LEGAL ISSUES OF USER ENGAGEMENT WITH INTERACTIVE RADIO STATIONS

Erich Schweighofer / Felix Schmautzer

Professor, University of Vienna, Centre for Computers and Law
Schottenbastei 10-16/2/5, 1010 Wien, AT
Erich.Schweighofer@univie.ac.at; https://rechtsinformatik.univie.ac.at

Researcher, University of Vienna, Centre for Computers and Law
Schottenbastei 10-16/2/5, 1010 Wien, AT
Felix.Schmautzer@univie.ac.at; https://rechtsinformatik.univie.ac.at/en/team/researchers/felix-schmautzer/

Keywords: ***Interactive Radio, Data Protection, Media Law, GDPR, Personalisation***

Abstract: *This contribution addresses the legal questions of interactive radio programs, in particular concerning data protection. We discuss data protection compliance issues regarding personalisation, individual user engagement and the inclusion of social media and communication tools in the context of radio making and broadcasting.*

1. Introduction

Not only radio, but any digital media broadcast strives towards individual user engagement and personalisation of not only advertisements but also content which has been a trend since the 1990s. This holds to be especially true for social network based and context awareness-based recommender systems.[1] Such a system, which enables listeners of hybrid radio to consume a personalized broadcast as well as to interact with a radio station through the means of their favourite platform or chatbots.[2] In this paper we will discuss legal issues, in particular of data protection in the light of the General Data Protection Regulation (GDPR), in particular personalisation and collection of personal data in listener engagement, dealing with aspects of personalised content and social media interaction and monitoring.

2. Interactive Radio

As linear broadcasts tackle the topic of individual user experiences only in a limited manner, new ways of communication have been sought by the industry. Such a platform has been developed through a unified backend which enables a broadcaster to use a managing application for the editorial team and presenter with plugins such as integrating indexing, personalization, interaction and clustering services while emphasizing data protection compliance in the meantime.[3] Personal data may be proposedly collected through three major applications. Users will have the opportunity to engage with a radio station of their choice through a webpage, a smartphone app or a chatbot implementation designed for the platform of their choice, for example, through the Facebook Messenger API.[4] As each of these three applications require to be set up distinctly as they fulfil several disparate purposes, they are going to be evaluated individually.

The following three objectives are central to this process and outline the general concept:

---

1 Lu et al., Recommender system application developments: A survey, Decision Support Systems 2015, 12-32.

2 MARCONI intends to move closer to a fully personalised and interactive user experience by offering the necessary tools to both radio companies and listeners to mutually engage in intensive interactions around live radio and beyond. See the website of project MARCONI, https://www.projectmarconi.eu/ (all Websites last accessed on February 2019).

3 Enabling users to interact through favorite communication channels such as Apps or social media and radio creators to search through automatically clustered sent in content. Employing chatbot services, strengthening innovation capacity.

4 Messenger, https://developers.facebook.com/docs/messenger-platform/getting-started/webhook-setup/.

- Enable the listeners to interact with radio in a personalized way through their preferred (social) channel and remain connected;
- Optimise tools and platforms for the radio editorial team to give them a better overview of interaction in order to engage more and better with their audience;
- Build innovative services and platforms to enable automation of user interaction;
- Through such objectives, multitudes of controllers and processors alike take part in processing operations. Processing activities include the training of neural networks for content recognition, indexing services to create searchable databases, deployment of personalisation services, integration of artist and music databases as well as maintaining user datasets.

Personalisation of services under collaborative filtering but not under recommendation-based systems inherently requires personal data to provide content suited to the individual.[5] As such, preference models, age, gender, social media accounts, content consumption and even client devices deliver important information on how and which content the data subject likes to consume. In mapping the preferences to a user account authenticated by an e-mail address or another UID[6] renders the user, as a natural person, identifiable and by that matter a data subject according to Art. 4 (1) GDPR[7]. As such, the material scope of the GDPR applies to any kinds of such operations until a user profile is being deleted or the data aggregated, therefore constituting a «*disproportionate effort*» in terms of time, cost and manpower to re-identify natural persons, the aforementioned being relative criteria.[8]

3. Grounds of Legitimate Processing

Personal data may be delivered by the data subject but also social media constitutes a major source for input for broadcasting services. Data made available to the public is very relevant for the justification of processing, in particular in scenarios using user generated content not only for the purpose of entertainment, but for news and other journalistic aims. In the following sections, the grounds of processing according to Art. 6 and 9 GDPR will be discussed and set into reference to the questions of user engagement.

