer to Chapter 5.4 for more information.

- Pseudonymised data

Pseudonymisation of data is a method of privacy by design. In case of MARCONI, it should be used as much as possible. Even if the link between data and an identifier of the data subject (e.g. name) is deleted/replaced, the data subject might still be identifiable.[178] This means that disguised identities are personal data.[179]

- Anonymised data: non-personal data

In contrast to pseudonymised data, anonymised data is no longer personal data. Therefore it does not fall under the scope of the GDPR. According to Recital 26 GDPR it is described as "*information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable*".

---

[172] Art. 4(1)(a) GDPR.

[173] ECJ 24 November 2011, Case C-468/10 ("ASNEF") ECLI:EU:C:2011:777, Rec. 44: In relation to the balancing which is necessary pursuant to Article 7(f) of Directive 95/46, it is possible to take into consideration the fact that the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources.

[174] See Chapter 1.3.3 (overview) and Chapter 4.4 for a more extensive description of the most relevant legal grounds of processing.

[175] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 9 point 21.

[176] *Haas* in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018) Die Verarbeitung besonderer Kategorien personenbezogener Daten, 67.

[177] As described in Chapter 5.4.

[178] WP29, Opinion 05/2014 on Anonymisation Techniques WP 187 (2014).

[179] *Ernst* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 9.

Co-funded by the Horizon 2020 Framework Programme of the European Union

One way to achieve anonymisation would be that of aggregation.[180] In this case data, that would individually be considered personal data, could no longer be traced back to a certain individual data subject, but rather to a group big enough that, considering the state of the art of technology, an individual could not be identified by means reasonably likely to be used.[181] Such a group could be created by collectively processing data of a larger geographical area. The problem with this approach could be, that certain services such as training the chatbot require personal data to operate as planned. To ask the question of in how far a certain service requires personal data is – just as the question of in how far pseudonymising is possible – a necessary precondition for privacy-by-design.

- Data made public by the data subject

When information is publicly available, it is generally treated differently than information that only a limited number of persons have access to. This also applies to personal data. Personal data is "made public" if the subject releases data into a public space.[182] It is not necessary that a certain amount of people actually take notice of this information. The accessibility to an indefinite number of people is therefore sufficient.

If a social media account should disclose information without the consent of the data subject the processing would still be lawful, as long as the data is not linked or connectable to said individual which could happen for example through aggregation. However, most of the time this will not be possible because it is impossible for data collection systems to identify which information has been made public in a lawful manner. For a detailed evaluation of publicly available data refer to Chapter 5.4.

- Copyright[183]

Contributions may be sufficiently innovative to be eligible for the copyright protection. In such cases, the author should have to grant a non-exclusive right to the radio station. It is required that a provision exists for such potential cases.

- Right to one's own image[184]

According to the ECHR a "person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development.

3.2 Data Types in Detail

In the following section, each dataset will be evaluated and classified. Since all datatypes within a dataset are linked, the resulting possibility of identifying a person must be taken into account. Roughly, a dataset contains personal data if a datatype can, via processing of additional and available data, lead to identification, if datatypes in the set can, via combination, be used to identify a natural person or the datatype is identifying itself as outlined in the previous Chapter 3.1.

We can classify datatypes to fit into three categories:

- Personal data according to Article 4(1) or 9(1) GDPR.
- Possibly personal data and legal grey areas.
- Only personal data when linked with additional data.[185]

Co-funded by the Horizon 2020 Framework Programme of the European Union

3.2.1 USER

The primary justification for storage of user data is consent. For this consent to be valid the user has to know all relevant circumstances of the processing of his data (Article 7 GDPR)[186]. Normally, the radio operator publishes a privacy policy which the user agrees to. The user can withdraw his consent at any time. In this case, the data might have to be deleted (Article 17 GDPR). Some data may alternatively be anonymised and retained in the system.

3.2.1.1 NAME

As the Name of the data subject, often combined with his date of birth which can be obtained by consulting a register of residents, is a primary source of identification of every natural person, it is considered personal data in the sense of Article 4(1) GDPR.

Obtaining this information is important in order to know for whom a service is performed. Therefore it can – depending on the service – be considered legitimate to process this data, if anonymised processing is not an option.

If a certain service can operate using only anonymised data, it should be implemented accordingly, as principle of data minimisation prescribes. It is also an application of privacy by design.

Deleting datatype **NAME** from a certain data set does not necessarily result in anonymisation of said data set.[187] The data set could still contain certain identifiers that could be used to identify the data subject. However, deleting the name from a data set and replacing it with a pseudonym ("pseudonymising")[188], still minimizes potential risks of a data subject in case of a data breach and should therefore be applied whenever possible.[189]

3.2.1.2 AGE/DATE OF BIRTH

The birthdate of a natural person can also be treated as personal data that is in need of anonymisation once the time for lawful processing has expired since it is objectively possible to identify the data subject by his date of birth by again employing additional data[190] of the set, for example a register of

---

[180] Refer to WP29, Opinion 05/2014 on Anonymisation Techniques WP 187 (2014); *Haimberger/Geuer*, Anonymisierende Wirkung der Pseudonymisierung Dako 2018/33, 57; *Haidinger*, Der Weg von personenbezogenen zu anonymen Daten, Dako 2015/34, 56.

[181] *Rücker* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 82f.

[182] *Haas* in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018) Die Verarbeitung besonderer Kategorien personenbezogener Daten, 67.

[183] Regarding Copyright and the Right to one's own image refer to Chapter 9.

[184] Regarding Copyright and the Right to one's own image refer to Chapter 9.

[185] *Ernst* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 4 points 8 & 11.

[186] AG Kehl, Urt. v. 29.04.2016 - 2 Cs 303 Js 19062/15.

[187] WP29, Opinion 05/2014 on Anonymisation Techniques WP 187 (2014).

[188] Article 4(5) GDPR.

[189] See Chapter 8 (Privacy by Design and Default Measures).

[190] ECJ 19 October 2016, C-582/14 ("Breyer") ECLI:EU:C:2016:779 Rec. 46; Opinion of the Advocate General, C-582/14, Rec.

Co-funded by the Horizon 2020 Framework Programme of the European Union

residents and location data. In general terms, a natural person can be considered “identified” when, within a group of persons, he or she is "distinguished" from all other members of the group. Accordingly, the natural person is “identifiable” when, although the person has not been identified yet, it is possible to do so[191]. In order to avoid the need of data minimisation and subsequent deletion while still employing analytic services it could be beneficial to only store the quarter period of a birth year since the aggregated mass that matching of additional data has to perform against does not lead to distinct identification of a single natural person.[192] This has benefits regarding statistical analysis where only approximated age and preferences can be processed.

MARCONI needs to know the age of the data subject in order to conduct market analysis. This encompasses the assessment of which age group will be the primary audience for a broadcast. Regarding data monitoring on Twitter, neither the determination of age, nor the obtainment via use of the Twitter API is possible. When inferring the age of the data subject, this would constitute processing that is not within the original intention of the data subject.

It should be noted that anonymisation could be achieved by collectively processing the data of members of a certain age group within one data set and therefore prevent a connection of certain data to a single data subject.

3.2.1.3 GENDER

Gender alone does not constitute personal data, only in connection with other identifying data. As the WP29 states: “*A person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognised by narrowing down the group to which he belongs which can also be achieved by gender*.” [193]

3.2.1.4 PLACE

The main issue regarding the datatype ‘place’ is that, if other data that renders the subject identifiable exists, it could be used to uniquely identify a natural person. One has to ask whether and how many additional data items are required in order to identify the subject. A city or a country alone as well as the location produced by an IP address (not the IP address itself) shall be not be considered personal data. This is to say that it depends heavily on the precision of the location and the way that it is linked to the individual in question. Should for example the location service be as precise as to pinpoint the position of a user who is associated with no more than a UID to identify the home address this datatype could be classified as personal data. Therefore, if the location should only encompass a city, the effort to identify the subject may be considered not “*reasonably likely to be used*”.[194] If possible, the required precision of the location data should be considered on a case-by-case basis.

68.

[191] Article-29-Working-Party, Opinion 4/2007 on the concept of personal data, WP 136.

[192] *Ernst* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 4 point 9

[193] Article-29-Working-Party, Opinion 4/2007 on the concept of personal data, WP 136.

[194] See Rec. 26 GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Linking data to a geographical area instead of the name of the data subject could, provided the geographical area is large enough so that data subjects can no longer be identified within proportionate means, may lead to anonymisation.

3.2.1.5 USER SOCIAL MEDIA ACCOUNT

According to the MARCONI general concept, the services in question are Twitter, Facebook, Instagram, SMS and e-mail. Concerning unique resource identifiers developers are able to choose whether or not to refer to an @-Handle or a UID with the difference that a Handle can contain information like last names by itself whereas the UID is usually composed of an integer alone like in the case of Facebook and Twitter. Article 4(1) GDPR constitutes that "*identification number, location data, an online identifier*" can be personal data. Combined with the ECJ Ruling C-582/14 ("Breyer") and the term "identifiable" it is safe to assume that with the objective approach the ECJ took these are to be treated as personal data. A requirement for this model is the possibility to acquire the necessary IP address in a lawful way (criminal procedures) if the user has not identified himself already.[195] Each username would have to be evaluated separately which is virtually impossible. In order to ensure compliance with the GDPR one should therefore treat any username as personal data since the possibility exists that social media users use their full name.

The use of social media data can, however, be based on consent or it concerns personal data which are manifestly made public by the data subject (Article 9(2)(e) GDPR). Social Media content is often personal data which are made public by the data subject. However it should be noted, that this is not always the case. If social media data is only visible to a certain number of users (including MARCONI) it cannot be considered to be "*made public by the data subject*".[196]

MARCONI should also implement systems which inform the data subject according to Article 14 GDPR if processed personal data should come from social media. This has to be performed in order to comply with transparency regulation since the data subject must be informed from where and for which purpose his personal data is being gathered.[197]

Regarding the use of profile pictures, there exist several hindrances. This is the case with intellectual property which almost always manifests in images. Furthermore, the right to one's own image as an expression of Article 8 of the European Convention on Human Rights which means that the picture of a user can only be used after a weighing of interests.[198] The use of a profile picture for advertisement purposes is therefore most likely prohibited since one could not establish (implicit) consent. It would therefore be better to include only a link to the profile. However, exceptions can be made under Article 85 GDPR.

Considering the context of social media data anonymisation is not an easy task. Pictures will in most cases be sufficient to identify the data subject. It should however be possible to anonymise data by linking them only to a group or a large geographical area.

---

[195] As in the case of ECJ 19 October 2016, C-582/14 ("Breyer") ECLI:EU:C:2016:779 Rec. 43.

[196] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 9 point 36; see Chapter 5 – Legal Grounds of Processing.

[197] See Chapter **Error! Reference source not found.**.

[198] See Chapter 9.4.

Co-funded by the Horizon 2020 Framework Programme of the European Union

3.2.1.6 RELATION

Using the target of the relations, the data subject itself can be identified by cross-referencing all content items to, for example, public social media groups and publicly identifiable user profiles thereof. Therefore, if additional data that is required is easily acquired it shall be considered personal data.

3.2.1.7 CLIENT

The client devices itself shall not be considered personal data unless more precise information about, for example, compositions of browser plug-ins or extensions or identification that would create a unique fingerprint of the device are being collected by MARCONI which could also be used by third party entities to determine the identity of the user. Therefore, it shall only be considered personal data when more data items should be gathered and linked so as to identify the subject.

3.2.1.8 PREFERENCE

Preferences of the user regarding music and artists shall only render the user identifiable if the information is (externally) linked to other identifying data.

3.2.1.9 CONTENT CONSUMPTION

Content consumption alone does not meet the requirements of "personal data" since too many entities share a common interest in music. This follows the assumption that radio content is always meant to be broadcasted to a larger audience. If a specific list of content items viewed by the user is saved, the monitoring of internet traffic could be used to identify the subject's device.

3.2.2 PERSON

As the dataset **Person** points to a user address of an online service, it is possible to indirectly identify a natural person, if the username of said service does not already contain personal data such as a name, via additional resources which could be acquired within the scope of the objective approach the ECJ took.[199]

3.2.3 CONTENT ITEM

3.2.3.1 TYPE

This is technical information – but also: the value **Type** encompasses a photography or video footage which holds personal data and possibly even personal data according to Article 9 GDPR. For information on Intellectual Property and Fair Use please refer to Chapter 9.

3.2.3.2 PROVENANCE

Provenance refers to a controlled value (radio station, user-generated-content or other professional), that indicates the provenance of a certain content item. As itself it is non-personal data.

[199] ECJ 19 October 2016, C-582/14 ("Breyer") ECLI:EU:C:2016:779 Rec. 43.

Co-funded by the Horizon 2020 Framework Programme of the European Union

3.2.3.3 LOCATION AND DATE

Since **Location** contains the data category **Place** please also refer to 3.2.1.4 **User** – **Place**. The Content Item is linked to a certain date. The date of an event (like the integration of content) is without additional data non-personal data.

The Location, as well as the Date could be anonymised if decoupled from **Contributor**.

3.2.4 CONTRIBUTOR

Radio listeners as contributors

As this set contains **Contributor** which is identified via an URI that is linked to the users profile it is deemed 'personal data' as long as the user account itself contains personal data.

In case of original content, a contributor has to transfer a license to the radio station. In such cases, records have to be kept to proof the permitted use of the content. A copyright record is allowed under the exception of Article 17(3)(e) GDPR which constitutes that the data subject has no right to erasure if the data controller needs said data "for the establishment, exercise or defence" of legal claims, reinforced by recital 65 GDPR ("defence of legal claims"). In some cases, a weighing of interests in favour of the processor under Article 9(2)(f) GDPR can be argued, which would allow the controller to process even 'special categories of data' for said purpose.[200]

Contributor as part of a contract to promote their work

A contributor can also be a band or a singer who wants to promote his work. In this case this data item may contain personal data as well, like the name of the singer, however, the processing of this data is generally data made public by the data subject which means that the weighing of interests in favour of the processor according to Article 6(1)(f) GDPR would justify processing.[201]

3.2.4.1 OTHER TECHNICAL MEDIA ITEM PROPERTIES

This is technical information relevant to adjust a certain **Content Item** to the timeline. Just as **Type** or **Provenance,** these are, standing alone, non-personal data.

3.2.5 PLACE

3.2.5.1 GEO-COORDINATES

It is possible that **geo-coordinates**, in and of themselves, are to be considered personal data, if it is within reasonable means to identify the data subject. This will generally be the case if there are additional information.[202]

[200] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 9 point 37.

[201] ECJ 19 October 2016, C-582/14 ("Breyer") ECLI:EU:C:2016:779 Rec. 44.

[202] Refer to WP29, Opinion 05/2014 on Anonymisation Techniques WP 187 (2014).

Co-funded by the Horizon 2020 Framework Programme of the European Union

3.2.5.2 NAME

This data item refers to e.g. geonames and TGN. The name of a certain location can't in and of itself be used to describe a data subject.

For the datatype **Place** please refer to Chapter 3.2.1.4 **User** – **Place**.

3.2.6 EVENT

3.2.6.1 EDITORIAL ITEM

This data item provides the category of a certain event and references to related programmes. It has no properties of its own that are used to identify a data subject.

3.2.6.2 PERSON

The dataset **Event** contains the dataset **Person** which is generally 'personal data'. The only possibility to store such a set indefinitely would be to make sure that no user is modelled by **Person**.

However, if it is data that has been made public by the data subject a weighing of interests according to Article 6(1)(f) GDPR will most likely justify processing. Refer to Chapter 5.4.

3.2.6.3 LOCATION AND DATE

Refer to 3.2.7.3 **Content Item** – **Location and Date.**

3.2.7 INTERACTION

3.2.7.1 INVOLVED USERS

Depending on whether the involved data subjects are processed similar to the data set **Person** or if the users are aggregated so that a single data subject is no longer identifiable within proportionate effort[203], this data item is personal data (which results in this data set to be personal data) or not.

3.2.7.2 ACTION

The data item **Action** consists of type and content. Content is describing details of the action, but also contains identifiers of preferences, content consumptions, relations, etc. expressed through the action. This data item can be anonymous data, if only aggregated data is processed.

3.2.7.3 CONTENT ITEMS

Refer to 3.2.3 – **Content Item.**

Containing the dataset **Content Item** as well as **User**, this dataset is personal data.

3.2.7.4 CHANNEL

This data item concerns channel communications and is technical information.

[203] Refer to Chapter 1.3.2.

Co-funded by the Horizon 2020 Framework Programme of the European Union

3.2.7.5 EDITORIAL ITEM

Refer to 3.2.6.1 **Event** – **Editorial Item**.

3.2.8 CLIENT DEVICE

3.2.8.1 NAME

Refer to 3.7.1 **User** – **Name**.

3.2.8.2 MANUFACTURER AND TYPE

The manufacturer and the **Type** of a client device (e.g. mobile phone, tablet, browser) may constitute personal data if it is possible to identify a data subject through external databases, without disproportionate effort.

3.2.8.3 RELATED CLIENT

The IMEI of a client device is being used as an example URI for a mobile device. In Austria, criminal procedure law enables executive forces to locate a device connected to a transmitting mast and uses either telephone number or an IMEI in order to uniquely identify a suspect.[204] In due consideration of the ECJ ruling ("Breyer")[205] and the fact that it would be possible to identify and locate the data subject with help of the telecommunication provider, an IMEI shall be considered 'personal data'.

3.2.9 ANALYSIS

3.2.9.1 PROFILE

This data item contains the analysis profile and a set of modules being applied and therefore concerns technical data.

3.2.9.2 CONTENT

Since the data item content contains the data set **Content Item**, refer to 3.2.3 **Content Item**.

3.2.9.3 INTERACTION

Since the data item **Interaction** contains **Content item** and **User**, it is deemed personal data. In order to anonymise the dataset, these must be removed (or anonymised). Please refer to the respective datatypes in the corresponding Chapters above. As it is only used to determine the origin of the machine learning input, the data is not to be stored longer than necessary. It has to be kept in mind, that each purpose requires a lawful basis.[206]

3.2.9.4 RESULTS

Depending on whether the input contained personal data or not, this data item might be considered personal data. However even the analysis of non-personal data can result in data that enable the

[204] *Lewisch*, Zulässigkeit von Funkzellenauswertungen, JBL 2016, 199-201.

[205] ECJ 19 October 2016, C-582/14 ("Breyer") ECLI:EU:C:2016:779.

[206] See Chapter 1.3.3 GDPR – Lawful Processing & Chapter 5 – Legal Grounds of Processing.

Co-funded by the Horizon 2020 Framework Programme of the European Union

identification of the data subject. Furthermore, in some cases personal data resulting from the analysis can be considered a special category of personal data (Article 9(1) GDPR).

3.2.9.5 DATE

Refer to 3.7.3 **Content Item** – **Location and Date**.

3.2.9.6 MACHINE

The ID of a machine, where analysis has been performed, like an IP-address, can constitute personal data, if the data subject is identifiable within means that are reasonably likely to be used.[207] However, since the datatype **Machine** only concerns processing units (such as servers) of the controller, who is therefore solely handling his own data, it can be processed without restriction.

3.2.10 INFERENCE

3.2.10.1 PROFILE

Refer to 3.7.9 **Analysis** – **Profile.**

3.2.10.2 SOURCE

The datatype **Source** links to the item **Result** of the dataset **Analysis** which is likely to be composed of personal data since the input may very well contain personal data itself. However, if individual statements, traits or preferences are no longer possible to associate or link with a single user (aggregation) these will fall out of the scope of the GDPR.

3.2.10.3 RESULTS

Refer to 3.2.9.4 **Analysis** – **Results**.

3.2.10.4 DATE

Refer to 3.2.3.3 **Content Item** – **Location and Date**.

3.2.10.5 MACHINE

Refer to 3.2.9.6 **Analysis** – **Machine**.

3.2.11 TRAINING

3.2.11.1 PROFILE

Refer to 3.2.9.1 **Analysis** – **Profile**.

3.2.11.2 SOURCE

Refer to 3.2.10.2 **Inference** – **Source**.

[207] Refer to Chapter 1.3.2 GDPR – Scope and Personal Data.

Co-funded by the Horizon 2020 Framework Programme of the European Union

3.2.11.3 **DATE**

Refer to 3.2.3.3 **Content Item** – **Location and Date**.

3.2.11.4 **MACHINE**

Refer to 3.2.9.6 **Analysis** – **Machine**.

Since it uses almost the same input as **Inference**, the dataset **Training** must be treated similar. However, if the training of analysis or inference models does not always require personal data, it should be considered to only use aggregated (and therefore anonymous) data within the training data set. Personal data of training sets should be subject to organisational and technical data protection and data security measures (e.g. pseudonymisation). Results of training sets do normally not contain personal data but only aggregated information.

Co-funded by the Horizon 2020
Framework Programme of the European Union

4 Role Allocation

Within each step during the processing of data, everyone involved may have different roles within the framework that is set up by the GDPR. It is important to allocate the role of each person involved, because depending on the outcome the obligations and therefore the liabilities differ.

4.1 Controller and Processor

The main question in determining the role of each person involved is that of who has detailed control of the processing of data.[208] According to Article 4(7) GDPR '**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means** of the processing of personal data whereas Article 4(8) GDPR defines the '**processor'** as a natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller**. 'Joint controllers' are defined in Article 26(1) GDPR as two or more controllers who jointly determine the purposes and means of processing.

On 16 February 2010 the Art-29-Working Party adopted an opinion on the concepts of "controller" and "processor" wherein it acknowledges that applying these concepts to concrete situations can be complex, even more so, if confronted with modern technology, like cloud-computing. As the Art-29-WP points out, it is, however, crucial to analyse how the term "determines"[209] should be understood.[210] The Art-29-WP differentiates between **control stemming from explicit legal competence**, control stemming from **implicit competence and** control stemming from **factual competence**, all of which may lead to a determination of purpose and/or means of processing.[211] This means that not only legal, but also factual influence may lead to the conclusion that an involved person "determines" purposes or means of processing.[212]

If there are more than two parties involved, a distinction between the controller and the processor can safely be made if the processor acts solely as the puppet of the controller.[213] In modern business, however, such is seldom the case. Considering cloud-computing, the cloud-provider technically gains access to data of the cloud-user. Even though the cloud-user is supposed to be the controller and the cloud-provider is supposed to be the processor, the cloud provider is generally in a position to decide where the data is stored, where it is replicated (for security reasons) or distributed or fragmented on different servers. Although this may be considered an enormous influence on the technical means of the processing of data, this does not necessarily include influence on which data is processed or when and if they should be deleted.

---

[208] *Dürager,* Outsourcing in die Cloud - Ein (un-)beherrschbares Risiko aus datenschutzrechtlicher Sicht? Ip Competence 18/2017, 36(47).

[209] Of „determines the purposes and means" (Art 4(7) GDPR.

[210] Art-29-Working Party, WP 169, 8.

[211] Art-29-Working Party, WP 169, 9f.

[212] Art-29-Working Party, WP 169, 12.

[213] *Spitzbart/Geuer*, Zielgerichtete Werbung für Kunden in sozialen Netzwerken, Dako 2017/21, 37(38).

Co-funded by the Horizon 2020 Framework Programme of the European Union

Because means and circumstances of processing are still determined by the cloud-user the cloud-provider remains mere processor of the data.[214] This conclusion is in accordance with the aforementioned opinion of the Art-29-WP, which states, that the determination of the "means" of processing can be delegated by the controller, as far as technical or organisational questions are concerned.[215] The deciding factor is who determines means and purposes in what detail.[216]

4.2 Joint Controllers

When a platform is created by two or more parties to process data, these parties could be considered joint controllers, if they all have control over which data is processed and in which way and also over the purposes for which these data are used.[217] When a third-party-platform is used, however, the role allocation has to be decided on a case-by-case basis.[218] To determine which role a third-party-service-provider possesses, careful consideration should be given to whether the third party has self-interest regarding personal data that is subject to the processing-activities in question and in how far processing-activities can be factually prohibited.[219]

The bigger the flexibility of the “processor” within each processing activity, the more permission of use of the “processor” and the lower the possibility to intervene by the “controller”, the more this could be considered a joint control instead of a processing agreement.[220]

The Art-29-WP states the following:

"Joint control will arise when different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterize a controller. [...] Indeed, in case of plurality of actors, they may have a very close relationship (sharing, for example, all

[214] *Dürager,* Outsourcing in die Cloud - Ein (un-)beherrschbares Risiko aus datenschutzrechtlicher Sicht? ipCompetence 18/2017, 36(47).

[215] Art-29-Working Party, WP 169, 17.

[216] *Dürager,* Outsourcing in die Cloud - Ein (un-)beherrschbares Risiko aus datenschutzrechtlicher Sicht? ipCompetence 18/2017, 36(47).

[217] *Fritz* in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018) Abgrenzungsschwierigkeiten bei der datenschutzrechtlichen Rollenverteilung nach der DS-GVO, 22.

[218] *Fritz* in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018) Abgrenzungsschwierigkeiten bei der datenschutzrechtlichen Rollenverteilung nach der DS-GVO, 23.

[219] *Ingold* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. Art. 28 point 15; *Dürager,* Outsourcing in die Cloud - Ein (un-)beherrschbares Risiko aus datenschutzrechtlicher Sicht? ipCompetence 18/2017, 36(47); *Fritz* in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018) Abgrenzungsschwierigkeiten bei der datenschutzrechtlichen Rollenverteilung nach der DS-GVO, 23; Art-29-Working Party, WP 169, 25.

[220] *Dürager,* Outsourcing in die Cloud - Ein (un-)beherrschbares Risiko aus datenschutzrechtlicher Sicht? ipCompetence 18/2017, 36(47).

Co-funded by the Horizon 2020 Framework Programme of the European Union

purposes and means of a processing) or a more loose relationship (for example, sharing only purposes or means, or a part thereof)."[221]

But it also states that "the mere fact that different subjects cooperate in processing personal data, for example in a chain, does not entail that they are joint controllers in all cases, since an exchange of data between two parties without sharing purposes or means in a common set of operations should be considered only as a transfer of data between separate controllers."[222]

Art 26(1) GDPR requires an arrangement, that determines their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, which (in "essence") has to be made available to the data subject.[223]

According Article 28(10) GDPR, if a processor "infringes this Regulation by determining the purposes and means of processing, the processor shall be considered a controller in respect of that processing". This is the case if a processor acts willingly against the explicit directive of a controller, but also if the processor oversteps the instructions of the controller without knowing or by accident.[224] Similar is the case of a flawed processing-contract, where controller and processor enter into an agreement, which exceeds the boundaries of a processing-contract, which means that purpose and means are not sufficiently determined within the processing contract[225].

So in addition to control stemming from explicit legal competence, control stemming from implicit competence and control stemming from factual competence, unauthorised processing activities of the processor have to be taken into account during role allocation.[226]

When determining the role of a party that is involved in processing of personal data, it has to be kept in mind, that the role within data protection law is a functional concept[227] and has to be determined within each processing activity.[228] So even regarding the same data, one party can apprehend different roles, if these data is subject to different processing activities.[229] The following test-scheme has been

---

[221] Art-29-Working Party, WP 169, 19.

[222] Art-29-Working Party, WP 169, 19.

[223] See also *Fritz/Paulus*, Die Joint-Controller Vereinbarung als Ausprägung des datenschutzrechtlichen Transparenzgrundsatzes, jusIT 2018/5, 13.

[224] *Fritz* in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018) Abgrenzungsschwierigkeiten bei der datenschutzrechtlichen Rollenverteilung nach der DS-GVO, 23.

[225] Art. 28(3) GDPR; *Ingold* in *Sydow,* Europäische Datenschutzgrundverordnung[1] (2017) Art. 28 point 24.

[226] *Fritz* in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018) 22.

[227] Art-29-Working Party, WP 169, 9.

[228] *Fritz* in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018) Abgrenzungsschwierigkeiten bei der datenschutzrechtlichen Rollenverteilung nach der DS-GVO, 21.

[229] "The concept of controller is a functional Concept" (Art-29-Working Party, WP 169, 9)

Co-funded by the Horizon 2020 Framework Programme of the European Union

proposed within the literature[230] to determine the roles of each party regarding certain processing activity:

- Determination of the processing activity
- Determination of processed data/data subject
- Determination of the controller
- Determination of the processor
- Determination which controllers are joint controllers

When determining whether processing is done by a controller or a processor, the following criteria as described above, should be considered:

- Legal, implicit or factual competence on the purpose
- Legal, implicit or factual competence on the essential elements of the means (not including technical

Without the MARCONI-partners having an explicit agreement on the purposes and means of processing, which have to be determined in the sense of Article 26 GDPR, they can't be considered "joint controllers". This means that processing of personal data within the project could be either that of separate controllers or that of joint controllers, depending on who determines the purpose of the processing or the essential elements of the means and on the existence of an agreement covering the determination of purpose and means of processing.

The ECJ recently ruled that the administrator of a fan page hosted on Facebook can be considered jointly responsible in relation to the processing of personal data of visitors to that page, considering that a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy is an explicit aim[231] of the Directive 95/46/EC.[232] The administrator of such a fan page can decide processing activities by defining parameters depending on its target audience and the objectives of managing and promoting its activities to determine the purposes and means of the processing activities, e.g. the placement of cookies on the visitors of the fan page and the analysis of their behaviour. The administrator may "*ask for* […] *demographic data relating to its target audience, including trends in terms of age, sex, relationship and occupation, information on the lifestyles and centres of interest of the target audience and information on the purchases and online purchasing habits of visitors to its page* […] *and geographical data which tell the fan page administrator where to make special offers and where to organise events, and more generally enable it to target best the information it offers*."[233]

[230] *Fritz* in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018) 22.

[231] Not only the Data Protection Directive (Art 1(1) and Rec 10 Directive 95/46/EC) but also the GDPR include the aim of a "consistent and high level of protection of natural persons" (Rec 10 GDPR).

[232] ECJ 5 June 2018, C-210/16 („Wirtschaftsakademie Schleswig-Holstein"), ECLI:EU:C:2018:388, Rec 39.

[233] ECJ C-210/16, Rec 37.

Co-funded by the Horizon 2020 Framework Programme of the European Union

The ECJ points out, that "the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case."

The reasoning of this case is not fully applicable to MARCONI as, contrary to Facebook, the MARCONI service provider – if MARCONI is implemented as a service – would only process data for the purposes determined by the radio stations. However, it should be considered that a MARCONI service provider and the radio station might be joint controllers. According to the criteria mentioned above this might depend on whether data is processed without the initial decision by the radio station.

4.3 Conclusion

As can be seen in Chapter 2.1, the intended usage of MARCONI involves various actors. The MARCONI application will be applicable to a variety of platforms, i.e. to Facebook, Twitter and other social media platforms and can also be used via smartphone. Via a communication adapter, each user can communicate with the radio station through the MARCONI application. Each communication through the MARCONI application will (provided the user gives his/her consent[234]) be analysed and the extracted metadata will be stored within a database, not, however, the original messages. The same principles apply to the analysing of social media data.

When MARCONI is used within its intended purposes and applied by the radio stations, it appears that each radio station can determine the purpose of the processing and even which data should be processed, while MARCONI would provide the database and the means of the processing. Therefore, it appears that even if MARCONI processes personal data, these data would be processed as a processor on behalf of the radio station as a controller, since the radio station may decide the purpose of the processing. MARCONI does not process data in pursuit of its own interests, which is, however, an essential element of a processor[235] but involves some obligations.[236] According to Article 79(2) GDPR, every natural person may bring before the courts of the Member State proceedings against not only the controller, but also against the processor.

If MARCONI would be used as a software by each radio station as controller, the developer will not be considered as a processor and thus is without obligations under the GDPR.

[234] See Chapter 5.1.

[235] *Anderl/Tlapak*, Vom Dienstleister zum Auftragsverarbeiter - was ändert sich mit der DSGVO?, ZTR 2017, 59; *Ingold* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 28 point 15.

[236] See i.e. *Fritz*, Der Auftragsverarbeiter im Fokus der DS-GVO, Jahrbuch Datenschutzrecht 2017, 9(19).

Co-funded by the Horizon 2020 Framework Programme of the European Union

4.4 Electronic Commerce

According to the Directive 2000/31/EC (Electronic Commerce Directive)[237], access as well as host providers are **exempted from certain liabilities** occurring through information transferred or hosted through/on their systems. The content provider is solely responsible for its content.

The GDPR also acknowledges this in its material scope in Article 2(4) GDPR as well as in Recital 21 meaning that the GDPR exists without prejudice to said directive.

4.4.1 SOCIAL MEDIA PLATFORM – HOST PROVIDER

The social media platform can be considered a host provider according to Article 14 of the Directive 2000/31/EC since the service "*consists of the storage of information provided by a recipient of the service*".

According to Article 14 leg. cit., a host provider shall not be held "*liable for the information stored at the request of a recipient of the service*".[238] This privilege only applies if the "*service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored*". Austrian case law further broadens the significance of the rule as it requires the offense to be obvious and therefore recognizable for the layman.

As within MARCONI, the controller has full control as well as knowledge over data, this shall not apply.

Every conversation with a user has the possibility to yield personal data of a third party. Appropriate safeguards should therefore be in place in order to ensure that the data is processed in a precise manner ('accuracy'). If such safeguards are in place, the data in question should be associated with the account that is making it public. In order to scan for such third-party data, MARCONI would face the need to process it itself.

The "poster", if not falling under the exception of "personal activity", would be a controller himself and could be held liable to remove the information from his page. An ostensible authority of the "poster" (content provider) in relation to the data subject can be assumed. An argument can be made in proposing that an individual might impersonate another. MARCONI and no other data controller could detect such behaviour unless identification via state ID is being conducted which would not be feasible for the types of data MARCONI collects.

Therefore, social media monitoring develops into a primary showcase of conflict between economic interest of the controller and informational freedom as regulated by Article 85(1) GDPR which constitutes a soft opening clause for Member States in order to institute more precise regulation in

[237]Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17/07/2000 P. 0001 – 0016.

[238] ECJ 23 March 2010, C-236/08 to C-238/08 ("Google France") ECLI:EU:C:2010:159.

Co-funded by the Horizon 2020 Framework Programme of the European Union

the context of journalistic tasks.[239] It is to be understood, that Article 85 GDPR shall therefore be a *lex specialis* to Article 6(1)(f) GDPR.[240]

[239] Rec. 153 GDPR.

[240] *Martini*, Wie neugierig darf der Staat im Cyberspace sein? Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen (2016), VerwArch 2016, 353.

Co-funded by the Horizon 2020
Framework Programme of the European Union

5 Legal Grounds of Processing

A processing of personal data by MARCONI must be justified by at least one of the six possible grounds of justifications according to Art. 6 GDPR. The most relevant are described in the following sections: consent, performance of a contract, legitimate interests and public availability of data.

When determining how to process personal data in a lawful manner, however, it should be mentioned that the other provisions of the GDPR must be also respected, like the principles of processing[241], and the rights of the data subject as well as administrative duties.[242]

5.1 Consent

The most important ground of justification will be consent according to Article 4(11) GDPR of the data subject with requirements as outlined in Article 7 GDPR. Consent means that the data subject has given his approval for a personal data processing activity restricted to one or more specific purposes.[243] While consent must not be in written form, an equally affirmative expression must be provided from the user.[244] Without proper consent, other grounds of lawful processing must be checked. If consent was given by data subjects that was compliant with Directive 95/46/EC,[245] there is no need that consent to be given a second time.[246]

Recital 32: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent*." Any other implicit consent such as inactivity and mere tolerance is not envisaged.

According to Article 7(1) GDPR, the burden of proof that informed consent has been given lies with the controller. An oral agreement is therefore not practical. Terms and Conditions must therefore be clearly structured and in case of using the app, must be easily reachable, preferably within a single 'click'.

According to a very recent ruling of the Berlin Regional Court[247] (Landgericht Berlin) the terms "acknowledgement" and "read and understood" should not be used as they would move the burden

[241] Art. 5 GDPR.

[242] Refer to Chapter 1.3 General Data Protection Regulation (GDPR).

[243] *Stemmer* in BeckOK DatenschutzR, DS-GVO[23] Art. 7 points 55-60.

[244] *Stemmer* in BeckOK DatenschutzR, DS-GVO[23] Art. 7 point 32.

[245] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

[246] Rec. 171 GDPR.

[247] LG Berlin 16 O 341/15.

Co-funded by the Horizon 2020 Framework Programme of the European Union

of proof to the user. Every purpose of processing data must be explained and elucidated; otherwise no 'informed consent' is possible.

The safest approach would be using the most vital information the user must "scroll through" in order to reach a confirmation dialog while providing the possibility to further 'investigate' the rest.

When employing the dataset "Content" it is to be ensured, that presented photographs or video recordings are not in violation of the right to one's own image meaning that the right to privacy must not be infringed. This right may vary from Member State to Member State (see national media law for journalistic exceptions and freedom of press). In general, public events and shots of public streets are usually allowed and can be handled by the radio station as usual. Regarding the GDPR, images of such events may be collected under Art. 6(1)(f) ("weighing of interest") which applies to relations under civil entities[248] and can be structured into three parts.[249] The interest of the controller (or a third party), which must be 'legitimate', and which is not overridden by interests or fundamental rights and freedoms of the data subject. A guideline for evaluating such a 'legitimate interest' can be found in Rec. 47 which says, that one must take "*into consideration the reasonable expectations of data subjects based on their relationship with the controller*". This means that processing of personal data for other legitimate interests is not dependent on a contract itself.[250] This holds especially true if the formation of a contract or the user giving consent is hardly possible.

Since MARCONI will only have the possibility to engage directly with its listeners through means of a mobile application, web application, a chatbot and e-mail, for each option a compliant model must be established:

According to Article 4(11) GDPR, consent shall be:

- Freely given
- Specific
- Informed
- An unambiguous indication of the data subject's wishes

Free implies that a data subject should not suffer from an imbalance of power, conditionality or detriment if he should choose not to provide consent.[251] While the text shall be presented in a granular fashion it shall also be easy to understand. Since radio stations and therefore MARCONI also aim their services at a younger audience it shall be imperative to design the consent agreement in a fashion that enables users under the age of 18 to understand it.

MARCONI shall, in order to comply with the principle of conditionality stated in Article 5(1)(c) GDPR ("data minimisation"), only acquire consent from a data subject in an extent where personal data is required to perform its respective services. That is the minimal amount of data in order to let the

[248] *Ernst* in *Paal/Pauly*, DSGVO[2] (2018) Art. 6 point 26.

[249] *Ernst* in *Paal/Pauly*, DSGVO[2] (2018) Art. 6 point 27.

[250] *Ernst* in *Paal/Pauly*, DSGVO[2] (2018) Art. 6 point 28.

[251] WP29, Guidelines on Consent under Regulation 2016/679 wp259, first revision (2018), 4.

Co-funded by the Horizon 2020 Framework Programme of the European Union

service function as intended: "processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract."[252]

As the burden of proof according to Article 7(4) GDPR is on the controller, MARCONI will be in need to declare **why** it needs **which** personal data for **what** purpose as the principle of purpose limitation requires. Therefore, the scope of MARCONI must be clearly defined and as it will be further developed, the data protection statement properly adjusted.

MARCONI has to list the collected data and assign it to respective processing operations. As of now the MARCONI use cases according to Deliverable 1.2 describe several small purposes which can be

- ➔ Categorisation (clustering) of incoming information based on metadata extraction and indexing services.
- ➔ Personalised radio content based on user preferences and profiles.
- ➔ The operation of a chatbot and associated learning algorithms.

generalised into the following larger ones:

Consent has to be given voluntarily for the particular case, in an informed and unambiguous manner in the form of a declaration or any other unambiguous confirmatory act by which the data subject indicates that he / she agrees to the processing of personal data, as stated above.[253] Together with a Layered Privacy Notice[254], this could be achieved by presenting the data subject a short but clear version coupled with a brief explanation which data is gathered for what purpose such as:

Forcing the user to share data non intrinsic to the service is unlawful and as in case of doubt, the user agrees involuntarily.[255] This also applies to a notification of non-intrinsic disadvantages. Article 7(3) GDPR provides the need to inform the data subject of his rights according to Chapter 2 of the GDPR. If such an admonition is missing, it is unclear whether the consent is void in its entirety or just in its respective sections.[256]

Recital 32 GDPR: "*Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent*." Any other implicit consent such as inactivity and mere tolerance is not envisaged.

---

[252] WP29, Guidelines on Consent under Regulation 2016/679 wp259 (2017), 9.

[253] *Ernst* in *Paal/Pauly*, DS-GVO² (2018) Art. 4 point 62.

[254] WP29, Opinion 10/2004 on more harmonised Information Provisions (2016), 6.

[255] *Ernst* in Paal/Pauly, DS-GVO² (2018) Art. 4 point 7.

[256] *Ernst* in Paal/Pauly, DS-GVO² (2018) Art. 4 point 77.

Co-funded by the Horizon 2020 Framework Programme of the European Union

According to Article 7(1) GDPR, the burden of proof for these premises for informed consent lies with the controller. An oral consent is possible but not always practical.

Also an **imbalance of power** shall be considered if a public institution or authority should use MARCONI. However, also in other possible situations this might be the case. The data subject must be able to "*exercise a real choice*".[257] This means that the data subject must be able to consume the service, if public, in a traditional manner without the necessity to share personal information which will rarely be possible.[258] As MARCONI merely channels radio systems, the user could still enjoy traditional radio via a short wave or ultra-short-wave radio signal reception.

Even where MARCONI could base its processing on the necessity for the performance of a contract, consent is required for the special categories of personal data (Art. 9 and 10 GDPR) which does not include the option "necessary for the performance of a contract". Another advantage may be that special categories of personal data could not be easily identified by MARCONI.

In order to be specific, consent must be given in a **granular** manner. That is separate consent not for separate data types or processing but for distinct purposes (Rec. 32 GDPR). It does not matter if data is collected by a chatbot or the MARCONI app is used for different services (e.g. use cases). Though each service must generally be consented to separately,[259] it is possible that the services are categorised in groups so as to prevent the user from being faced with too many checkboxes.[260] Purposes should not be conflated but be general enough in order to provide necessary functionality.