3.1. Legitimate Interest

Processing shall be lawful for purposes of legitimate interests of the controller that must be weighed against the interests of the data subject (Art. 6 (1) (f) GDPR). This provision shall be interpreted in harmony with the fundamental freedoms of the European Union (e.g. freedom of press and radio broadcasting).[9] It encompasses economic interests which involves both user interaction as well as news reporting. To further determine this rather abstract provision, Rec. 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.» Art. 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*».[10] To mitigate such negative effects the normative and individual[11] weighing of interests between controller and data subject shall be taken into account.[12] It should therefore be evaluated among the following points:

---

5 Ricci/Rokach/Shapira, in: Ricci/Rokach/Shapira/Kantor (Eds.), Recommender Systems Handbook (2011), p 1-35.

6 Unique Identifier.

7 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 May 2016.

8 ECJ 19. October 2016, C-582/14, *Breyer* Rec. 46.

9 Rec. 4 GDPR.

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

11 ECJ 19 October 2016, C-582/14, *Breyer* Rec. 44.

12 Albrecht/Jotzo, Das neue DatenschutzR (2017), Part 3 point 5.

- Affiliation with the controller;
- if the processing is foreseeable or customary in trade;
- reasonable expectations of the data subject.[13]

As further outlined below, data subjects will expect processing activities only if they actively try to share stories or media content with a station by, for example, using a corresponding hashtag for a radio program.

3.1.1. Media

In the context of (public) media, the right to freedom of expression (as enshrined in Art. 11 of the EU Charter of Fundamental Rights) should be addressed. Art. 85 (1) GDPR reads: «*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.*» Even without an explicit law of Member States the right to freedom of expression has to be taken into account when balancing interests since freedom of expression can amount to a «*legitimate interest pursued by the controller or a third party*».[14] In addition Rec. 153 GDPR, which corresponds to Art. 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.*»[15] When public data is used for the purpose of sharing it for journalistic purposes it is in general justified depending on the national implementation of Art. 85 GDPR. Therefore radio broadcasters shall be allowed to skim public media for the purpose of journalistic tasks.

3.1.2. Publicly Available Data

If a broadcaster wants to know about current trends and events, having a look at trending hashtags on Twitter or using his own for the purpose of user engagement has almost become common practice. Personal data is «made public» if the subject releases data into a public space.[16] As such, the accessibility to an indefinite number of people, e.g. no restrictions on who may be part of a social network, is therefore sufficient.[17] According to Art. 9 (2) (e) GDPR processing of personal data shall not generally be exempted 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. Even if Art. 9 GDPR is applicable only to processing of «special categories of personal data», this clause is still relevant regarding processing of «normal» personal data. One even may argue that the legal basis for processing sensible data allows for an *argumentum a maiore ad minus*.[18]

However, the fact that personal data is publicly available can also be considered when weighing the interests or if it remains unclear if the data subject published his own data. In respect to publicly available data the ECJ ruled that, «*in relation to the balancing which is necessary pursuant to Art. 7(f) of Directive 95/46*[19]*, 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.*»[20] Compared to the Satamedia case, also the processing purposes and the

---

13 ECHR J 22 February 2018, Libert v. France, Nr. 588/13, Rec. 23; ECHR J 5 September 2017, Bărbulescu v. Romania, 61496/08, Rec. 73.

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

15 Rec. 153 GDPR.

16 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.

17 Petri, in: Simitis/Hornung/Spieker, Datenschutzrecht (2018), Art. 9 point 58.

18 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.

19 Equivalent to Art. 6(1)(f) GDPR.

20 ECJ, 24 November 2011 C468/10 and C469/10, ASNEF and FECMD Rec. 44.

means of redistribution shall be taken into account.[21] 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*.»[22]

From a technical point of view, social media as well as web forums usually allow searching and indexing their services either through an API or allow or deny access to their sites through Robots Exclusion Standard Protocol in order to decide if an indexer (or crawler) should have access for his specific purposes. Services like Twitter and Facebook use their own interfaces when it comes to searching through posts and the respective user database. Since the application of «robots.txt» on a website means only a prohibition of indexing by search engines, it does not necessarily imply the objection of a data subject to data processing. According to some opinions, the requirements for processing publicly available data according to Art. 9 (2) (e) GDPR are not being met just by the data subject publishing.[23]

According to the principle of informational freedom, publicly available data shall be used by anyone[24] and, according to Martini, *«no limits*» exist regarding purpose limitation.[25] As Jahnel points out correctly, 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.[26] Such generation of «added value» by, for example analysis of «big data» sets, would therefore conflict with such postulation, not only because the data subject may not reasonably expect such activities. This seems to be the logical conclusion when considering the fact that this additional information cannot be attributed to the original intention of the data subject.