MARCONI will have to make clear that the data subject does not have to fear coercion or any other detriment if consent should either not be provided or revoked at a later point in time (Rec. 42 GDPR). If the user should not be able to withdraw his consent as easily as he was able to give, no valid consent has been reached as the mechanism does not meet the necessary requirements.[261]

Recital 42: *"For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."*

The data subject will have the right to withdraw his consent at any given time.[262] This must be as easy as giving consent and may be achieved, by unticking a checkbox or uninstalling the app. Informal ways of withdrawing consent shall be considered and the user shall bear no more difficult way to do so.[263] MARCONI should include a section noticing that the user can freely revoke his consent according to

[257] WP29, Guidelines on Consent under Regulation 2016/679 WP 259 (2017), 8.

[258] WP29, Guidelines on Consent under Regulation 2016/679 wp259, first revision (2018), 6;
In this matter, consent will rarely be a viable option.

[259] WP29, Guidelines on Consent under Regulation 2016/679 wp259 (2017) 11.

[260] WP29, Guidelines on Consent under Regulation 2016/679 wp259, first revision (2018), 10 (17);
A purpose may require many (micro-)services and only one consent request, a single service may require several consent requests.

[261] WP29, Guidelines on Consent under Regulation 2016/679 wp259, first revision (2018), 22.

[262] Art. 7(3) GDPR.

[263] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018), Art. 7 point 17.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Article 17(1)(b) GDPR.[264] The right to object according to Article 21 GDPR does however not apply although Article 7(3) provides the same consequence.

No consent can be established when social media platforms allow third parties to search and process user content since an agreement would only be possible *inter partes*. A divergent contract shall be qualified as unlawful.[265] See also Article 5(1)(a) GDPR ("lawfulness" and "fairness").

The user, in order to have an informed **consent** must be provided with the following information which are the "minimum requirements" as provided by the WP29 recommendation:

- The controller's identity.
- The purpose of each of the processing operations for which consent is sought.
- What (type of) data will be collected and used.
- The existence of the right to withdraw consent.
- Information about the use of the data for decisions based solely on automated processing, including profiling, in accordance with Article 22 (2) GDPR, and
- If the consent relates to transfers, about the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards (Article 49 (1)(a) GDPR).

Consent by electronic means: When pre-formulated written declarations are being used they shall be presented in a clearly separate window before starting the service. It interrupts the user experience at the very beginning. Constant requests might induce a certain "click fatigue" to the user and may be no longer properly read. It may also be important to elaborate on **explicit** (Art. 9 GDPR) versus **unambiguous** consent (Art. 6 GDPR). Explicit consent is required for sensible data e.g. medical records.

The lawful ground of processing under Article 6 must be established prior to the onset of processing and bound to a specific purpose. The WP29 states that, as the "lawful basis" for processing cannot be modified, the controller will not be allowed to retroactively use a different one such as legitimate interests.[266]

Consent and scientific research: As MARCONI will undertake further steps to develop the product within scientific research, purpose limitation and consent can be interpreted in a more flexible manner (Rec. 33 GDPR).

Recital 33: "*It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards*

[264] WP29, Guidelines on Consent under Regulation 2016/679 WP 259 (2017) 8.

[265] *Martini*, Wie neugierig darf der Staat im Cyberspace sein? Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen (2016), VerwArch 2016, 307.

[266] WP29, Guidelines on Consent under Regulation 2016/679 wp259 (2017) 22.

Co-funded by the Horizon 2020 Framework Programme of the European Union

for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose."

"Scientific research" is defined in Rec. 159 GDPR:

Recital 159: "*Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research."*

The WP29 notes that stretching the term must be compliant with the "*sector-related methodological and ethical standards*".[267] This statement may refer to best practices, corporate governance and certification.

The purpose limitation will be addressed in a more general and flexible manner, resulting in the possible slight change or shifting of the purpose at a later point in time. The WP29 therefore states that a data subject should be given the opportunity to consent to purposes which are already known at a certain research stage and in more general terms for the rest.[268] If specific consent cannot be sought from the data subject, transparency shall act as an additional safeguard as consent shall not exempt the controller from the processing principles in Art. 5 meaning that personal data shall still not be processed in an excessive manner in relation to the provided purpose.[269] This applies in particular to the special categories of personal data according to Art. 9 GDPR.

The last sentence of Art. 7(2) GDPR says, that parts of the consent shall not be binding if they should infringe the regulation. Thus, the consent agreement is modular. However, if formal requirements should not be fulfilled, a reduction of the meaning to a legally permitted core is not possible.[270]

5.1.1 STRUCTURE FOR A DECLARATION OF CONSENT

Consent - General Information

We, the MARCONI Consortium [radio station] aims to provide personalised services. We ask you to give your consent to process personal data concerning personalised music experience. More …. [website, or specific question].

Consent – Website

[267] WP29, Guidelines on Consent under Regulation 2016/679 wp259 first revision (2018) 28.

[268] WP29, Guidelines on Consent under Regulation 2016/679 wp259 first revision (2018) 29.

[269] WP29, Opinion 15/2011 on the definition of consent (WP 187) 7.

[270] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 7 point 15.

Co-funded by the Horizon 2020 Framework Programme of the European Union

The MARCONI Consortium aims to provide personalised services. We ask you to give your consent to process personal data provided by registration, list of preferences, dialogue, or interview, as given below, depending on the service. We ask your permission to review third party data about you, for example, your Twitter, Instagram or Facebook feeds.

All non-personalised services will be provided if you do not give or chose to withdraw your consent. You can withdraw your consent at any time (or change its scope), without any negative consequences besides the service itself not being available to you.

You can choose which data may be processed by MARCONI for the following purposes:

- Personalised music experience:

Name, contact details, e-mail, birthday, social media accounts,

Messages that are received from and send to the station (one-on-one communication including chatbot conversation), messages pinned/starred/bookmarked from social media like Twitter/Instagram, publicly available data on the internet (Tweets, a Google search, Facebook, YouTube comment, etc). Please note that only the analysis data is stored, not the original messages.

- Personalised interaction with the radio station:

Name, contact details, e-mail, birthday, social media accounts,

Messages that are received from and send to the station (one-on-one communication including chatbot conversations), messages pinned/starred/bookmarked from social media like Twitter/Instagram, learning publicly available data on the internet (Tweets, a Google search, Facebook, YouTube comment, etc). Please note, that only the analysis data is stored, not the original messages.

Messages that are received from and send to the station (one-on-one communication including chatbot conversations), messages pinned/starred/bookmarked from social media like Twitter/Instagram, learning publicly available data on the internet (Tweets, a Google search, Facebook, YouTube comment, etc). Please note, that only the analysis data is stored, not the original messages.

These data may be analysed for automated clustering. Data protection principles will be respected. The results will be used for improving our services but also for marketing purposes.

- Improvement of our services (training of our chatbot, …): [Data that is processed for this purpose]

5.2 Performance of a Contract

Another ground of justification would be the fulfilment of contractual obligations, e.g. using the MARCONI app. According to Article 6(1)(b) GDPR the processing shall be lawful if it is “necessary for the performance of a contract” to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. However this justification won’t cover all

Co-funded by the Horizon 2020 Framework Programme of the European Union

intended processing since on the one hand, not all processing is preceded by a contract and on the other hand not all processing is necessary for the performance of a contract or in order to take steps prior to entering into a contract.

Recital 40: *"Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract."*

The definition of a contract is not provided by the GDPR and must be determined in an autonomous manner according to union law. According to the E-Commerce-Directive,[271] a contract is a legal transaction or obligation similar to a legal transaction.[272] A quasicontractual relationship can therefore be designated as a contract if they are based on a voluntary decision of the data subject.[273] A different approach is being taken by *Frenzel* who excludes services provided on a goodwill basis *a priori*.[274] Quasi-contractual relations on a goodwill basis are seen as being included by *Albers*[275] as well as *Kühling/Buchner/Buchner/Petri*[276] while *Gola*[277] and *Frenzel*[278] uphold a different opinion as free services shall not be included. According to the latter, unilateral contracts may be also included (e.g. "Auslobung" in Germany).[279] Even if no classical payment is required as economic counter performance, such a service still remains synallagmatic if the user provides personal data for purposes such as market analysis and personal advertisement.[280] This leads to a situation where users "pay" for a service with personal data which is a business model used by Google, Facebook and other social media platforms. Thus, as strongly practiced by online services with quasicontractual relations, it is possible for MARCONI to process data under the lawful basis of Art. 6(1)(b).

So even where MARCONI could base its processing on the necessity for the performance of a contract, consent shall be preferred since every message MARCONI might receive could potentially fall under the special category of personal data which requires justification under a different lawful basis (Article 9(2) GDPR). This generalisation is necessary since MARCONI will not be able to determine on a semantic or contextual basis which data contains special categories and which does not and in scanning said data "processing" (Article 4(2) GDPR) will already be performed.

To bundle consent with terms and conditions of a contract over personal data not necessary for the performance of said contract is therefore presumed to be not freely given.[281] This is for example the

---

[271] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, 1–16.

[272] *Albers* in BeckOK DatenschutzR[23] (2017) DS-GVO Art. 6 Point 31.

[273] *Albers* in BeckOK DatenschutzR[23] (2017) DS-GVO Art. 6 Point 32.

[274] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 6 Point 13.

[275] *Albers* in BeckOK DatenschutzR[23] (2017) DS-GVO Art. 6 Point 32.

[276] *Buchner/Petri* in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 6 point 27-32.

[277] *Schulz in Gola*, DS-GVO (2017) Art. 6 Point 27.

[278] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 6 Point 13.

[279] *Schulz* in *Gola*, DS-GVO (2017) Art. 6 point 27; different opinion: *Buchner/Petri* in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 6 point 28.

[280] *Buchner/Petri* in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 6 point 59*; Zankl*, E-Commerce-Gesetz (2016) § 3 point 63.

[281] Recital 43 GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

case in social media networks with having to agree to the terms and conditions of a service provider with no possibility to revoke consent when personal data is being used for marketing purposes such as personal advertisement.[282] Rendering the agreement to the collection of additional data compulsory to the data subject via the method of consent is therefore illegitimate and consent not possible.

The data is needed for the performance of a contract when[283]:

- The data processing is needed for the characteristic counter performance
- Expediency of the processing for better performance
- Indispensability

Personal data that is not strictly needed for the performance of a contract shall require a different justification for processing. This could be consent. It must be presented aside from the privacy notice in a separate form.[284]

Natural persons sharing media or stories using the MARCONI app have to be given the opportunity to consent coupled to the terms and conditions.

It is allowed to couple the data protection guidelines with the regular Terms and Conditions, however it must be highlighted specifically.[285] This is not the case if Terms and Conditions are found in a subsection containing several pages. So in order to gain valid consent as required by Article 6(1) GDPR, this should be avoided.

Terms and Conditions must therefore be clearly structured and, in case of using the app, must be easily reachable, preferably within a single 'click'.

The app should hold all information as described in a way that the user can only agree via an informed consent. While this is impossible to achieve as the user cannot be forced to read and comprehend what the text says, the safest approach would be using an abbreviated abstract with the most necessary information the user must "scroll through" in order to reach a confirmation dialog while providing the possibility to further 'investigate' the rest.

However, the lawful basis 'performance of a contract' can be helpful when a data subject could withdraw his consent (Article 17(1)(b) GDPR). After said action, it is being debated if the controller can switch to another legal basis of processing.[286]

---

[282] *Bräutigam*, Das Nutzungsverhältnis bei sozialen Netzwerken - Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten, MMR 2012, 635.

[283] *Buchner/Petri* in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 6 point 39-46.

[284] See Chapter 6.2.

[285] *Ernst* in *Paal/Pauly*, DS-GVO² (2018) Art. 4 point 85.

[286] Art. 17 (1) (b) GDPR: "*where there is no other legal ground for the processing*"; *Schulz* in *Gola*, DS-GVO Art. 6 point 11; dissenting: WP29, Guidelines on Consent under Regulation 2016/679 wp259, first revision (2018), 22; *Buchner/Petri* in *Kühling/Buchner,* DS-GVO² 2018, Art. 6 point 22.

Co-funded by the Horizon 2020 Framework Programme of the European Union

5.2.1 MARCONI WEBSITE

While MARCONI is at its early stages, it will allow users to access an embedded chat interface as it was being performed on the homepage of Stadtfilter. No affirmative action will be required on the user side. A contract requires affirmative or at least conclusive action by one party; this has to be a declaration of intention. The subject is able to access the feature by simply entering and sending text. This was being utilised in order to train the chatbot and related services. However, the user is usually not being presented with the possibility to enter into a contract as well as will not have the general impression of doing so since, on a goodwill basis, no declaration of intent happens. This effect could be mitigated by an application that will let the user sign in before using the service itself, rendering it easier to construct an obligation.

5.2.2 MOBILE APPLICATIONS

MARCONI will provide a mobile application through the means of an App-Store like Google Play or the Apple App-Store. The user will, before entering into relations with the app provider, be presented a text message or text box. Multiple opinions exist on with whom a contract will be concluded when a user downloads an app via the app store. *Lachenmann* uses the agreement between the app stores and the developer[287] whereas *Bisges* finds that for the reasons of liability issues and developers being the ones offering their various services and should be the ones a contract will be concluded with.[288] As following the opinion of *Lachenmann*, the Apple App-Store would yield the result of the contract being concluded between the data subject and Apple Inc. a message shall be presented, designating the user and MARCONI as parties.[289] While using the MARCONI app data such as the client device name, the manufacturer as well as the IMEI will be processed. Even though it will be important for MARCONI to know the device type of messages in order to customize messages and notifications, data such as the IMEI will not be strictly necessary for the performance of the service as mobile applications can store other identifying data in the local cache in addition to the user logging into an account.

All processing activities must be mentioned in the Privacy Policy Statement or Terms and Conditions of a contract in the download section (or page) before downloading the app itself.[290] This would also correspond to the best practice. The GDPR requires a granular approach, meaning that comprehensibility needs to suit the technical and legal layman while referring to the full "Terms and Conditions" on a side note. The Article 29 Working Party suggests that consent notices should have layers of information so that they do not overload viewers with information, but make necessary details easily available which is important concerning mobile devices as the screen often does not permit sufficient space.

5.3 Legitimate Interests

According to Article 6(1)(f) GDPR processing shall be lawful if "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests

[287] *Lachenmann* in Solmecke/Feldmann/Taeger, Mobile Apps (2013), Chapter 3, point 339.

[288] *Bisges*, Schlumpfbeeren für 3000 Euro – Rechtliche Aspekte von In-App-Verkäufen an Kinder, NJW 2014, p 183.

[289] *Peschel/Schwamberger*, Der Vertragspartner beim App-Erwerb, ZIIR 2016, p 413.

[290] *Koreng/Lachenmann*, Formularhandbuch Datenschutzrecht[2] (2018) 520.

Co-funded by the Horizon 2020 Framework Programme of the European Union

are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

Even though within MARCONI, it appears that this weighing of interests as stated in Article 6(1)(f) GDPR would primarily be relevant in the context of processing publicly available data (see below, Chapter 5.4). However, since Article 6(1)(f) GDPR does not require a specific source of data (i.e. public or private) and since there is a more specific ground for justification of processing regarding data that has been made public, it seems appropriate to include a separate Chapter that focuses on Article 6(1)(f) GDPR

Legitimate interests according to Article 6(1)(f) GDPR can also encompass economic interests of the controller. Additionally, this provision has to be interpreted in harmony with the fundamental freedoms of the European Union (e.g. freedom of press and radio broadcasting, see below).[291] To further determine this rather abstract provision, Recital 47 states that one must consider whether the data subject can "reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place."

These legitimate interests of the controller (or a third party) need not outweigh the interests or fundamental rights and freedoms of the data subject but should simply not be overridden by them.[292] Article 6(1)(f) GDPR should, however, not be understood as a catch-all provision that would allow almost any processing, as long as there is an "argumentative facade".[293]

The controller shall face the necessity to process said data in order to pursue a purpose which serves certain legitimate interest. The next step includes the normative and individual[294] weighing of interests between controller and data subject.[295] However, the weighing of interests according to Article 6(1)(f) GDPR should not be understood as a case of a principle of proportionality but rather as a corrective[296].

The weighing of interests should be evaluated among the following points:

- Affiliation with the controller
- The processing is foreseeable or customary in trade
- Reasonable expectations of the data subject

In the context of MARCONI, the Right to Freedom of Expression (as enshrined in Article 11 of the Charter) should be addressed in this context. It is a fundamental freedom of the European Union, and as such, has to be considered when interpreting provisions the GDPR.[297] According to Article 85(1)

[291] Rec. 4 GDPR.

[292] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 6 point 26.

[293] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 6 point 26 and *Schulz* in *Gola*, DS-GVO (2017) Art. 6 point 13.

[294] ECJ 19 October 2016, C-582/14 ("Breyer") ECLI:EU:C:2016:779; Rec. 44.

[295] *Albrecht/Jotzo*, Das neue DatenschutzR (2017) Part 3 point 5.

[296] *Albers* in *Wolff/Brink* BeckOK Datenschutzrecht[23] DS-GVO (2017) Art. 6 point 50.

[297] *Dienst* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 414.

Co-funded by the Horizon 2020 Framework Programme of the European Union

GDPR: "Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression." This means that Article 85 GDPR constitutes a soft opening clause for Member States in order to institute more precise regulation in the context of journalistic tasks.

But even without an explicit law of the Member States the right to freedom of expression has to be taken into account when balancing of interests according to Article 6(1)(f) GDPR since freedom of expression can amount to a "legitimate interest pursued by the controller or a third party".[298] In addition Recital 153 GDPR, which corresponds to Article 85 GDPR, states that "[i]n order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly".[299]

Even though MARCONI strives to transcend data protection law and will, wherever possible base processing on the consent of the data subject, there can be cases where MARCONI is processing personal data without consent of the data subject or for the performance of a contract. In this case it is hard to predict pro futuro, whether processing is lawful or not.[300] However, considering the criteria mentioned above, it should be possible to determine at least to some extent if processing can be considered lawful (regarding publicly available data, i.e. social media data, see immediately below).[301]

5.4 Public Availability of Data

An - if not the most - important source of information has to be the Internet. It enables all of its users to instantaneously communicate with others and share information all over the world. When information is publicly available, it is generally treated differently than information that only a limited number of persons have access to. This also applies to personal data. Since the Internet is also an important source of data for MARCONI, a closer look has to be taken on which grounds the processing of personal data that is publicly available, such as data appearing on a website or a Facebook-profile, is justified.

Firstly it has to be noted, that the GDPR is also applicable on personal data that were disclosed to the public via the Internet.[302] In the Case of Lindqvist[303] the court ruled that even if the website on which data is shared is not commercially used data protection law would be applicable. In addition the court ruled, that the so-called "household exemption" does not apply when the processing of personal data consists in the publication on the Internet. This exemption is stated in Article 2(2)(c) GDPR according to which "[t]*his regulation does not apply to the processing of data* [...] *by a natural person in the course*

[298] As can be seen especially in Rec. 4 but also as a general theme (see: Rec. 65, 153 and Art. Art. 17(3)(a) and 85 GDPR).

[299] Rec. 153 GDPR.

[300] *Buchner/Petri* in *Kühling/Buchner*, DSGVO[2] (2018) Art Art. 6 point 142.

[301] Regarding the „balancing test" refer to *Dienst* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 395.

[302] ECJ 16 December 2008, C-73/07 ("Satakunnan Markkinapörssi and Satamedia") ECLI:EU:C:2008:727 Rec. 38.

[303] ECJ 6 November 2003, C-101/01 ("Lindqvist") ECLI:EU:C:2003:596.

Co-funded by the Horizon 2020 Framework Programme of the European Union

of a purely personal or household activity"[304]. The ECJ ruled that the household exemption "must [...] be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the Internet so that those data are made accessible to an indefinite number of people"[305].

It may be difficult to establish if a website is "public", e.g. accessible by an unrestricted number of people.[306] Restrictions of access have to be taken into account in the assessment (e.g. sharing via social media or privacy settings).

Most data subjects using social media are generally unaware that posts are being indexed by third parties. Through the terms and conditions of the respective service consent is required in order to gain access to the platform. However, consent of the data subject may justify processing only if it is freely given, specific, informed and an unambiguous indication of the data subject's wishes (see Chapter 5.1).

When applying social media analysis where the potential data subject cannot be informed of the processing beforehand, there is need for another ground for justification of processing (other than consent).

According to Article 9(2)(e) GDPR processing of personal data shall not be prohibited if processing relates to personal data which are manifestly made public by the data subject. This ground of justification also applies to "public posts" on social media platforms.

Personal data is already "made public" if the subject releases data into a public space.[307] It is not necessary that a certain amount of people actually take notice of this information. The accessibility to an indefinite number of people is therefore sufficient.

Even if Article 9 GDPR is applicable only to processing of "special categories of personal data", this clause is still relevant regarding processing of "normal" personal data. This is because the fact that processing data that is not encompassed by the categories of Article 9(1) GDPR does not even require said special grounds of justification, allows an *argumentum a maiore ad minus*.[308] The important question is whether or not data is "manifestly made public" by the data subject. However since social media data may be personal information not about the user himself this ground for justification may not always be applicable, when analysing social media data. In this case the need for a weighing of interests according to Article 6(1)(f) GDPR arises (see Chapter 5.3). However, the ECJ already stated that the fact, that personal data is publicly available can be considered when weighing the interests. In respect to publicly available data the ECJ ruled that, "*in relation to the balancing which is necessary*

[304] Art. 2(2)(c) GDPR is identical to Art. Art. 3(2)(2) of the Directive 95/46/EC.

[305] ECJ 6 November 2003, C-101/01 ("Lindqvist") ECLI:EU:C:2003:596.

[306] See *Bessant*, "The application of Directive 95/46/EC and the Data protection Act 1998 when an individual posts photographs of other individuals online", European Journal of Law and Technology Vol 6 No 2 (2015), 8.

[307] *Haas* in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.) Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018) Die Verarbeitung besonderer Kategorien personenbezogener Daten, 67.

[308] A weighing of interests according to Art. Art. 6(1)(f) GDPR would yield a similar result, since processing of data made public by the data subject would not infringe his fundamental rights in a significant manner and therefore the business or market interests of the controller would prevail.

Co-funded by the Horizon 2020 Framework Programme of the European Union

pursuant to Article 7(f) of Directive 95/46[309], it is possible to take into consideration the fact that the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources.[310] The ECJ also states that "[u]*nlike the processing of data appearing in public sources, the processing of data appearing in non-public sources necessarily implies that information relating to the data subject's private life will thereafter be known by the data controller and, as the case may be, by the third party or parties to whom the data are disclosed. This more serious infringement of the data subject's rights enshrined in Articles 7 and 8 of the Charter must be properly taken into account by being balanced against the legitimate interest pursued by the data controller or by the third party or parties to whom the data are disclosed.*"[311]

Processing of data already publicly available is generally a less serious infringement of a data subject's right to privacy, than that of non-public data.

From a technical point of view, social media as well as forums usually allow searching and indexing their services either through and API or allow or deny access to their sites through robots.txt in order to decide if an indexer should have access for his specific purposes. Services like Twitter and Facebook use their own interfaces when it comes to searching through posts and a user database. Since the application of "robots.txt" on a website means only a prohibition of indexing by search engines, it does not expressly exclude consent to processing data publicly available.

According to the principle of informational freedom, publicly available data shall be used by anyone[312] and, according to *Martini,* "*no limits*"[313] exist regarding purpose limitation. As *Jahnel* points out, when gathering posts from social media networks it shall be considered whether additional information is gained by processing (e.g. via profiling) which themselves are not publicly available.[314] This seems to be the logical conclusion, when considering the fact that this additional information cannot be included in the intention of the data subject when deciding to make it publicly available. Also Gola considers that if public data shall be saved in any way, the intended purpose of the discernible, original data publication shall be considered.[315]

If the processing is not based on the data subject's consent or on a Union or Member State law[316], according to Article 6(4) GDPR, processing for a purpose other than that for which the personal data have been collected can be justified. In order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, the controller has to take into account, inter alia:

---

[309] Equivalent to Article 6(1)(f) GDPR.

[310] ECJ, 24 November 2011, C-468/10 and C-469/10 ("ASNEF" and "FECEMD") ECLI:EU:C:2011:777, Rec. 44.

[311] ECJ, 24 November 2011, C-468/10 and C-469/10 ("ASNEF" and "FECEMD") Rec. 45.

[312] *Martini*, Wie neugierig darf der Staat im Cyberspace sein? Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen, VerwArch 2016, 331.

[313] *Martini*, Wie neugierig darf der Staat im Cyberspace sein? Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen (2016), VerwArch 2016, 354.

[314] *Jahnel*, Datenschutzrecht (2010) Points 1/45 ff, 2/19 & 4/25.

[315] *Schulz* in *Gola*, DS-GVO (2017) Article 6 point 92.

[316] Which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1).

Co-funded by the Horizon 2020 Framework Programme of the European Union

- any link between the purposes for which the personal data have been collected and the purposes of the intended further processing
- 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, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10
- the possible consequences of the intended further processing for data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymisation

It seems, however, that Article 6(4) GDPR only refers to data that is already processed by the controller and allows only to extend processing of said data to another purpose that is linked to the original purpose of processing. It does not however justify processing of newly generated data, as is the case with profiling. Such generated data can only be processed, if processing is justified by Article 6 or 9 GDPR. The criteria mentioned in Article 6(4) GDPR should, however, be considered when weighing the interests according to Article 6(1)(f) GDPR.

In conclusion: while the processing of public data is in general more easily justifiable than data that is not in the public domain, data protection law is still applicable. As described above, when evaluating justification of processing of publicly available data, differentiation has to be made between the way the data has been made public (by the data subject itself or otherwise) and between the intended purpose of processing.

When public data is used for the purpose of sharing it unaltered with an audience this processing of personal data is justified. If the data has been manifestly made public by the data subject, this even applies to special categories of data.

When public data is used for the purpose of profiling, it has to be considered that profiling might generate new data that has not been made public and is therefore – even if based on data that has been made public by the data subject itself – not justified on the basis of its publication. However, processing can be justified if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party and such interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. This means that as long as the profiling is restricted to certain purposes (i.e. musical preferences) and does not generate special categories of data (sexual preferences, medical data) it is still justified by the legitimate (business) interests of the controller. In any case the controller needs to consider Article 13 and 14 GDPR which constitute the duty to inform the data subject when their personal data is being processed.

Co-funded by the Horizon 2020
Framework Programme of the European Union

6 Transparency

The GDPR as well as the Electronic Commerce Directive 2000/31/EC constitute several obligations concerning information provisions. Pursuant to Article 5 of the EC-Directive that information of the service provider such as name, geographic address, communication details, trade registers and relevant supervisory authorities must be easily and permanently made available.[317]

6.1 Terms and Conditions

In the Terms and Conditions, the user has to give his consent to the envisaged data processing activities. Thus, such provisions should be included in the special part of the Terms and Conditions concerning data protection, subject to appropriate form of consent.

The Privacy Policy Statement should not be hidden in the Terms and Conditions but be prominent at the beginning or as a pull-down menu.[318]

An important part of the terms and conditions is granting of a non-exclusive license to the radio station of all materials uploaded on the website.

Terms and conditions may also contain disclaimers.

6.2 Privacy Policy Statement

All processing activities must be mentioned in the Privacy Policy Statement. The GDPR requires a granular approach, meaning that comprehensibility needs to suit the technical and legal layman while referring to the full "Terms and Conditions" on a side note. This is also known as a **Layered Privacy Notice**.[319] It means that the user should be able to "click" through the "levels" of the Terms and Conditions and the Privacy Policy. This can also be accomplished by using accompanying graphical hints[320] and signs to aid the user in distinguishing between the use cases of data which may be specified by the European Commission at a later point in time.[321] The WP29 suggests that consent notices should have layers of information so that they do not overload viewers with information, but make necessary details easily available. It is allowed to couple the data protection guidelines with the regular Terms and Conditions; however, it must be highlighted specifically.[322] It therefore should not be buried underneath an overwhelming amount of information.

---

[317] *Zankl*, E-Commerce-Gesetz (2016) § 5 point 96-107.

[318] *Wille* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 1198.

[319] Article-29-Working Party, Opinion 10/2004 on more harmonised Information Provisions, WP100, 6; BMVJ, Best Practice Catalogue for consumer-friendly apps (2017) 5.

[320] Art. 12(8) GDPR.

[321] The initial GDPR draft included signs. These have been discarded in the final version.

[322] *Ernst* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 4 point 85.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Natural persons sharing media or stories using the MARCONI application should have the opportunity to take notice of the Privacy Policy. As opposed to consent, which has to be given voluntarily for the particular case, in an informed and unambiguous manner in the form of a declaration or any other unambiguous confirmatory act by which the data subject indicates that he / she agrees to the processing of personal data[323], the privacy policy should only be presented in order for the subject to take notice and agree to the Terms and Conditions. For the sake of transparency, this could be achieved by presenting the data subject a short but clear version coupled with a brief explanation which data is gathered for what purpose such as:[324]

- Who shall use the data?
- Which data may be used?
- For which purpose will it be used?
- Is the controller allowed to distribute the data? And if yes, to whom?
- How long will data be saved?
- Where will the data be processed?

Forcing the user to share personal data is unlawful and as in case of doubt, the user agrees involuntarily.[325] This also applies to a notification of non-intrinsic disadvantages. Article 7(3) GDPR provides the need to inform the data subject of his rights according to Section 2 of the GDPR. If such an admonition is missing, it is unclear whether the consent is void in its entirety or just in its respective sections.[326]

Information provided to the data subject shall increase the transparency of data processing activities for individuals and permit them to effectively exercise their rights. Every communication with the data subject shall be governed under the principle of transparency (Art. 5(1) GDPR) together with conciseness, easy access as well as intelligibility combined with clear and plain language (Art. 12 GDPR).[327]

Conciseness requires the information provided to be comprehensive in regards to its content.[328] As it must be intelligible, unnecessary information should not be provided.

Accessibility means that the controller must ensure that the target group of data subjects must be considered as far as the adaptation of information is concerned.[329] Since MARCONI does not target an adolescent audience, no specification of information is needed. However, it is for the radio stations deploying MARCONI to decide on a different approach concerning audiences.

---

[323] *Ernst* in *Paal/Pauly*, DSGVO² (2018), Art. 4 point 62.

[324] *Ernst* in *Paal/Pauly*, DSGVO² (2018), Art 4 point 81-83.

[325] *Ernst* in *Paal/Pauly*, DSGVO² (2018) Art. 4 point 7.

[326] *Ernst* in *Paal/Pauly*, DSGVO² (2018) Art. 4 point 77.

[327] *Dienst* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 257.

[328] *Paal* in *Paal/Pauly*, DS-GVO² (2018) Art. 12 point 28.

[329] *Paal* in *Paal/Pauly*, DS-GVO² (2018) Art. 2 point 26.

Co-funded by the Horizon 2020 Framework Programme of the European Union

The developer has to ensure that, according to directive Art. 5 Directive 2000/31/EC, legal information such as the data protection statement is "*easily, directly and permanently accessible*."[330] In Germany

[330] Article 5(1), Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, 1–16.

Co-funded by the Horizon 2020
Framework Programme of the European Union

a "two-click-rule" has been established by the Higher Regional Court Munich.[331] The transparency requirements are thereby met when the user may access this information from anywhere on a webpage or in an app through less than three actions. This could be handled via a menu button and the menu item "Legal" as Art. 12(1) GDPR also allows electronic means for information to be presented.[332]

The information needed can be deducted from Articles 13 and 14 as well as from Article 12 GDPR and needs to be presented to the user **prior to personal data being processed** (Art. 13(1)) as the principle of fairness and transparency requires. This means at the time of collection. When data is being collected from another source, MARCONI will need to provide the subject with the necessary information without undue delay,[333] however latest within:

- one month, having regard to the specific circumstances in which the personal data are processed;
- if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
- if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.[336]

Recital 60: "*The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data.*"

The minimum information required remains largely the same in regards of where data is being collected directly from the user or from another source with the main difference being that the subject must be informed about the source the data originated from (Art 14(2)(f)). In the case of MARCONI, this would be "**publicly available sources**".[334]

The privacy policy statement should, while comprising a general core, be adjusted according to the application the subject engages through. Optional wording for apps should therefore be envisaged.[335]

---

[331] OLG München, Judgement of 11.09.2003, 29 U 2681/03.

[332] *Wille* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) points 1194 & 1220.

[333] *Hennemann* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 14 point 34.

[334] Art. 14(2)(f) GDPR.

[335] *Koreng/Lachenmann*, Formularhandbuch Datenschutzrecht (2018), 520.

[336] Article 14 (3) GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

6.2.1 COLLECTION OF DATA FROM THE DATA SUBJECT

As Article 7(2) GDPR states: "*the request for consent shall be presented in a manner which is clearly distinguishable from the other matters*". Therefore it is important to keep consent requests separate from other terms and conditions.[337] This shows that certain information may be presented twice rendering it even more important to distinguish between these formal requirements. However, valid consent can exist even when requirements of Article 13 and 14 GDPR are not met.[338]

The minimum information required as constituted in Art. 13(1) GDPR is:

- the **identity** and **contact details** of the controller and, where applicable, its **representative**;
- the contact details of the **data protection officer**, where applicable;
- the **purposes** of the processing for which the personal data are intended as well as **the legal basis for the processing**;
- where the processing is based on point (f) of Article 6(1), the **legitimate interests** pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- the fact that the controller intends to **transfer personal data to a third country** or international organisation and the existence or absence of an adequacy decision by the Commission.

Thus, the controller would need to provide details concerning their summonable address, name their DPOs and explain which data are being gathered for which purpose along with the legal basis for processing. Legitimate interests will play an important role when data from other sources is being gathered.

[337] *Frenzel* in *Paal/Pauly*, DS-GVO[2] (2018) Art. 7 point 13.

[338] WP29, Guidelines on Consent under Regulation 2016/679 wp259, first revision (2018) 15.

Co-funded by the Horizon 2020 Framework Programme of the European Union

In order to create a balance of information between subject and controller, additional information shall be presented. However, the provision of the following information must be deemed generally necessary:[339]

- the **period** for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of **automated decision-making**, including profiling, referred to in
- Article 22(1) and (4) and, at least in those cases, meaningful **information about the logic involved**, as well as the significance and the envisaged **consequences** of such processing for the data subject.
- the existence of the right to request from the controller **access** to and **rectification** or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the **right to withdraw consent** at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right **to lodge a complaint** with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as **whether the data subject is obliged to provide the personal data** and of the possible consequences of failure to provide such data;

According to Article 13(2)(f) GDPR, such additional information would include the information about the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR.

Article 22 GDPR constitutes that automated decision making has to "*produce legal effects concerning him or her* [data subject] *or similarly significantly affects*" the data subject. Since basically anything could show regards to a legal effect, this specific regulation has to be interpreted restrictively.[340] Does the selection for a prize game (User Scenario 1) already fall under the scope of "legal effects"? Looking at Recital 71 GDPR, it might appear that only negative and restricting legal consequences fall under the scope. With regards to the wording of Article 22(1) GDPR "*similarly significant affects"* or in the German wording "in ähnlicher Weise […] beeinträchtigt", meaning that the additional scope of similar effects encompasses only adverse consequences, the second element would therefore also not be fulfilled.[341] The same applies for queries the user sends to the MARCONI bot to find song names.

[339] *Paal* in *Paal/Pauly*[2], DSGVO (2018) Art. 13 points 22–23.

[340] *Lewinski* in BeckOK DatenschutzR[24], DS-GVO (2018) Art. 22 point 28.

[341] *Buchner* in *Kühling/Buchner*, DSGVO[2] (2018) Art 22 point 25.

Co-funded by the Horizon 2020 Framework Programme of the European Union

While every translation of the text of the directive is equally valid and is therefore of the same importance as the initial (English) version, there still is some discussion in the literature regarding the necessity of said negative impact since the GDPR does not define the threshold of "similarly significantly effects". The WP29 states, however: "similarly significant effects may be positive or negative."[342] Ultimately, this depends on how the radio station uses MARCONI, e.g. for automatically selecting a "winner" or simply engaging with his audience. "Legal effects" should only occur when a contract should be formed or the data subject should gain non-contractual claims on another basis.[343]

Direct advertisement shall not be considered a 'similar effect' according to the WP29 though there are possible exceptions to this rule.[344] This varies for the extent the profiling is being performed. MARCONI does in this stage not process detailed information about individual preferences that could be used to classify the subject in terms of solvency, financial security and similar properties meaning that targeted advertisements would not discriminate a specific group of people with sufficient effects. The WP29 names as example with malicious intent in showing an insolvent individual advertisements for online gambling.[345]

Automated decision making is explicitly forbidden unless one out of three requirements in Article 22(3) GDPR is met. Pursuant to Article 22(3) GDPR, allowed automated decision making requires either the necessity for the performance of a contract, the authorisation by a Member State law or 'explicit' consent. In the MARCONI project, explicit consent should be used, regardless of the possibility of the first option. Consent "*must be specifically confirmed by an express statement rather than some other affirmative action*".[346]

Necessary transparency must also be taken into account. It is important to inform the data subject that processing according to Article 22 GDPR is being carried out along with the consequences this operation might bear and to briefly explain the logic involved.[347]

In this context, the user has a "right of access" according to Article 15(1)(h) GDPR. The user should be informed about his categorisation, for example, according to the music he "likes" and about the use of said profiles to engage individually with him/her in order to gain feedback for the show via the modalities of MARCONI. The WP29 also states that it shall be good practice to inform the user of such processing regardless if requirements of the scope of Article 22 GDPR are fulfilled.[348] MARCONI must ensure that the user is able to view the collected personal data corresponding to his profile as well on demand.

Profiling as a special case of data processing is relevant for Article 22 GDPR which grants the data subject the right "*not to be subject to a decision based solely on automated processing, including*

[342] Article 29 WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2017), WP 251, 11

[343] *Buchner* in *Kühling/Buchner*, DSGVO[2] (2018), Art. 22 point 24.

[344] Also: *Buchner* in *Kühling/Buchner*, DSGVO[2] (2018), Art 22 point 26.

[345] Article 29 WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2017), WP 251, 20.

[346] Ibidem.

[347] Refer to Chapter 6.2.

[348] See above.

Co-funded by the Horizon 2020 Framework Programme of the European Union

profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". The qualification as profiling is also important in regard to Article 35 GDPR which lists preconditions regarding the necessity for a privacy impact assessment.[349]

6.2.2 COLLECTION OF DATA FROM ANOTHER SOURCE

Pursuant to Article 14(1) GDPR, the controller must provide the data subject with additional information in addition to Article 13(1) GDPR. This encompasses the

- ➔ source of the personal data and whether it is
- ➔ publicly accessible (Article 14(2)(f) GDPR).

Where the origin of the personal data cannot be provided due to the amount of sources use, general information shall be provided.[350]

If pilots are being run, MARCONI participants have to be informed about their rights considering Articles 15 to 22 GDPR along with the right to file a complaint against the controller. However, it is **not necessary** to **provide the data subject with names or contact details of data protection authorities** (DPA).[351]

As MARCONI changes the scope of operations and integrates more data and datatypes, the privacy statement must be adjusted and presented before additional processing operations are carried out.

6.2.3 WEBSITE AND APP

The following is an example for the privacy policy statement of MARCONI based on *Koreng/Lachenmann*.[352]

Information regarding the processing of personal data
[The data controller], provides you, the consumer, with a digital service and a mobile app which you are able to install on your consumer device. In the following, we inform you about the processing of personal data which is information that renders you identifiable by us or a third party, e.g. your name, address, Email address, user behaviour.

The controller according to Art. 4(7) General Data Protection Regulation (GDPR) is [controller]. (Our DPO is [DPO] with the following contact information: [contact information].)

If you choose to register at our platform we will collect your Email address and, if you choose to, your full name as well as your address in order to stay in contact with you and provide our service. After processing is no longer necessary your personal data will either be deleted or anonymised or – in case of legal obligations to keep data – processing will be restricted.

---

[349] See Chapter 8.4 – Data Protection Impact Assessment.

[350] Rec. 61 GDPR.

[351] *Schmidt-Wudy* in *BeckOK* DatenschutzR[23], DS-GVO (2018) Art. 15 point 71.

[352] *Koreng/Lachenmann*, Formularhandbuch Datenschutzrecht, Beck (2018) 521.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Where personal data will be processed by third parties or for different purposes, more detailed information can be found below.

Your rights
You have the following rights concerning your personal data:

- right to access;
- right to rectification or deletion;
- right to restriction of processing;
- right to object the processing;
- right to data portability.

In addition, you maintain the right to lodge a complaint with a [supervisory authority].

Website
Should you decide to use our website without registering we only collect personal data that your browser sends to our webserver under Art. 6(1)(f) GDPR. If you want to view our website on your device we only collect the data which are necessary to show you content as well as maintain stability and safety which are:

- your IP address;
- date and time of your request;
- the webpage requested;
- the transferred amount of packets;
- your Browser;
- your operating system and the user surface;
- HTTP-status code;
- language and version of your browser.

In addition, we use cookies, which are text files with information located in your browser cache. These are being placed by us and help in re-identifying your browser after your IP changes.

[In this section, the use of cookies should be explained. Will it help to re-identify the user? Will these be used for automatic login? Grounds of justification should remain either Art. 6(1)(f) or Art. 6(1)(b) if consent is not feasible.]

Co-funded by the Horizon 2020
Framework Programme of the European Union

Transient cookies are being deleted after you close your browser session and are needed to connect your browser requests to a single session. Persistent cookies will delete themselves after a certain amount of time, however you can block our or third party cookies in your browser settings.[353]

App
If you should decide to use our app we collect the following personal data in order to maintain stability and safety of our system under Art. 6(1)(f) GDPR:

- your IP address;
- date and time of your request;
- the webpage requested;
- the transferred amount of packets;
- your operating system and the user surface;
- HTTP-status code;
- language and version of your browser.

Furthermore, we require

- the IMEI (International Mobile Equipment Identity) as well as the MAC-address when used with WiFi;
- the name of your device manufacturer and your device.

6.3 Cookies and Trackers

Special transparency requirements arise with the use of cookies ("*access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information*"[354]) as long as they carry personal data.[355] This can either happen through the privacy policy statement as outlined above or directly through a banner.[356] According to the WP29, cookies must conform to two criteria[357] in being either strictly necessary for communications or being requested by the user and required to perform a service of the information society. For detailed information regarding the implementation of the transparency requirement please refer to the Chapter above. MARCONI will use cookies from social plugins such as

[353] Art. 5(3), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201 , 31/07/2002, 37 – 47.

[354]Art. 5(3), Directive 2002/58/EC.

[355]Christoph Berdenich, Datenschutz online: Analytics & Tracking-Cookies, Dako 2016/51 (81).

[356] Example on http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm (19.6.2018).

[357] WP29, Opinion 04/2012 on Cookie Consent Exemption, 00879/12/ENWP 194, 2-4 (2012).

Co-funded by the Horizon 2020 Framework Programme of the European Union

the Facebook login which will not match the first criterion if the user is not already logged in.[358] The user is therefore required to opt in. Otherwise, the general principles of the GDPR apply.

Social Plugins shall be considered trackers as well, as they gather personal data in order to generate statistical information about website use or store personal preferences of the subject to display personal advertisement. A Facebook Plugin transmits data such as session cookies and transient cookies of the implemented webpage as well as cookies used for identification of the subject from other partner sites.[359] It is debatable whether website operators are fully responsible as controllers for the data collected by such plugins but should take full responsibility for any personal data collected on their website.[360] However, considering the latest ruling of the ECJ, *Schleswig-Holstein,* entities processing personal data are being considered joint controllers if the operator is able to request analytics from the service provider.[361] *Wille* suggests a "*double-click solution*" in order to gain the user's consent.[362] This can be achieved by letting users enable social plugins themselves or only providing a link to the social media platform, thereby assuring that no personal data is being collected by the website and immediately shared with another entity.

6.4 Record of Processing Activities

Each controller and processor shall maintain a register of processing activities (Art. 30 GDPR) if processing is either performed in an organization employing more than 250 persons, the processing is likely to result in a risk to the rights of the data subject or contains special categories of data according to Article 9 GDPR or the processing is not being performed only occasional. It applies to controllers and processors of MARCONI, e.g. the radio stations as well as their technical partners. A processing register must be auditable as Art 30(4) GDPR stipulates that it must be made available to a DPA on request. Such register can therefore either be maintained through specialized software to manage larger data-flows and processing activities or simply in a spreadsheet. The DPA of Belgium released a template that may be used by the consortium partners.[363]

[358] WP29, Opinion 04/2012 on Cookie Consent Exemption, 9 (2012).

[359] Oberlandesgericht Düsseldorf: EuGH-Vorlage zur datenschutzrechtlichen Verantwortlichkeit eines Internetanbieters für Einbindung eines Social Plugin - Like-Button, GRUR Int. 2017, 466 (467).

[360] *Wille* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 1194f.

[361] ECJ, 5. June 2018, C-210/16 („Schleswig-Holstein"), ECLI:EU:C:2018:388, Rec. 33-37.

[362] *Wille* in *Rücker/Kugler*, New European General Data Protection Regulation (2018) point 1196.

[363] https://www.gegevensbeschermingsautoriteit.be/model-voor-een-register-van-de-verwerkingsactiviteiten (19.6.2018); Alternative in English: https://onetrust.com/wp-content/uploads/2017/09/Belgian-DPA-Registry-of-Processing-Activities-Template-20170907-EN.xlsx (19.6.2018).

Co-funded by the Horizon 2020 Framework Programme of the European Union

7 Sharing of Data

The sharing of personal data between the various actors involved in MARCONI is processing of personal data as "disclosure of transmission".[364] This should be an overview of the guidelines that have been developed in the chapters before.

7.1 MARCONI and Radio Stations

As concluded in Chapter 4.3, as of now, it seems likely that MARCONI services will be given as processors on behalf of radio stations, which will act as controllers.

Data that will be generated within MARCONI and transmitted to the radio station, depending on the requirements of each radio station. The sharing of personal data will therefore be part of the processing agreement between the radio station and MARCONI service providers.

Since the processor is not a third party[365], but still a recipient[366], even though the processor may enjoy some privileges, the data flow between controller and processor is still a processing activity that falls under data protection law.[367]

Even more, processing by a processor shall be governed "by a contract or other legal act under Union or Member State law" to set out the essential criteria of the processing activities.[368] So, even though data protection law applies to the sharing of data between processors and controllers[369] the sharing of such data would be an essential part of that contract and therefore be necessary for its performance.[370]

According to Article 28 GDPR, the processor shall not engage another processor without prior specific or general written authorisation of the controller, and has to inform the controller in that case.

7.2 Radio Stations and Third Parties

From a data protection perspective, the sharing of personal data from MARCONI with third parties is, in general, not lawful. If the user contacts the radio station, the radio station could, however, obtain consent of the data subject to process personal data, in which case the data subject may also give

[364] Art. 4(2) GDPR.

[365] Art. 4(10) GDPR.

[366] Art. 4(9) GDPR.

[367] *Fritz*, Der Auftragsverarbeiter im Fokus der DS-GVO, Jahrbuch Datenschutzrecht 2017, 9(15); *Gola* in *Gola*, DS-GVO (2017) Art. 4 point 57.

[368] Art. 28(3) GDPR.

[369] *Fritz*, Der Auftragsverarbeiter im Fokus der DS-GVO, Jahrbuch Datenschutzrecht 2017, 18.

[370] See Art. 6(1)(b) GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

consent to make personal data public. In that case third parties may also process such publicly available data (see Chapter 5.4).

If the data subject however withdraws consent, the radio station would have to take reasonable steps to inform other controllers of the withdrawal of consent. Controllers would have to erase these personal data in accordance with Article 21 GDPR (see Chapter 5.1).

Regarding personal data from MARCONI, this will be different. MARCONI may use publicly available data but generates new data from it. Such data is of itself not manifestly made public by the data subject. Sharing data that is generated within MARCONI therefore requires separate justification (i.e. catastrophes). Without a separate legal ground for the sharing of such data with third parties, it is not lawful (see Chapter 5.4).

The sharing of personal data between Radio Stations and third parties will also be prohibited within terms and conditions between MARCONI service providers[371] and radio stations.

[371] Depending on whether MARCONI will be provided as a service by separate service providers or as a software, that is independently controlled by the radio stations.

Co-funded by the Horizon 2020
Framework Programme of the European Union

8 Privacy by Design and Default

Privacy by Design means, in essence, to design organisational and technical operations in a way that limits all the privacy invading activities to the minimum.[372]

Following Ann Cavoukian, Information and Privacy Officer of Ontario Canada, "[p]*rivacy must be embedded into technologies, operations, and information architectures in a holistic, integrative and creative way. Holistic, because additional, broader contexts must always be considered. Integrative, because all stakeholders and interests should be consulted. Creative, because embedding privacy sometimes means re-inventing existing choices because the alternatives are unacceptable*."[373]

According to Article 25(1) GDPR, the controller "shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement **appropriate technical and organisational measures**, such as pseudonymisation, which are designed **to implement data-protection principles**, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects".

This means that, according to Article 25(1) GDPR Data Protection by Design (or Privacy by Design) aims to implement data protection principles in an effective manner and to integrate necessary safeguards into the processing. To achieve these goals, the controller should take the "appropriate measures". In determining these appropriate measures, the controller should take into account, "*the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*."[374]

The usage of the term "state of the art" is another sign of the flexible approach. Measures taken by the controller should be state of the art in the sense that the most sophisticated technological product or code of conduct should be implemented as far as appropriate. The "cost of the implementation" should be taken into account, but a high cost of an appropriate measure does not mean, that the controller may refrain from implementing it, but rather that the controller should refrain from this specific processing activity, if the implementation of this measure would be uneconomic. When considering the "nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons", the scale of the processing operation, the categories of these data, and the affected number of data subjects should be considered[375] and compared to the potential risks and their severity for rights and freedoms of natural persons.

---

[372] *Hörbe/Hötzendorfer,* Privacy-by-Design-Anforderungen für das Federated Identity Management - Eine datenschutzrechtliche und architektonische Betrachtung, Jahrbuch Datenschutzrecht 2014, 305(307); see also: van Rest/Boonstra/Everts/van Rijn/van Paassen, Designing Privacy-by-Design, in Preneel/Ikonomou, Privacy Technologies and Policy, APF 2012, LNCS 8319 (2014), 55(65).

[373] See *Cavoukian*, Privacy by Design in Law, Policy, and Practice. A White Paper for Regulators, Decisionmakers and Policy-makers (2011) (addressed 10.05.2018 at https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf).

[374] Art. 25(1) GDPR.

[375] Referring to Rec. 92 GDPR & Art. Art. 35 GDPR; in particular the criteria which are relevant to determining when a Data

Co-funded by the Horizon 2020 Framework Programme of the European Union

8.1 Privacy by Design

Article 25(1) GDPR follows a flexible, "risk-based" approach.[376] Depending on the risk of privacy invading activities and their potential consequences,[377] the appropriate measures should be determined dynamically and in the context of these potential risks.[378]

Organisational Measures

The first measure, which is proposed in the GDPR is that of internal policies.[379] Such internal policies may include a privacy impact assessment or a concept of erasure/anonymisation.

Even though a data protection impact assessment according to Article 35 GDPR is only mandatory[380] in case of

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- a systematic monitoring of a publicly accessible area on a large scale,

it is nevertheless useful for the controller to carry out an assessment, that may not be as detailed as that of Article 35, but still includes a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller[381], which can be used as part of the record of processing activities[382] and within the

Protection Impact Assessment is mandatory; see also below.

376 *Hartung* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) 25 point 19; Veil, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip - Eine erste Bestandsaufnahme, ZD 2015, 347; *Voigt/von dem Bussche*, The EU General Data Protection Regulation (GDPR) (2017) 31.

377 Art. 25(1) GDPR.

378 *Hartung* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) 25 point 19.

379 See Rec. 78 GDPR.

380 Art. 35(3) GDPR.

381 See Art. 35(7)(a) GDPR.

382 Art. 30 GDPR; see Chapter 6.4.

Co-funded by the Horizon 2020 Framework Programme of the European Union

information provided to the data subject[383] and an internal assessment of the rights and freedoms of data subjects and the measures to address the risks.[384]

According to Recital 78 GDPR another measure is to grant "*transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features*".[385] Though this is also part of the technical measures since it requires a technical implementation, the importance of transparency[386] should be communicated to every person involved in the act of processing.

Internal policies should also include security training for each person involved. To ensure the security of processing stated in Article 32 GDPR including in particular Article 32(4) GDPR, according to which "[t]*he controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law*." It should be kept in mind that, even though Article 25 GDPR is addressed to the controller, both the controller and the processor must take security measures as stated in Article 32 GDPR.[387]

From an organisational point of view, the controller should also determine which categories of data should be erased, if they are no longer needed. In the example of backups such a concept or policy should include[388], that

- only a limited number of persons should be involved in such backups,
- backups should be accessible only for those persons,
- persons that usually process those personal data should not be allowed to access backups,
- the process of restoring data should be determined precisely (access-restriction and examination of the database),
- the backup-process should be carried out regularly and backup-files should be regularly overwritten.

Technical Measures

[383] Art. 13 & 14 GDPR.

[384] See also *Sassenberg/Schwendemann* in *Sydow,* Europäische Datenschutzgrundverordnung (2017) Art. 35 point 40.

[385] Rec. 78 GDPR.

[386] Regarding the principle of transparency, see also Chapter 1.3.3.

[387] Art. 32(1) GDPR.

[388] For more detail: *Schweiger*, Löschen in Backups – Anforderungen und rechtliche Möglichkeiten nach der DSGVO, Dako 2018/7,10(11).

Co-funded by the Horizon 2020 Framework Programme of the European Union

Recital 78 GDPR also includes data minimisation[389] and pseudonymisation[390] of personal data as possible measures of Privacy by Design.[391]

Data minimization should be implemented by analysing at the early stages of the development of an IT-application which data is needed to achieve the intended purposes.[392] Data minimisation is the specification of the proportionality principle within data protection law.[393] Since appropriate measures are required, the controller should determine which processing of data could be avoided without disproportionately affecting the intended (and legitimate) processing activity.[394]

The other measure that is demonstratively mentioned in Recital 78 GDPR is "*pseudonymising personal data as soon as possible*". "'*Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information*" and provided the additional information is kept separate and is subject to security measures.[395] However, it should be noted that equating pseudonymised data to anonymised data is one of misconceptions among many controllers.[396] Many "anonymisation techniques", like encryption or hashing, may result only in pseudonymized data rather than in anonymised data, depending on whether the data subject is still identifiable.[397]

This means that pseudonymisation of data is a method of privacy by design. In case of MARCONI, it should be used as much as possible. Even if the link between data and an identifier of the data subject (e.g. name) is deleted/replaced (e.g. via pseudonymising), the data subject might still be identifiable which means that the data would still have to be considered personal data.[398] The GDPR does not distinguish between the means through which a person can be identified. According to Article 4(1) GDPR a person can be identified directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This means that movement profiles through geo-information can constitute personal data[399].

Recital 78 GDPR does not explicitly mention anonymisation of personal data. In contrast to pseudonymised data, which can still be connected to a certain data subject, anonymised data is no

---

[389] Art. 5(1)(c) GDPR.

[390] Art. 4(5) GDPR.

[391] *Hartung* in *Kühling/Buchner*, Datenschutz-Grundverordnung² (2018) 25 point 16.

[392] *Pollirer*, Checkliste Datenschutz durch Technikgestaltung und datenschutz-freundliche Voreinstellungen, Dako 2018/27, 43; See also: *Leissler*, Intelligentes Spielzeug: Der Datenschutz im Kinderzimmer, ecolex 2017, 99.

[393] *Feiler/Forgo*, EU-DSGVO (2017) Eine Praxiseinführung in die Datenschutz-Grundverordnung, 9.

[394] *Hartung* in *Kühling/Buchner*, Datenschutz-Grundverordnung² (2018) 25 point 19.

[395] Art. 4(5) GDPR.

[396] *Esayas*, European Journal of Law and Technology Vol 6, No 2 (2015),8; Art-29-WP, Opinion 05/2014 on Anonymisation Techniques, WP 216.

[397] *Esayas*, European Journal of Law and Technology Vol 6, No 2 (2015), 9; regarding personal data refer to Chapter 1.3.2.

[398] *Ernst* in *Paal/Pauly*, DS-GVO² (2018) Art. 9.

[399] *Bergauer* in *Knyrim*, Datenschutz-Grundverordnung (GDPR) – das neue Datanschutzrecht in Österreich und der EU (2016), 54.

Co-funded by the Horizon 2020 Framework Programme of the European Union

longer personal data. This means that data protection law is no longer applicable.[400] Consequently, the evaluation whether certain data driven services can operate by only using anonymised data could be a crucial step in evaluating such services. [401]

One way to achieve anonymisation would be that of aggregation. In this case, data that would individually be considered personal data, could no longer be traced back to a certain individual data subject but only to a certain group of data subjects and could therefore be considered non personal data.[402] Such a group could be created by collectively processing data of a larger geographical area.[403] The problem with this approach could be that certain services require personal data to operate as planned. To ask the question of in how far a certain service requires personal data is – just as the question of in how far pseudonymising is possible – a necessary precondition for privacy-by-design.[404]

To ensure a level of security, appropriate to the risk, both controller and processor shall take appropriate measures, including pseudonymisation and encryption of personal data, ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services as well as the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident and to develop a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational[405] measures for ensuring the security of the processing.[406] Similar to Art. 25, Art. 32 GDPR states that appropriate measures should be taken by the controller as well as the processor[407], taking into account "*the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*".[408]

8.2 Privacy by Default

Similar to Privacy by Design, the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. Both principles – Privacy by Design and Privacy by Default – have similar goals.[409]

---

[400] Rec. 26 GDPR.

[401] *Hartung* in *Kühling/Buchner*, Datenschutz-Grundverordnung² (2018) 25 point 16.

[402] *Haidinger*, Der Weg von personenbezogenen zu anonymen Daten, Dako 2015/34, 56.

403 On the concepts of *k-anonymity, l-diversity* and *t-closeness* refer to WP29, Opinion 05/2014 on Anonymisation Techniques WP216 (2014).

[404] *Hartung* in *Kühling/Buchner*, Datenschutz-Grundverordnung² (2018) 25 point 16.

[405] Security measures should also include organisational measures.

[406] Art. 32(1) GDPR.

[407] *Jandt* in *Kühling/Buchner*, Datenschutz-Grundverordnung² (2018) Art. 32 point 4.

[408] Art. Art. 32(1) GDPR, see also Art. Art. 32(2) GDPR: "In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

[409] *Leissler/Wolfbauer*, EU-Datenschutz-Grundverordnung – ein Weckruf an die Unternehmen, ecolex 2016, 1117.

Co-funded by the Horizon 2020 Framework Programme of the European Union

In particular, measures of Privacy by Default should ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.[410] Privacy by Default also includes the obligation to default settings of processing activities that ensure privacy.[411]

In terms of storing data for marketing purposes, German pre-GDPR law has constituted a period of 2 years to store "lists" of user data for marketing purposes as amended in September 2014. This "deadline" is dependent of the individual case and could be elongated but also shortened.[412] This was the case as well with the previous data protection directive and the timeframe in question should not be in conflict with the subject's rights as constituted in Art. 15 to 22 GDPR and shall not be a burden for the controller.[413]

8.3 Erasure of Data

Data may only be kept, according to the principles of **data minimisation** and **storage limitation** (Art. 5 GDPR), in ways that confine them to the bare minimum needed to perform the necessary services. Recital 39 of the GDPR mentions, that *"time limits should be established by the controller for erasure or for a periodic review."* Thus, all personal data have to be deleted if the user requests to deactivate his account. If the user is in passive mode, an appropriate deletion policy is subject to further investigation. As long as the app stays installed, it may be assumed that the user does not implicitly dissent with the processing of his data.

The question is more difficult to answer when MARCONI applications store personal data gathered on social media. If the data subject should delete the original content, the weighting of interests might lead to the conclusion that the data – though previously public – should be deleted. A possible interpretation of these circumstances under Article 17(1)(d) GDPR may be that a user deleting his content or even his account should result in the deletion of data that was shared via this account. However, it can be argued that data that has been made public by the data subject himself is still to be considered as such, even when the data subject deletes the original version.

Regarding back-up data the prevailing opinion is of practical nature, namely deletion in the same cycles as the back-up is being stored. For instance, a cascading model that gets revised once every day, once a month and then once per year can delete concerned data with the respective work flow steps.[414]

As described in the MARCONI use cases, data may also be gathered not from the user himself, but from social media such as Twitter or Facebook. While under the possibilities listed above, the controller shall also comply with duties to inform the data subject. Please refer to Chapter 6.2.2 for further information.

---

[410] Ibidem.

[411] *Hartung* in *Kühling/Buchner*, Datenschutz-Grundverordnung[2] (2018) Art. 25 point 24.

[412] Düsseldorfer Kreis, Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke, Bavaria (2014), 7;
Reimer in *Sydow*, DS-GVO (2018), Art. 5 point 39.

[413] ECJ 7 May 2009, C-553/07 („Rijkeboer")ECLI:EU:C:2009:293.

[414] *Marzi/Pallwein-Prettner*, Datenschutzrecht auf Basis der DS-GVO (2018) 40.

Co-funded by the Horizon 2020 Framework Programme of the European Union

8.4 Data Protection Impact Assessment

As previously stated a Data Protection Impact Assessment (DPIA) may, according to the non-exhaustive listing of Art. 35(3) GDPR, be necessary when either a "large scale" of personal data according to Art. 9(1) are processed, a systematic monitoring of a publicly accessible area or a systematic and extensive evaluation of personal aspects is performed. This is another part of the risk-based approach of the GDPR, taking into account which processing operations with which data might especially infringe the basic rights of a data subject.

Recital 91: *"This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a **large number** of data subjects **and** which are likely to result in a **high risk**, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures […]."*[415]

Supervisory authorities (DPAs) may specify processing operations in need of a DPIA which will be collected by the European Data Protection Supervisor (EDPS)[416]. Some countries such as Belgium as well as Poland already created a list.[417] In Austria, a draft for a whitelist exists, exempting research and statistics as well as informational services of official functions.[418]

The WP29 has recommended on if and how to conduct a DPIA indicating what DPAs will expect of controllers when compliance checks or audits are being conducted.[419] In Article 35(1) GDPR, evaluation points on when to conduct a DPIA are listed.

In the following sections, the terms "high risk", "large scale" as well as "new technologies" will be elaborated.

[415] Rec. 91 GDPR.

[416] European Data Protection Supervisor, https://edps.europa.eu/.

[417] Belgium, Recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable (CO-AR-2018-001), https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2018.pdf;

Poland, Polish Data Protection Authority, http://www.klattorneys.pl/wp-content/uploads/2018/04/Mandatory-DPIA-Poland-klattorneys.pl_.pdf (English translation).

[418] Austria, https://www.dataprotect.at/2018/04/03/dsfa-white-list-verordnungsentwurf/

[419] WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN WP 248 rev.01 (2018).

Co-funded by the Horizon 2020 Framework Programme of the European Union

8.4.1 LIKELY TO RESULT IN A HIGH RISK

As the term "likely" is being used the GDPR references a possible incident in the future which entails a significant threat to a natural persons basic rights. Therefore, a previous assessment such as described in Art. 32 GDPR shall be referenced.[420] Said Article considers the "*nature*[421]*, scope, context and purposes of processing*" as well as the "*cost of implementation*" of safety and security measures. Based on these points, MARCONI will have to take into account:

- the quantity; and
- the categories of data processed;
- the modalities of processing (processing steps, collection, timeframe);
- the purposes (which must be clearly defined[422]).

All the above points will be set in relation to the costs of implementation. For example, as MARCONI stores the audience database and shares personal data with its partners, safeguards must be implemented in order to assure that no unauthorized personnel is able to use the API key.

Article 35 GDPR lists three processing operations that in particular require a DPIA[423]:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
- a systematic monitoring of a publicly accessible area on a large scale.

As MARCONI aims to process personal data of a substantial amount of listeners of several radio programs in the Netherlands, Belgium and Switzerland, data may be shared to augment databases of multiple partners. MARCONI apps will process data according to Article 9 GDPR of which the user has consented that it may be made public via a radio program or associated news or entertainment outlet. The nature of the data collected will consist out of music preferences. Metadata will be extracted in order to cluster information, however, it is inherent to the information provided and not newly created. Users will create a profile according to their needs and will be targeted with specific content to personalise their radio experience. As MARCONI will store automatically generated user profiles, the term "personal aspects" should be evaluated as it only relates to properties. Recital 71 GDPR gives examples such as: "*data subject's performance at work, economic situation, health, personal*

[420] *Jandt* in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 6 (2018) point 7.

[421] Types of data collected.

[422] *Buchner/Petri* in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 5 (2018) points 35-36.

[423] Art. 35(3) GDPR; further examples in Rec. 89 and 91.

Co-funded by the Horizon 2020 Framework Programme of the European Union

preferences or interests, reliability or behaviour, location or movements […]". Such data will neither be collected, nor evaluated as "profiling" according to Art. 22 GDPR or is used to analyse or make predictions about individuals. The WP29 states that this evaluation depends on the purpose of classification which considers drawing conclusions and predictions instead of mere clustering.[424] However, it shall be considered that an inference may be drawn by the radio editor that only chooses to engage with a certain kind of group in the listener database despite having no legal consequence.[425] Also, MARCONI as a system does not process a "large scale" of special categories of personal data according to Recital 91 GDPR since the MARCONI consortium only uses the services for piloting as well as does not invite users to share a substantial amount of personal data. This might change when a radio station uses the system for surveys on, for example, political opinions or sexual preferences (see user scenario 4 in Chapter 12.4 for more details). MARCONI does also not systematically monitor a publicly accessible area.[426]

The WP29 lists several processing operations where it deems a DPIA practicable despite it not being a necessity.[427] The criteria relevant for MARCONI are:

- evaluation and scoring;
- special categories of personal or data of a highly personal nature;
- matching or combining datasets without reasonable expectation of the user;
- new technological or organisational solutions.

For evaluation and scoring, please see the outline above. MARCONI does not process a large scale of special categories of personal data. However, MARCONI matches and combines datasets as radio stations will be able to combine the audience database with their own in regards to users who have previously registered a profile under their terms and conditions. While the databases are therefore matched, the user will have a reasonable expectation for this process to happen due to the nature of the relationship between the user and the controller. "*In general, the more unexpected or surprising the further use is, the more likely it is that it would be considered incompatible*". [428] The context of collection would, as the user will interact with MARCONI either over the website or a mobile app of a radio station, that data will be collected and combined as it is also mentioned in the privacy statement.

8.4.2 NEW TECHNOLOGIES

There are several opinions regarding "new technologies" as stated in Art. 35 (1) GDPR. *Martini* states that typically risk-inclined processing methods such as facial recognition, learning algorithms as well

[424] WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 WP 251 rev.01 (2018) 7.

[425] Ibidem.

[426] *Jandt* in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 35 point 12.

[427] WP29, Guidelines on Data Protection Impact Assessment (DPIA) WP 248 rev.01 (2017) 9.

[428] WP29, Opinion 03/2013 on purpose limitation WP 203 (2013), 24.

Co-funded by the Horizon 2020 Framework Programme of the European Union

as sentiment analysis would fit this description.[429] While this is the only opinion on specific technologies, according to *Hansen*[430] and *Sassenberg/Schwendemann*[431] this term shall only emphasize, as it is not further mentioned and specified within the GDPR, the general framework concerning "high risks". *Schmitz/von Dall'Armi* generally emphasize, that "cloud computing" and "smart application[s]" have been around since the early 2000s as well as the internet of things and should be therefore not considered as "new technologies". [432] As MARCONI is also not processing "big data"[433] in this phase, no DPIA shall be required.

[429] *Martini* in Paal/Pauly[2], DS-GVO (2018) Art. 35 point 18.

[430] *Hansen* in *BeckOK*[23], DS-GVO (2018) Art. 35 point 5.

[431] *Sassenberg/Schwendemann* in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 35 point 10.

[432] *Schmitz/von Dall'Armi*, Datenschutz-Folgenabschätzung – verstehen und anwenden, ZD 2017, 57.

[433] *Ward/*Baker, Undefined by Data: A Survey of Big Data Definitions, University of St. Andrews (2013), p 2: "*Big data is a term describing the storage and analysis of large and or complex data sets using a series of techniques including, but not limited to: NoSQL, MapReduce and machine learning.*"

Co-funded by the Horizon 2020
Framework Programme of the European Union

9 IP Law & GDPR, in particular concerning User Generated Content, Images and Videos

Within MARCONI various content of every user and possibly that of other persons (i.e. anonymous users) will be processed. These data can be relevant, not only for the evaluation of data protection compliance, but also regarding intellectual property rules.

IP law is governed by international treaties under the umbrella of the WIPO. Since the 1990's, the EU is harmonising the framework, in particular concerning copyright in the information society, computer programmes, databases, term extension and enforcement. New proposals are in discussion.[434] According to Article 2 Directive 2001/29/EC, Member States shall provide exclusive rights to authorize or prohibit reproduction, communication to the public and distribution of the public in particular for authors in respect of their work.[435]

There are various national differences regarding intellectual property rules between the Member States, which can – at this point – not be included in this summary version.

Data protected by IP law might also contain personal data, and therefore processing of such data might also require grounds of justification according to the GDPR.[436]

In the context of MARCONI, user-generated content, images and videos have to be considered.

9.1 User-Generated Content

Content uploaded by a user may amount to a "work" and therefore be protected by copyright. There is no uniform definition of a "work" within the European framework of copyright law.[437] However, following the ECJ's decision in the case of Infopaq International[438], every "work" would only require to be "original in the sense that they are their author's own intellectual creation" to be protected by copyright. Such original work requires, for example regarding photographs, that they are an intellectual creation of the author reflecting his personality and expressing his free and creative choices in the production. [439]

If it is to be considered an original work, it is protected for the lifetime of the author and in general at least 70 years after death of the author (post mortem auctoris).[440] Copyright applies as soon as the

[434] *Appl* in *Wiebe*,Wettbewerbs- und Immaterialgüterrecht[3] (2016), 183.

[435] Art. 2(a), 3(1), 4(1) Directive 2001/29/EC.

[436] Refer to Chapters 1.3.3 and 5.

[437] *Appl* in *Wiebe*,Wettbewerbs- und Immaterialgüterrecht[3] (2016), 183.

[438] ECJ 16 July 2009 ("Infopaq International") ECLI:EU:C:2009:465.

[439] ECJ 1 December 2011, C-145/10 ("Painer") ECLI:EU:C:2011:798.

[440] Art. 1(1) Directive 2006/116/EC

Co-funded by the Horizon 2020 Framework Programme of the European Union

original work is created. This means that as soon as the user has typed a literary work, copyright is attached and there are no further steps for the author to take, like registration for example.

Since a difficult case-by-case analysis of each post seems impractical, the usage of each post should be considered a use of potential original works which would require justification. Since there is no "fair use" approach within EU-law, careful consideration and/or preparation is needed to tackle legal issues regarding intellectual property. The EU Directive 2001/29/EC allows various limitations to copyright. According to Article 5(1) Directive 2001/29/EC "temporary acts of reproduction […], which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable […] a transmission in a network between third parties by an intermediary, or […] a lawful use of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction[…]".[441] Other limitations as stated for example in Article 5(2) Directive 2001/29/EC, depend on the implementation of such limitations by each Member State

If users (as authors) make their works available to the public themselves, they have to grant a license to the radio station. Re-use from a social media platform may not be covered by a license to the social media platform.

Metadata can be created freely by the radio station as the extraction of metadata cannot be considered the usage of a work.

Therefore, if works are to be made public or distributed by radio stations, this will – not withstanding specific exceptions within national legislation – require a licensing agreement.

9.2 Content Created by Third Parties

It can be presumed that the user uploading content is either the author or has a license to do so but it can be proven of the contrary. Therefore, a statement of the user is required that they are entitled to upload the content.

9.3 Personal Data

As outlined in Chapter 1.3.2 the GDPR only applies to processing of personal data. Some content may contain personal data, in particular concerning images and videos. Therefore, a statement of the user is required that they are entitled to upload and/or make the content publicly available.

[441] Art. 5(1)(a)&(b) Directive 2001/29/EC.

Co-funded by the Horizon 2020 Framework Programme of the European Union

9.4 Pictures and Videos

Three issues have to be considered concerning pictures and videos: copyright, data protection and right to one's own image.

Firstly, the right of the author must be transferred via a licence. It has to be taken into account that even pictures of buildings (original work) may be protected (since not all Member States have made use of Article 5(3)(h) Directive 2001/29/EC).

Secondly, the GDPR comes in. When applying Article 4(1) and Recital 26 GDPR to photographs, the applicability depends on whether information visible on a photograph relates to an identifiable person. Since a natural person can be identified, "in particular by reference to an identifier such as a name, […] location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person", a photograph can in and of itself be regarded as personal data, if such identifiers can be determined within "means reasonably likely to be used […] by the controller or by another person.

Thirdly, a person has a right to one's own image. The right to one's own image is protected under Article 8 of the European Convention on Human Rights which requires national legislation to allow the usage of a picture of a user only after a weighing of interests.

9.4.1 PERSONAL DATA

Pictures or videos may also contain personal data, if a person is depicted and the quality of the media is in sufficient quality, or if they are processed in context of other data that serve as an identifier, since the decision on whether data is personal data depends on all the means reasonably likely to be used by the controller. This means it also depends on the context of the storage. If photographs are stored as part of data extracted from one social media profile, these data – including the photograph – will most likely be personal data. If photographs are personal data, they might even be of a special category of personal data according to Article 9(1) GDPR.[442]

According to Recital 51 GDPR, "those personal data should include personal data revealing racial or ethnic origin".[443] This, however, does not mean that every photograph should be considered to be of a special category of personal data. Recital 51 further states that "[t]*he processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person*."[444]

[442] See Chapter 1.3.3.

[443] "[...] whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races" as Recital 51 further states.

[444] See Recital 51 GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Also, data about the appearance are not in general "genetic data"[445] if such health relevant data can't be established "uniquely" from such photographs.[446] However, photographs may contain personal "data concerning health".[447] For example, if the person on the photograph is wearing glasses.[448]

Other data that refers only to one's lifestyle and not to one's health, is not generally to be considered data concerning health, even though such data could be extracted from such data.[449] This means that photographs can, in some circumstances be sensitive personal data. However, if photographs are processed after they have been manifestly made public[450] or the data subject has given explicit consent[451], these photographs may be processed lawfully, even if they are special categories of personal data. If processing of photographs includes sharing them with the audience, the ground of justification should be that of explicit consent[452], since this would also be a matter of intellectual property law.[453]

The lawfulness of processing of special categories of personal data additionally depends on the context[454] which the wording of the regulation does not immediately imply. The so called "twin function" of data is a prevalent problem: data that has been collected to suit a specific objective but can also be applied to suit other needs which may be forbidden.[455] However, no canon has been formed by the jurisprudence and future ECJ decisions will be necessary in further determining this issue.

9.4.2 RIGHT TO ONE'S OWN IMAGE

The right to one's own image is recognised in European law[456] as well as in national laws.[457] According to the ECHR a "person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development. It mainly presupposes the individual's right to control the use of that image, including the right to refuse publication thereof […]".[458] The right to one's own image has to be balanced with

[445] Art. 4(13), Rec. 34 GDPR.

[446] See also *Frenzel* in *Paal/Pauly*, DS-GVO² (2018) Art. 9 point 14.

[447] Rec. 35, Art. 4(15) GDPR.

[448] *Frenzel* in *Paal/Pauly*, DS-GVO² (2018) Art. 9 point 15.

[449] Also *Frenzel* in *Paal/Pauly*, DS-GVO² (2018) Art. 9 point 15.

[450] Art. 9(2)(e) GDPR.

[451] Art. 9(2)(a) GDPR.

[452] Art. 9(2)(a) GDPR.

[453] Refer to Chapter 9.

[454] *Ernst* in *Paal/Pauly*, DSGVO² (2018) Art. 9 point 6;
Schiff in *Ehmann/Selmayr* DS-GVO Art. 9 point 14

[455] *Frenzel* in *Paal/Pauly*², DS-GVO (2018), Art. 9 point 11.

[456] Art. 8 ECHR.

[457] For example § 22 KunstUrhG (Kunsturhebergesetz, German federal copyright law), §78 UrhG (Urheberrechtsgesetz, Austrian federal copyright law).

[458] ECHR, von Hannover v. Germany (no. 2), Grand Chamber judgment of 7 February 2012, § 96.

Co-funded by the Horizon 2020
Framework Programme of the European Union

the freedom of expression. In case of a public interest, pictures may be taken. The national laws provide a balancing of these interests, in particular the right to data protection and copyright.

Therefore, the use of one's profile picture for advertisement purposes is generally prohibited since one could not establish an implicit consent. It would therefore be better to only include a link to the profile. In the Austrian copyright law, a user uploading pictures of himself does not implicitly forfeit his rights. Therefore, the use of profile pictures as promotion shall need previous consent from the subject.

Co-funded by the Horizon 2020
Framework Programme of the European Union

10 Radio Services in the EU

Radio is mostly governed by national law of the Member States. The use of the radio spectrum is determined by rules of the ITU. Radio frequencies are determined by the International Telecommunication Union (ITU) and its ITU Radio Regulations. Audiovisual media services are partly harmonised by the Audiovisual Media Services Directive 2010/13/EU[459] (AVMSD) that is in the process of revision.

This Directive establishes a framework for cross-border audiovisual media services. EU Member States shall not restrict retransmissions on their territory of audiovisual media services from other EU countries except for reasons of violence, incitement to hatred, pornography, protection of minors, public policy, health and security or consumer protection. Access for people with a visual and hearing disability should be improved. European and independent works should be promoted. Audiovisual commercial communication must comply with certain conditions.

A new legislative proposal amending the AVMSD has been adopted by the European Commission on 25 May 2016 (COM(2016) 287). The cornerstone of origin principle (COO) will be maintained and facilitated. Modifications concerning commercial communications should reduce the administrative burden but protect the most vulnerable. The provisions concerning the prohibition of hate speech will be aligned with Decision 2008/913/JHA. The proposed directive applies to 'information society services' as defined in Directive 2015/1535[460], i.e. to "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. Therefore, the directive applies to on-demand audiovisual media services such as video-on-demand services but does not apply to scheduled (linear) broadcasting services. Further, the proposed directive does not affect Community or national measures that aim to promote cultural and linguistic diversity and ensure the defence of pluralism.

[459] OJ L 95, 15.4.2010, 1.

[460] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015, p. 1.

Co-funded by the Horizon 2020 Framework Programme of the European Union

11 Jurisdiction over Consumer Contracts

11.1 Introduction

The jurisdiction over consumer contracts is one of the special jurisdictional provisions subject to restrictive interpretation[461].

This jurisdiction is, as the ECJ repeatedly held, inspired by the concern to protect the consumer as the party deemed to be economically weaker and less experienced in legal matters than the other party to the contract, this jurisdiction does not apply to an applicant who is not himself a party to the consumer contract in question and therefore cannot enjoy the benefit of the jurisdiction relating to consumer contracts[462]. The same considerations also apply to a consumer to whom the claims of other consumers have been assigned.[463]

11.2 Consumer

As part of a consumer protection regulation within the jurisdiction framework, this special jurisdiction applies only to contracts where one party is a natural person for which the purpose of this contract can be regarded as being outside his trade or profession (a consumer) whereas the other is acting in the exercise of his trade or profession.[464] A person may be a professional vendor within some contracts but a consumer within others. It all depends on whether a certain contract is entered into for the purpose of exercising a person's trade or profession or not.

To determine whether a person concludes a contract intended for purposes which are within his trade or profession the court must not take account of facts or circumstances of which the other party to the contract may have been aware when the contract was concluded, unless the person who claims the capacity of consumer behaved in such a way as to give the other party to the contract the legitimate impression that he was acting for the purposes of his business.[465] This applies also for a legitimate impression that the contract was concluded with a view to pursuing a trade or profession, not at the present time but in the future.[466]

[461] See i.e. ECJ 3 July 1997, C-269/95 ("Benincasa v Dentalkit") ECLI:EU:C:1997:337, ECJ 10 September 2009, C-292/08 ("German Graphics Graphische Maschinen") ECLI:EU:C:2009:544, and ECJ 14 March 2013, C-419/11 ("Česká spořitelna") ECLI:EU:C:2013:165 regarding exceptions (of the general jurisdiction) in general.

[462] ECJ 19 January 1993, C-89/91 ("Shearson Lehman Hutton v TVB") ECLI:EU:C:1993:15 Rec. 18, 23 and 24.

[463] ECJ 25 January 2018, C-498/16 ("Schrems") ECLI:EU:C:2018:37.

[464] See Art. 6 of the REGULATION (EC) No 593/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 June 2008 on the law applicable to contractual obligations (Rome I).

[465] ECJ 20 January 2005, C-464/01 („Gruber") ECLI:EU:C:2005:32.

[466] ECJ 3 July 1997, C-269/95 ("Benincasa v Dentalkit") ECLI:EU:C:1997:337.

Co-funded by the Horizon 2020 Framework Programme of the European Union

In the recent case of Max Schrems vs. Facebook Ireland Limited[467] the ECJ decided that in accordance with the requirement to construe strictly the notion of 'consumer' within the meaning of Article 15 of Regulation No 44/2001, it is necessary, in particular, to take into account, as far as concerns services of a digital social network which are intended to be used over a long period of time, subsequent changes in the use which is made of those services.

11.3 Consumer Contract

Because this jurisdiction applies only to claims regarding consumer contracts it has to be checked whether an award/prize winning is a consumer contract in regard to Article 17 of the Regulation 1215/2012/EU. It has to be noted that such a contract has to be concluded between the consumer and the professional. A contractual chain[468] or the assignment of claims[469] hinders the applicability of this jurisdiction.

Within ECJ C-180/06 (Ilsinger/Dreschers)[470] a case was brought before the ECJ where a consumer (Ms Ilsinger) received a prize notification. The ostensibly won prize did not depend on an order of certain goods. Because of this, it was argued that claims regarding this ostensibly won prize did not concern a contract in regard to Article 15 and 16 of Regulation 44/2001/EC[471] and therefore the jurisdiction of consumer contracts would not be applicable. However the ECJ ruled that even though the jurisdiction of consumer contracts by virtue of the actual wording requires a contract to have been concluded, a contract in that sense does not require both parties to assume a legal obligation. For a contract to exist within the meaning of that provision it would suffice that one of the parties merely indicates its acceptance without assuming itself any legal obligation to the other party to the contract. In this context a prize notification may be regarded as a contract within the meaning of this provision if there has been a legal commitment contracted by the mail-order company or in other words: the latter must have expressed clearly his intention to be bound by such a commitment if it is accepted by the other party by declaring itself to be unconditionally willing to pay the prize at issue to consumers who so request.

In light of the aforementioned decision of the ECJ it has to be concluded that draws or raffles performed by a professional vendor with the expressed intention to be bound by such a commitment to pay the prize at issue constitute a contract in regard to Article 17 and 18 Regulation 1215/2012/EU.

[467] ECJ 25 January 2018, C-498/16 ("Schrems") ECLI:EU:C:2018:37, Rec 37.

[468] ECJ 28 January 2016, C-375/13 ("Kolassa") ECLI:EU:C:2015:37 Rec. 35.

[469] ECJ 25 January 2018, C-498/16 ("Schrems") ECLI:EU:C:2018:37 Rec.49.

[470] ECJ 14 May 2009, C-180/06 ("Ilsinger"), ECLI:EU:C:2009:303.

[471] The recast of this regulation (Regulation 1215/2012/EU) has almost identical wording within the special jurisdiction, this ruling is still relevant in regard to Art. Art. 17 and 18 Regulation 1215/2012/EU; The ECJ already held that the interpretation provided by the Court in respect of provisions of the convention is valid also for those of the regulation whenever the provisions of those instruments may be regarded as 'equivalent (see ECJ 28 January 2016, C-375/13 ("Kolassa") Rec.21).

Co-funded by the Horizon 2020 Framework Programme of the European Union

11.4 Covered Consumer Contracts

Not every consumer contract leads to the applicability of the provisions in Section 3 of the Regulation 1215/2012/EU. According to Article 17 Nr 1 Regulation 1215/2012/EU jurisdiction shall be determined by this section without prejudice to Article 6 and point 5 of Article 7 if:

a) it is a contract for the sale of goods on instalment credit terms

b) it is a contract for a loan repayable by instalments, or for any other form of credit, made to finance the sale of goods; or

c) in all other cases, the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities.

Since a) and b) are not relevant for MARCONI it is point c) and especially the persuasion or the direction of commercial or professional activities in/to the Member State of the consumer's domicile that need closer examination.

The 'direction' of commercial or professional activities to the Member State of the consumer's domicile is apparently to be seen farther as persuasion in the Member State.

Persuasion of commercial or professional activities in the Member State of the consumer's domicile means that the professional vendor is established in said Member State or has an agency or a sales branch within said Member State.

In contrast to the persuasion of one's commercial or professional activities to one of the Member States the 'direction' has been subject of various proceedings before the ECJ.

The first question that had to be answered was if websites, that were in principle accessible in all States, and therefore throughout the European Union, would be a 'direction' of a traders activities to Member States other than that in which the trader concerned is established. The ECJ held that the mere accessibility of a website does not suffice.[472] It must be determined, in the case of a contract between a trader and a given consumer, whether, before any contract with that consumer was concluded, there was evidence demonstrating that the trader was envisaging doing business with consumers domiciled in other Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with those consumers.[473]

The ECJ differentiated between "clear expressions" of the intention to solicit the custom of that State's consumers and "other items of evidence" thereof. Clear expressions include mention that it is offering its services or its goods in one or more Member States designated by name or the disbursement of expenditure on an internet referencing service to the operator of a search engine in order to facilitate access to the trader's site by consumers domiciled in various Member States.

[472] ECJ 7 December 2010, C-585/08 and C-144/09 ("Pammer and Alpenhof") ECLI:EU:C:2010:740.

[473] ECJ 7 December 2010, C-585/08 and C-144/09 ("Pammer and Alpenhof") Rec. 76.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Other items of evidence, would be certain tourist activities; mention of telephone numbers with the international code, use of a top-level domain name other than that of the Member State in which the trader is established, for example '.de', or use of neutral top-level domain names such as '.com' or '.eu'; the description of itineraries from one or more other Member States to the place where the service is provided; and mention of an international clientele composed of customers domiciled in various Member States, in particular by presentation of accounts written by such customers whereas language and currency do not constitute relevant factors for the purpose of determining whether an activity is directed to other Member States.

The ECJ also held that for the applicability of the jurisdiction of consumer contracts it is not required for the contract between the consumer and the trader to be concluded at a distance[474] and also that the it does not require the existence of a causal link between the means employed to direct the commercial or professional activity to the Member State of the consumer's domicile and the conclusion of the contract with that consumer.[475]

In this respect it has to be noted that even if the consumer contract does not come within the scope of the commercial or professional activity 'directed' by the professional 'to' the Member State of the consumer's domicile, but was nevertheless concluded as a direct extension of that activity, and it is complementary to the contract, in that it seeks to make it possible for the economic objective of that contract to be achieved, this close (economic) link may suffice for the applicability of the jurisdiction over consumer contracts.[476]

11.5 Prorogation of Jurisdiction within Consumer Contracts

Within consumer contracts prorogation of jurisdiction is quite restricted. According to Article 19 Regulation 1215/2012/EU the provisions of Section 4[477] may be departed from only by an agreement

- which is entered into after the dispute has arisen
- which allows the consumer to bring proceedings in courts other than those indicated in this Section; or
- which is entered into by the consumer and the other party to the contract, both of whom are at the time of conclusion of the contract domiciled or habitually resident in the same Member State, and which confers jurisdiction on the courts of that Member State, provided that such an agreement is not contrary to the law of that Member State

[474] ECJ 06 September 2012, C-190/11 ("Mühlleitner") ECLI:EU:C:2012:542 Rec. 45.

[475] ECJ 17 October, C-218/12 ("Emrek") ECLI:EU:C:2013:666 Rec. 32;
According to which the existence of such a causal link constitutes evidence of the connection between the contract and such activity.

[476] ECJ 23 December 2015, C-297/14 ("Hobohm") ECLI:EU:C:2015:844.

Rec. 35.

[477] Jurisdiction over consumer contracts, Art. Art. 17-19 Regulation 1215/2012/EU.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Consequentially if the consumer and the other party are at the time of conclusion of the contract not domiciled or habitually resident in the same Member State, clauses within the consumer contract may not prevent a consumer to bring proceedings against the other party to a contract in the courts for the place where the consumer is domiciled or may not enable the other party to bring proceedings against a consumer in courts other than the courts of the Member State in which the consumer is domiciled.

11.6 Conclusion

Within the Regulation 1215/2012/EU the relevant provisions regarding prizes issued via MARCONI are to be found in Section 3 – jurisdiction of consumer contracts.

When prizes are issued via MARCONI within for example raffles, users that are not using the service for their professional activities (consumers) are entering into a contract[478] with the issuing radio station ("other party to the contract"[479]) if the latter expresses clearly its intention to be bound by such a commitment and the consumer merely indicates its acceptance. This contract may lead to the applicability of this jurisdiction if the professional at least directs his activities to the Member State of the consumer's domicile.

This means, that a consumer may bring proceedings against the other party to a contract in the courts for the place where the consumer is domiciled – regardless of the domicile of the other party.[480] Additionally the other party to the contract may bring proceedings against the consumer only in the courts of the Member State in which the consumer is domiciled.[481] Even with a prorogation of jurisdiction in advance both parties (consumer and the other party) of the contract may depart from these provisions, with only few narrow exceptions.[482]

[478] In regard to Section 3 Regulation 1215/2012/EU.

[479] In regard to Section 3 Regulation 1215/2012/EU.

[480] Art. 18(1) Regulation 1215/2012/EU.

[481] Art. 18 (2) Regulation 1215/2012/EU.

[482] Art. 19 Regulation 1215/2012/EU.

Co-funded by the Horizon 2020 Framework Programme of the European Union

12 MARCONI Use Cases Evaluation

In this evaluation of the MARCONI use cases (see document regarding Use Cases and requirements of MARCONI), individual use cases will be analysed and further guidelines will be recommended. Media and intellectual property law will only be briefly outlined as the scope is of territorial nature, therefore varying by country.

12.1 Scenario 1 – Facilitating Relevant Feedback

The presenter of the radio event acts under direct authority of the radio station as the controller. MARCONI's role depends whether it acts as processor[483] or a provider of a software. As the latter, MARCONI would be a "third party" according to Article 4(10).[484]

The display in the rundown is a separate act of processing, namely structuring according to Article4(2) GDPR[485]. The same applies to display of the separate content block, displayed on the rundown. Also the display of additional information on a certain group, along with media that has been sent in by them is alignment/combination of personal data and therefore "processing" according to Article 4(2) GDPR[486]. Especially the combination of datasets as stated by scenario 1.2 by different radio stations could potentially be problematic as the WP29 sees matching and combining of datasets by separate controllers as a possible reason for a DPIA if the subject should not be able to identify or expect said processing operations.[487] This would not be the case if MARCONI as a platform should be operated by the consortium since all partners are being listed in the privacy statement and the purpose encompasses research. Therefore, the data subject is able to reasonably expect a matching of datasets. In the future the application may be handled differently by the radio stations once the product is ready to be distributed and the facts and circumstances will have to be re-checked.

Sent-in media should be analysed as pictures and videos are subject to copyright, right to one's own image and special data protection rules. In using these data, consent of the copyright holder, the pictured person and the data subject must be obtained (see Chapter 9.4.2) or complying to media law. As pictures or videos might easily qualify as "work", they could be protected by copyright law.[488] Depending on whether it is user-generated content or content created by third parties, a licence of either, the user or the third party as the author, must be obtained for the use of the picture. Since it is not feasible to research the origin of such picture or video, a statement of the user is required that he is entitled to upload the content.

---

[483] See Chapter 4 – Role Allocation.

[484] *Regenhardt* in *Sydow*, DS-GVO (2017), Art. 4 point 151.

[485] UC 1.1.

[486] UC 1.2.

[487] WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679 WP248 rev.01 (2018), 10;
WP29, Opinion of Purpose limitation WP 203 (2003), 24.

[488] *Appl* in *Wiebe*, Wettbewerbs- und Immaterialgüterrecht[3] (2016), 183.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Pictures or videos may also contain personal data if a person is depicted and the quality of the media is sufficient, or if they are processed in context of other data that serve as an identifier[489] ultimately leading to the application of data protection laws. Pictures may even be of a special category of personal data according to Article 9(1) GDPR, if they include personal data revealing racial or ethnic origin (Recital 51 GDPR, see Chapter 9.4).

As described in Chapter 9.4.1, however, the lawfulness of processing of special categories of personal data depends on the context.[490] The so called "twin function" of data is a prevalent problem: data that has been collected to suit a specific objective but can also be applied to suit other needs which may lack a lawful basis of processing.[491] However, no canon has been formed by jurisprudence or literature and future ECJ decisions will be necessary in further resolving this issue. In this case it can be argued, that the datatype "content", while linked to a user, does not fall under Article 9 GDPR.

If pictures qualify as special categories of personal data according to Article 9(1) GDPR, processing of such pictures requires the prior explicit consent of the data subject or should only include pictures that have been manifestly made public by the data subject Article 9(2)(e) GDPR. Further, the right to one's own image requires consent of the pictured person, if, for example, the picture should be distributed.

If the user sends in relevant media for the purpose of publication, this will be sufficient consent. This requires information about the usage of the sent-in media beforehand ("We would like to share your stories with other listeners.") (UC 1.3 & 1.4). The adaptation of the content depending on which group is in front of the microphone requires an analysis of certain criteria of the groups. This will generally be covered on the grounds of prior consent as the audience will have to agree to the use of their content (voice) on life radio and can be handled together with such a request.

The analysis of the story represents automated processing, as well as the smart alert that is triggered by relevant keywords resulting from the analysis. The consent in these processing activities will be given by the user, when downloading the app or has otherwise taken part in MARCONI (i.e. via the website) (UC 1.10, UC 1.11).

The request of the telephone number to talk about the story can be a valid consent. It is good practice that MARCONI asks for a telephone number for a single use, leaving the option to store it for future contacting. However, MARCONI will need to specify for how long such data will be stored (Article 13(2)(a) GDPR). As a user that communicates over the radio station app enters into a quasicontractual relationship with the station, data may be processed for an longer time. However, UC 1.12 also fulfills the necessary modalities for a consent under Article 6(1)(a) GDPR.

Telephone numbers can generally be considered personal data (Article 4(1) GDPR) since it is easy for a third party to identify a natural person by consulting a telephone register. The MARCONI app asks for separate consent in sharing said information as well as regarding future storage. In order to comply with the principle of data minimisation, the storage duration ends when the purpose of processing has been fulfilled. To contact the subject at a later point in time with his consent, the data may be stored as long as the MARCONI app stays installed since the consent is coupled to the application (privacy

[489] See Chapter 1.3.2 and 9.4.

[490] *Ernst* in *Paal/Pauly*, DSGVO[2] (2018) Art. 9 point 6;
Schiff in *Ehmann/Selmayr* DS-GVO Art. 9 point 14

[491] *Frenzel* in *Paal/Pauly*[2], DS-GVO (2018), Art. 9 point 11.

Co-funded by the Horizon 2020
Framework Programme of the European Union

settings) and the user would not necessarily assume that his phone number will be stored, for other purposes than for providing the service. However, in order to meet the requirements of informed consent, at least the reasoning behind deletion or a timeframe must be stated. This does not need to be an fixed date but can depend on business law storage requirements for correspondence.[492] The term "for future use" is therefore not sufficient. MARCONI can be integrated with the telephone system of the radio station. A conversation on air is also processing of personal data, if the name of the listener (especially in combination with the city the listener lives in) is mentioned. This would require previous consent or other legal grounds[493] (UC 1.13).

Consent through a button popped up next to the phone number is possible. To ensure it is an informed consent, the "future use" should be specified (for future notifications about interesting topics). Please refer to Chapter 5.1 for further information on other requirements for consent which should be possible to revoke at all times, for example via the settings. This should be communicated to the user (UC 1.14).

In the case of an event such as a concert, the organizer has an interest to take photographs of the crowd for reasons of promotion. Different cases require different treatment. Intimate depictions of a natural person for example will in general not fulfil the requirements of Article 6(1)(f) GDPR. One should be aware of Article 9(2)(g) GDPR and national laws (e.g. sec. 22 – 24 KunstUrhG[494]) which can as well constitute the processing of images in terms of artistic work.

When an editor rejects a media item, it is no longer used by the radio station. According to Article 5(1)(b) and (e) GDPR, the item which might bear personal information should not be stored longer as necessary as the purpose is showcasing and publishing such data. However, upon rejecting media, a small period of time may be assigned in which the editor may reverse a mistake such as a "miss click".

Automatic analysis and profiling according to Article 4(4) GDPR is intrinsic to the service since without the requested real-time response it is not possible to deliver. Consequently even with regard to Article 7(4) GDPR, it is not required for the controller to obtain the data subject's consent through a separate agreement. Profiling means "evaluation of personal characteristics"[495], therefore facts or identity markers are excluded and the context of processing shall be taken into account.[496] According to Article 22 GDPR, a mere pre-selection or structuring of personal data does not fall under this provision.[497] MARCONI only generates instant messages after categorizing user responses without analysing the characteristics of the user in this user scenario. Also, the editorial team has the final say when it comes to contacting a user.

In this user scenario MARCONI automatically analyses incoming messages and tries to derive the context in order to suggest responses. Personal attributes, however, are not processed, merely facts

[492] *Feiler/Horn*, Umsetzung der DSGVO in der Praxis (2018), 49.

[493] See Chapter 5 and immediately below.

[494] German Artistic Copyright Act, Kunsturhebergesetz, BGBl. I S. 266 as amended on 16. 2.2001 I 266.

[495] Rec. 91 GDPR; Art. 35 (3) (a) GDPR.

[496] *Lewinski* in BeckOK DatenschutzR[22], DS-GVO (2018) Art. 22 point 9-11.

[497] Lewinski in BeckOK DatenschutzR[22], DS-GVO(2018) Art. 22 point 16.

Co-funded by the Horizon 2020 Framework Programme of the European Union

and opinions for the sake of storytelling, not in the context of personal evaluation. At this point, no actual profile is built. Therefore, this scenario does not encompass profiling.

12.1.1 SCENARIO 1.2 – AS A SERVICE FOR THE LISTENERS

To evaluate the MARCONI app, it appears that the use of the Facebook messenger does not impose relevant legal issues besides the possible application of the information obligation (Article 14 GDPR). As the GDPR does not specify "obtained from the data subject" it is derived from the context that the place of collection is being described. Personal data is not being "collected from the data subject" when the controller must be sure that the subject itself is not discernibly involved in the collection process.[498] This is not the case here since the user knows precisely with whom he is communicating. If a listener wants to stay in contact and communicate with the radio station, this can be included within the user's consent form but at least in the privacy statement (UC 1.15).

The chatbot categorizes the likes of the users and subsequently stores the information (UC 1.16).

Message from radio station, prize game and invitation to an exclusive live set tonight as a promotion: Bear in mind to limit participation as people around the world will be able to tune in to the program or use the app. Refer to Chapter 11 for more detailed information (UC 1.17).

The live stream provides no relevant problems, however, see Chapter 9 (UC 1.18).

Since MARCONI's purpose is an interactive radio experience, it fulfils its role by providing the option for easy feedback. No particular legal problems arise (UC 1.19).

The analysis of music, played within MARCONI may be considered personal data in regard to the artist/s, however, these criteria are in public domain and can be considered data that has manifestly been made public by the data subject. The offering of a preview version will have to be included in the license from the artist (UC 1.20 & 1.21).

As the user will engage anonymously with the chatbot no further personal data is being logged except for the necessary information required to run the webpage which is justified by Article 6(1)(f) GDPR (UC 1.22).

To log in with a Facebook account or MARCONI profile (alignment of choice with account) will require consent by the user. Since this is optional, the user faces no detriment and will have the necessary information read in the privacy statement in order for the necessary information to be scraped to further personalize the radio experience (UC 1.23). This must be highlighted in the data protection statement as well as taking into account Article 13 GDPR as MARCONI must provide a list of data that will be scraped from the app. Concerning function calls such as user friends[499] do not imply a duty to inform according to Article 14 GDPR as personal data will only be transmitted and saved if individuals have already registered a profile with MARCONI, therefore already being informed.

[498] *Schmidt-Wudy* in BeckOK DatenschutzR[23], DS-GVO (2018), Art. 14 points 30-32.

[499] https://developers.facebook.com/docs/facebook-login/permissions#reference-user_friends (19.6.2018).

Co-funded by the Horizon 2020 Framework Programme of the European Union

There should not be an immediate transmission of user data to Facebook, as there is no chance for the user to opt-in.[500]

Facebook will also collect data which MARCONI will not be able to control. This will ultimately depend on which data will be shared though Facebook-Connect. Such practice could be in need of additional assessment as it will have to be specifically addressed in the privacy policy statement. See Chapter 6.3 for general information.

The choice of the chatbot is a way to give consent to the notification. Therefore, no spam happens since the user can regulate notification settings (UC 1.24).

A chatbot integration on social media relays content to MARCONI which generates a user profile and sends notifications to the client. The user is able to also submit content in form of comments. Using the chatbot the user implicitly consents with the modalities of communication. This means that content that is being sent and received by the Facebook API, possibly contains personal data and special categories of personal data[501] and will be scanned (processed) by Facebook[502].

The process of profiling, as stated above, encompasses the "evaluation of personal characteristics" (Rec. 71 GDPR), meaning the analysis of preferences, behavioural patterns, etc. which are linked to the user profile. As long as they are linked to an URI that renders a user identifiable, such processing falls under the scope of the GDPR. The analysis itself must bear a relative level of complexity[503]; otherwise even simple processing activities would fall under the scope of Article 22 GDPR as automated decision making as well which is not appropriate.

Since a radio station uses prize games to attract listeners and collects personal data in the process to select the winner or to determine the participants in the first place one should be wary of the fact that the winner will be able to file a claim for his prize as he has a subjective right granted by Directive 2011/83/EU[504]. However, the automated decision making is quite trivial as it is described in the use cases as the first 100 to answer or react will receive their prize and no extensive evaluation on the subjects has taken place. Therefore, these user scenarios do not describe automated decision making according to Article 22 GDPR because of the simplicity of the prize game and the fact that a mere pre-selection is carried out.

Since MARCONI in this scenario creates a user profile to determine preferences MARCONI will have to comply with Article 21 GDPR. According to this Article, the data subject may object to profiling if it is justified by means of Article 6(1)(e) and (f) GDPR. If personal data is processed for direct marketing

[500] Moser-Knierim, „Facebook-Login" – datenschutzkonformer Einsatz möglich? – Einsatz von Social Plug-ins bei Authentifizierungsdiensten, ZD 2013, 263 (264).

[501] *Kosinski/Stillwell/Graepelb*: Private Traits and Attributes Are Predictable from Digital Records of Human Behavior. PNAS, March 2013. Online: http://www.pnas.org/content/110/15/5802.

[502] Section 1 of the Facebook Data Policy: https://www.facebook.com/full_data_use_policy.

[503] *von Lewinski* in BeckOK Datenschutzrecht[22], DS-GVO (2017), Art. 22 point 12.

[504] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance, OJ L 304, 22.11.2011, 64–88.

Co-funded by the Horizon 2020 Framework Programme of the European Union

purposes, no weighing of interests is possible. In this case, consent is required that can be revoked at any time.

12.2 Scenario 2 – Co-Creating Content

Listeners using e-mail often use providers that may not comply with the GDPR. Sending them personal data or receiving such from their mail account can be compared to using the Facebook messenger as stated above. The same applies to Instagram.

To structure incoming personal data via the unified interaction interface (UC 2.1, 2.2 & 2.3) can be considered processing Article 4(2) GDPR ("collection", "structuring", "alignment" or "combination"). These processing activities can be based on consent by the user or legitimate interests of the controller, since they do not have a relevant impact on the rights of the data subject.[505]

When listeners are classified by properties and given an animal category based on these properties, this may can be considered as profiling (UC 2.5).

Shared videos impose questions if natural persons can be identified and have an interest in nondisclosure. Consent of the data subject is the best option for processing of personal data. Processing of data in the public domain[506] requires justification either through Article 9(2)(e) or Article 6(1)(f) GDPR, depending on the way the data has been made public (by the data subject itself or otherwise) and the intended purpose of processing. Publicly available data can be shared it unaltered with an audience if the sharing of such data serves any legitimate interest, such as business interests or the interests of public service. If the data has been manifestly made public by the data subject, this even applies to special categories of data.

For the rest of the scenario the above mentioned applies. However, IP law should be considered when featuring user opinions on a show. As the territorial scope of IP law is a national one, this aspect will most likely be already worked out by the radio stations. The same applies for video footage which can only be used without consent within the bounds of the respective IP and media law framework. Licences of each should be given, if their messages are considered "works", which require certain originality.[507]

Consent to the participation in co-creating content can in general be given implicitly by the user by sending the message, provided the user knows about the usage of this information within the article on the website.

Even though it might be considered that sending the link to the website with the final article could be direct-advertisement since the own service is promoted, it is within reasonable expectations of the data subject to receive (and the data subject will most likely have their own interest to receive) such a link.

---

[505] See Chapter 5.3 – Legitimate Interests.

[506] See Chapter 5.4 – Public Availability of Data.

[507] Refer to Chapter 9 – IP Law & GDPR.

Co-funded by the Horizon 2020 Framework Programme of the European Union

12.3 Scenario 3 – Allowing Personal Services

For using a personalized service of the MARCONI app, consent is required for processing of personal data. As stated above, consent of the data subject will be the most relevant ground of justification for processing[508]. If the processing does not include special categories of personal data, consent can be given implicitly, as long as it is "unambiguous"[509] and meets the other criteria of consent.

As described in Chapter 5.1, according to Article 4(11) GDPR, consent shall be:

- Freely given
- Specific
- Informed
- An unambiguous indication of the data subject's wishes

If personalising the services of MARCONI requires personal data, this consent will be given, when opting-in for the service in question. However, in this case it appears that the "personal radio" that can be aborted or listened to with a time-lag does not require the processing of personal data that is not already necessary for classic consumption of the program via the app, but could be simply adjusted via the settings. Notifications about certain topics also will not require further processing of personal data.

However, the evaluation on location data in the GDPR depends on the app knowing about the location change via geo coordinates or only the Bluetooth connection to a vehicle. As only the latter applies, the data concerning the assumption that the data subject is commuting cannot be considered personal data. If the app at a later point in the development process should map the user location and profile him accordingly, the above under profiling may apply. Then, the service that MARCONI offers by adjusting the options depending on whether the user is in the car or not, is a service that should be opt-in separately, informing the user of the processed geo-location beforehand.[510]

A noteworthy aspect can be found in Article 35 GDPR which constitutes a 'data protection impact assessment' where, according to Article 35 and Rec. 75 GDPR, 'risks to the rights and freedoms' are in question. The latter passage also mentions "location or movements" which would fall under the scope of the MARCONI project. The data processing must be evaluated in terms of type, size and frequency of the operation. If such a self-assessment under Article 35 GDPR would result in the identification of such a 'high risk' the supervisory authority must be contacted and duly notified before processing. However, since MARCONI does merely extract metadata from images and makes assumptions based on Bluetooth connectivity of mobile devices, no precise location data is being recorded and the data

[508] See Chapter 5.1.

[509] Rec. 32, Art. 4(11) GDPR.

[510] See Chapter 5.1 - Consent.

Co-funded by the Horizon 2020 Framework Programme of the European Union

subject not systematically monitored as the system merely makes an assumption that the data subject is commuting.[511]

However, as described in Chapter 8.4, such a data protection impact assessment is not required, considering the processing activities that are intended within MARCONI at this state. This does not mean that such an internal privacy impact assessment would not be useful, since some of the required assessments are necessary for the records of processing activities or the privacy statement.[512]

12.4 Scenario 4 – Providing Content on Demand

When other entities are involved in a processing activity, it is important to determine the role of each entity.[513] Personal data that is processed within the service "Alexa" is processed by Amazon[514]. Personal data that is used for the interaction process between "Alexa" and the user is processed, not on behalf of the radio station, but as a separate controller by Amazon. Since there is no relevant influence on the processing of one party by the other or vice versa, both entities will remain separate controllers.[515]

As described in Chapter 4, if MARCONI service providers will offer their service to the radio stations, these service providers will be acting as processors (as long as their processing activities remain within the boundaries of the contract, that governs the processing of such processor[516]). If MARCONI will be used as a software, there would be no processor involved. Instead, only the radio station would process data.

Information provided by the radio station via Alexa will, in general be within public domain. When the user shares information via Alexa, it is, from the point of view of the radio station, not different then the sharing of data via Facebook. Information shared by the user will have to be evaluated separately, regardless of the processing activities of Alexa.

It should be considered which kinds of personal data are being shared with Amazon in order to notify the user according to Article 13(1)(e) GDPR.

Opinions, especially of a political nature such as an opinion on military service, are quite eclectic. It shall be subject to further investigation if Article 9 GDPR is applicable. Since a political mindset can be inferred by almost any comment this should be interpreted restrictively.[517] It depends on which data is stored within MARCONI. If the data is just used for the poll, this use is unproblematic if stored in aggregated form. If the user's answers are processed separately, they should be deleted/or aggregated

[511] WP29, Guidelines on Data Protection Officer 16/EN WP 243 (2016): occurring according to a system, methodical, taking part as a general plan of data collection.

[512] See Chapter 7 (Privacy by Design and Default Measures).

[513] See Chapter 4 – Role Allocation.

[514] Amazon Europe Core SARL, Amazon EU SARL, Amazon Services Europe SARL or Amazon Media EU SARL.

[515] It is however possible, to change that relationship to one of a controller and a processor, by entering into a contract according to Art. 28(3) GDPR.

[516] Art. 28(3) GDPR.

[517] *Ernst* in *Paal/Pauly*, DSGVO[2] (2018) Art. 9 point 12

Co-funded by the Horizon 2020 Framework Programme of the European Union

after the poll. If metadata is extracted from that opinion, it should be kept in mind that the user does not automatically agree to publishing the answers of a poll. Thus, profiling may not include or generate special categories of personal data (Article 9(1) GDPR).

If processing is based on consent, the existence of such consent has to be proven by the controller[518] that the consent given via Alexa is informed, free and unambiguous.

[518] Art. 24(1) GDPR: "[t]o demonstrate that processing is performed in accordance with this Regulation."

Co-funded by the Horizon 2020
Framework Programme of the European Union

13 Conclusions and Recommendations

In the MARCONI project, personal data according to Article 4(1) GDPR and special categories of personal data (Article 9 and 10 GDPR) will be processed (see Chapter 3).

The most relevant justification for the processing of personal data within MARCONI will be consent (Article 6(1)(a) GDPR), performance of a contract (Article 6(1)(b) GDPR), further data made public by the data subjects themselves (Article 6(1)(f) and 9(2)(e) GDPR) or weighting of interests (Article 6(1)(f) GDPR).

Consent may be used for interactive communication within websites (e.g. chatbots, visitor's comments). It can also cover special categories of personal data, subject to explicit consent. Consent must be freely given, specific, informed and unambiguous. Consent can be withdrawn at any time (Article 7 GDPR).

In order to get consent, the user should be guided to a special window (e.g. drop-down) or should be asked questions (e.g. chatbot) offering the possibility to give his consent for the various scenarios of MARCONI. Considering the scientific nature of the project, the purpose limitation can be interpreted in a more flexible manner (Rec. 31 GDPR).

Another ground for justification would be the fulfilment of contractual obligations, e.g. using the MARCONI app. According to Article 6(1)(b) GDPR the processing shall be lawful if it is "necessary for the performance of a contract" to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This ground for justification may be mostly relevant for the MARCONI app providing additional services.

According to Article 6(1)(f) GDPR processing shall be lawful if "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." The main use of this ground for lawful processing will be data made public by the data subject.

Data made public by the data subject (e.g. internet, Facebook, Instagram, Twitter) can be processed subject to weighing of interest and information of the data subject.

So informed consent should necessarily accompany other grounds for justification to ensure comprehensive justification of the intended processing. Therefore it appears to be crucial to the project to establish a privacy policy that ensures information for the data subject and establish a process to gain informed consent.

Privacy by design and default measures should be implemented, in particular pseudonymisation, data minimisation and appropriate technical and organizational measures.

Some classification and clustering of users takes place that may be considered as profiling. If it produces legal or similar effects, an explicit consent should be obtained from the data subject.

For completeness, records of processing activities (Article 30 GDPR) and data security measures (Article 32 GDPR) must be implemented.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Pictures and videos are subject to copyright, right to one's own image and special data protection rules. In using these data, consent of the copyright holder, the pictured person and the data subject must be obtained.

Radio is mostly governed by national law of the Member States. The use of the radio spectrum is determined by rules of the ITU. Radio frequencies are determined by the International Telecommunication Union (ITU) and its ITU Radio Regulations. Audiovisual media services are partly harmonised by the Audiovisual Media Services Directive 2010/13/EU that is in the process of revision.

In case of contractual relations, European international private law has to be respected (in particular Regulation No. 1215/2012, Regulation No. 593/2008 (Rom I) and Regulation No. 864/2007 (Rom II).

Co-funded by the Horizon 2020
Framework Programme of the European Union

Bibliography

Literature

Albers in Wolff/Brink, BeckOK DatenschutzR[23] (2017) DS-GVO Article 6.

AlbrechtJotzo, Das neue DatenschutzR (2017) part 3.

Anderl/Tlapak, Vom Dienstleister zum Auftragsverarbeiter - was ändert sich mit der DSGVO?, ZTR 2017, 59.

Appl in *Wiebe*, Wettbewerbs- und Immaterialgüterrecht[3] (2016) 183.

Bäcker in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 13.

Berdenich, Datenschutz online: Analytics & Tracking-Cookies, Dako 2016/51 (81).

Bergauer in *Knyrim*, Datenschutz-Grundverordnung (GDPR) – das neue Datenschutzrecht in Österreich und der EU (2016).

Bergt, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, 365.

Bessant, The application of Directive 95/46/EC and the Data protection Act 1998 when an individual posts photographs of other individuals online, European Journal of Law and Technology Vol 6 No 2 (2015) 8.

Bisges, Schlumpfbeeren für 3000 Euro – Rechtliche Aspekte von In-App-Verkäufen an Kinder, NJW 2014, 183.

Bräutigam, Das Nutzungsverhältnis bei sozialen Netzwerken - Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten, MMR 2012, 635.

Buchner/Petri in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 5, 6.

Dürager, Outsourcing in die Cloud - Ein (un-)beherrschbares Risiko aus datenschutzrechtlicher Sicht? Ip Competence 18/2017, 36.

Ennöckl, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung (2014).

Ernst in *Paal/Pauly*, DS-GVO[2] (2018) Art. 4, 9.

Esayas, European Journal of Law and Technology Vol 6, No 2 (2015) 8.

Feiler/Forgo, EU-DSGVO (2017).

Feiler/Horn, Umsetzung der DSGVO in der Praxis (2018).

Frenzel in *Paal/Pauly*, DS-GVO[2] (2018) Art. 4, 5, 7, 9.

Fritz, Der Auftragsverarbeiter im Fokus der DS-GVO, Jahrbuch Datenschutzrecht 2017, 9.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Fritz in *Schweighofer/Kummer/Saarenpää/Schafer* (Eds.), Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018), Abgrenzungsschwierigkeiten bei der datenschutzrechtlichen Rollenverteilung nach der DS-GVO, 23.

Gola in *Gola*, DS-GVO (2017) Art. 4.

Ingold in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 28, 30.

Haas in *Schweighofer/Kummer/Saarenpää/Schafer (Eds.),* Data Protection/LegalTech, Proceedings of the 21st International Legal Informatics Symposium - IRIS 2018 (2018), Die Verarbeitung besonderer Kategorien personenbezogener Daten, 67.

Haidinger, Der Weg von personenbezogenen zu anonymen Daten, Dako 2015/34, 56.

Haidinger, Die Rechte auf Löschung, Berichtigung, Einschränkung und Datenübertragbarkeit nach der DSGVO (Teil XI), Dako 2017/34, 56.

Hansen in BeckOK, DS-GVO[23] (2018) Art. 35.

Hennemann in *Paal/Pauly*, DS-GVO[2] (2018) Art. 14.

Herbst in Kühling/Buchner, Datenschutz-Grundverordnung (2017) Art. 17.

Holt/Lampke, Exploring stolen data markets online: products and market forces, Criminal Justice Studies, 23:1, (2010) 33-50.

Hörbe/Hötzendorfer, Privacy-by-Design-Anforderungen für das Federated Identity Management - Eine datenschutzrechtliche und architektonische Betrachtung, Jahrbuch Datenschutzrecht 2014, 305.

Jahnel, Datenschutzrecht (2010).

Jandt in *Kühling/Buchner*, Datenschutz-Grundverordnung (2017) Art. 6, 35.

Koreng/Lachenmann, Formularhandbuch Datenschutzrecht[2] (2018).

Kosinski/Stillwell/Graepelb, Private Traits and Attributes Are Predictable from Digital Records of Human Behavior, PNAS (2013).

Leissler, Intelligentes Spielzeug: Der Datenschutz im Kinderzimmer, ecolex 2017, 99.

Leissler/Wolfbauer, EU-Datenschutz-Grundverordnung – ein Weckruf an die Unternehmen, ecolex 2016, 1117.

Lewisch, Zulässigkeit von Funkzellenauswertungen, JBL 2016.

Lachenmann in *Solmecke/Feldmann/Taeger*, Mobile Apps (2013), Chapter 3.

Mantz in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 32.

Martini, Wie neugierig darf der Staat im Cyberspace sein? Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen (2016), VerwArch 2016, 354.

Martini in *Paal/Pauly*, DS-GVO[2] (2018) Art. 35.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Marzi/Pallwein-Prettner, Datenschutzrecht auf Basis der DS-GVO (2018).

Moser-Knierim, „Facebook-Login" – datenschutzkonformer Einsatz möglich? – Einsatz von Social Plug-ins bei Authentifizierungsdiensten, ZD 2013, 263.

Narayanan/Shmatikov, Robust De-anonymization of Large Sparse Datasets, 2008 IEEE Symposium on Security and Privacy, (2008) 111-125.

Nowak/Januszewski/Hofstätter (eds.), All Human Rights for All – Vienna Manual on Human Rights (2012).

Paal in *Paal/Pauly*, DS-GVO[2] (2018) Art. 2, 12, 13.

Peschel/Schwamberger, Der Vertragspartner beim App-Erwerb, ZIIR 2016, 413.

Peuker in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 17.

Pollirer, Checkliste Datenschutz durch Technikgestaltung und datenschutz-freundliche Voreinstellungen, Dako 2018/27, 43.

Regenhardt in *Sydow*, DS-GVO (2017) Art. 4.

Rücker et al in *Rücker/Kugler(eds.)*, New European General Data Protection Regulation (2018).

Sassenberg/Schwendemann in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 35.

Schantz in *Wolff/Brink*, BeckOK[2] (2017) Art. 5.

Schild in *Wolff/Brink*, BeckOK Datenschutzrecht[23] (2018) DS-GVO Art. 4.

Schmidt-Wudy in BeckOK DatenschutzR[23] (2018) DS-GVO Art. 15.

Schmitz/von Dall'Armi, Datenschutz-Folgenabschätzung – verstehen und anwenden, ZD 2017, 57.

Schulz in *Gola/Schulz,* DS-GVO (2017) Article 6.

Schweiger, Löschen in Backups – Anforderungen und rechtliche Möglichkeiten nach der DSGVO, Dako 2018/7, 10.

Spitzbart/Geuer, Zielgerichtete Werbung für Kunden in sozialen Netzwerken, Dako 2017/21, 37.

Stemmer in BeckOK DatenschutzR, DS-GVO[23] (2017) Art. 7.

Sydow in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 20.

van Rest/Boonstra/Everts/van Rijn/van Paassen, Designing Privacy-by-Design, in *Preneel/Ikonomou*, Privacy Technologies and Policy, APF 2012, LNCS 8319 (2014), 55.

Lewinski in BeckOK DatenschutzR, DS-GVO[22] (2017) Art. 22.

Voigt, Datenschutz bei Google, MMR 2009, 377.

Voigt/von dem Bussche, The EU General Data Protection Regulation (GDPR) (2017).

Co-funded by the Horizon 2020 Framework Programme of the European Union

Ward/Baker, Undefined by Data: A Survey of Big Data Definitions, University of St. Andrews (2013).

Wille in *Rücker/Kugler*, New European General Data Protection Regulation (2018).

Zankl, E-Commerce-Gesetz (2016).

Ziehbarth in *Sydow*, Europäische Datenschutzgrundverordnung (2017) Art. 55.

ECJ – European Court of Justice

ECJ 23 March 2010, C-236/08 to C-238/08 ("Google France") ECLI:EU:C:2010:159.

ECJ, 24 November 2011, C-468/10 and C-469/10 ("ASNEF" and "FECEMD") ECLI:EU:C:2011:777.

ECJ 19 October 2016, C-582/14 ("Breyer") ECLI:EU:C:2016:779.

ECJ 13 May 2014, C-131/12 ("Google Spain und Google") ECLI:EU:C:2014:317.

ECJ 1 October 2015, C-230/14 ("Weltimmo") ECLI:EU:C:2015:639.

ECJ 8 April 2014, C-293/12 and C-594/12 ("Digital Rights Ireland and Seitlinger and Others") ECLI:EU:C:2014:238.

ECJ 14 May 2009, C-180/06 ("Ilsinger"), ECLI:EU:C:2009:303.

ECJ 7 December 2010, C-585/08 and C-144/09 ("Pammer and Alpenhof") ECLI:EU:C:2010:740.

ECJ 28 January 2016, C-375/13 ("Kolassa") ECLI:EU:C:2015:37

ECJ 06 September 2012, C-190/11 ("Mühlleitner") ECLI:EU:C:2012:542.

ECJ 17 October, C-218/12 ("Emrek") ECLI:EU:C:2013:666.

ECJ 23 December 2015, C-297/14 ("Hobohm") ECLI:EU:C:2015:844.

ECJ 3 July 1997, C-269/95 ("Benincasa v Dentalkit") ECLI:EU:C:1997:337.

ECJ 10 September 2009, C-292/08 ("German Graphics Graphische Maschinen") ECLI:EU:C:2009:544.

ECJ 14 March 2013, C-419/11 ("Česká spořitelna") ECLI:EU:C:2013:165.

ECJ 25 January 2018, C-498/16 ("Schrems") ECLI:EU:C:2018:37.

ECJ 19 January 1993, C-89/91 ("Shearson Lehman Hutton v TVB") ECLI:EU:C:1993:15.

ECJ 20 January 2005, C-464/01 („Gruber") ECLI:EU:C:2005:32.

ECJ 16 December 2008, C-73/07 ("Satakunnan Markkinapörssi and Satamedia") ECLI:EU:C:2008:727.

ECJ 6 November 2003, C-101/01 ("Lindqvist") ECLI:EU:C:2003:596.

ECJ 7 May 2009, C-553/07 („Rijkeboer")ECLI:EU:C:2009:293.

Co-funded by the Horizon 2020 Framework Programme of the European Union

ECJ 5 June 2018, C-210/16 („Wirtschaftsakademie Schleswig-Holstein“), ECLI:EU:C:2018:388.

ECHR – European Court of Human Rights

ECHR, von Hannover v. Germany (no. 2), Grand Chamber judgment of 7 February 2012.

German Federal Constitutional Court

German Federal Constitutional Court, BVerfGE 65,1.

German Federal Constitutional Court, 1 BvR 370/07, 1 BvR 595/07.

Article-29-Working Party

WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 WP 251 (2017).

WP29, Guidelines on Consent under Regulation 2016/679 WP 259, first revision (2018).

WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP 248 rev.01 (2018).

WP29, Guidelines on Data Protection Officer WP 243 (2016).

WP29, Opinion 03/2013 on purpose limitation WP 203 (2013).

WP29, Opinion 15/2011 on the definition of consent WP 187 (2011).

WP29, Opinion 10/2004 on more harmonised Information Provisions WP 100 (2004).

WP29, Opinion 04/2012 on Cookie Consent Exemption WP 194, (2012).

Legislation

Charter of Fundamental Rights of the European Union (Charter), OJ C 326, 26.10.2012, 391–407.

Treaty on European Union and the Treaty on the Functioning of the European Union (TEU), Official Journal C 326, 26/10/2012, 1 – 390.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, 1–88.Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

Co-funded by the Horizon 2020 Framework Programme of the European Union

on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995, 31.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, 89–131.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, 37–47.

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive), OJ L 105, 13.4.2006, 54–63.

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, 1–22.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Network and Information Security Directive – NIS-Directive), OJ L 194, 19.7.2016, 1–30.

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact, OJ L 26, 31.1.2018, 48–51.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ L 178, 17.7.2000, 1–16.

Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, (last visited May 08 2018 on: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680063765).

Convention for the protection of individuals with regard to automatic processing of personal data, Strasbourg 28.01.1981, ETS No. 108 (European Data Protection Convention).

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Strasbourg, 08/11/2001, ETS No.181 (Amendment to the European Data Protection Convention).

Co-funded by the Horizon 2020 Framework Programme of the European Union

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013), C(80)58/FINAL, as amended on 11 July 2013 by C(2013) 79.

OECD Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data 1980, C(80)58/FINAL.

International Covenant on Civil and Political Rights, adopted by the United Nations General Assembly on December 16 1966 - resolution 2200A (XXI), which came into force March 23 1976.

Austrian Data Protection Act, BGBl. I Nr. 165/1999 idF BGBl. I Nr. 24/2018.

Federal Copyright Act of Austria (Urheberrechtsgesetz, UrhG).

Federal Copyright Act of Germany (Kunsturhebergesetz, KunstUrhG).

Federal Data Protection Act of Germany (Bundesdatenschutzgesetz, BDSG).

Other

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe, COM(2015) 192 final (Digital Single Market Strategy).

Co-funded by the Horizon 2020 Framework Programme of the European Union