For radio broadcasters and editors however, social media analysis for market impact analysis plays an important role. Schulz does not condone an *argumentum a maiore ad minus* from Art. 9 (2) (e) but Art. 6 (1) (f) GDPR for passive research alone. Furthermore, such processing activities are privileged under Art. 5 (1) (e), 9 (2) (j) and 89 GDPR.[27] Such would yield massive benefits in the weighing of interests.[28] Due to the exception in Art. 89 (4) GDPR commercial purposes of a station would need to rely on the general framework, however, shall still be taken into account. If the processing is not based on the data subject's consent or on a Union or Member State law[29], according to Art. 6(4) GDPR, processing for a purpose other than that for which the personal data have been collected can be justified. The criteria mentioned in Art. 6 (4) GDPR should, however, be considered when weighing the interests. After a weighing of interests and consideration of general principles as outlined in Art. 5 GDPR, this also applies to special categories of personal data.[30]

In general, there is no incompatibility to be found between the publication of information on (public) social media and processing activities of a radio broadcaster and media services for user engagement. Especially

---

21 ECJ, 16 December 2008, C-73/07, *Satakunnan Markkinapörssi and Satamedia,* Rec 60.

22 ECJ, 24 November 2011, C468/10 and C469/10, ASNEF and FECEMD Rec. 45.

23 Kampert, in: Sydow/Bienemann, Europäische Datenschutzgrundverordnung: Handkommentar[2] (2018), Rec. 33.

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

25 Ibidem, 354; also Schulz, in: Gola, Datenschutz-Grundverordnung: VO (EU) 2016/679: Kommentar[2] (2018), Art. 9 Rec. 26.

26 Jahnel, Datenschutzrecht (2010) Points 1/45 ff., 2/19 and 4/25; Same opinion: Kastelitz/Hötzendorfer/Tschohl, in: Knyrim, DatKomm Art 9 DSGVO Rec. 42 (1 October 2018, rdb.at).

27 Schulz, in: Gola, DS-GVO (2017) Art. 6 points 91-94.

28 Austrian implementation see § 2d (6) FOG.

29 Which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Art. 23(1) GDPR.

30 Petri, in: Simitis/Hornung/Spiecker, Datenschutzrecht (2018), Art. 9 point 60.

considering the fact that in common practice, hashtags and trigger words are being used by the stations as well as by the users in order to find and be found.[31]

3.2. Consent

Radio stations see themselves confronted with processing additional information which will neither fall within the framework of weighing of interests, nor the performance of a contract. According to Art. 7 (4) GDPR, the controller has to prove why he needs which personal data for what purpose. However, the delicacy of the consent framework may be demonstrated by a recent ruling of the Berlin Regional Court against Facebook Ireland[32] (Landgericht Berlin) which states that the terms «acknowledgement» and «read and understood» should not be used as they would move the burden of proof to the user.

The literature is divided with regard to the relation between the information being provided according to Art. 13 and 14 GDPR in a «Privacy Policy Statement» and to whether or not these informational provisions should be used as a reference to Art. 4 (11) GDPR («informed»). A violation of Articles 13 or 14 GDPR do not automatically result in an invalid consent.[33] However, they must be clearly separated or at least be highlighted when presented together.[34] Therefore, concerning the minimum requirements for valid consent, several opinions exist.[35] The WP29 guidelines on consent have been partially adopted by legal commentaries[36] but also criticized by the literature (e.g. exclusion of information regarding storage limitation in the agreement itself[37] or the idea of only including processing purposes as well as notice if and with whom personal data might be shared[38]):

For a consent, economic aspects should be taken into account. How much information may a station be able to present on e.g. a mobile platform? A viable configuration shall therefore be the minimum information such as

- personal data in question,
- processing purpose(s),
- the identity of the controller or joint controllers

to be provided in addition to the information according to Art. 7 (3) GDPR with a general referral to the respective privacy policy in form of a(n) (embedded) link according to the WP29 document («*integrated approach*»).[39]

Concerning storage limitation, the consent agreement does not impose a particular threat to the fundamental rights of the data subject as his right to revoke the processing activity does not depend on how long personal data is saved by the controller. A link to the data protection statement shall therefore suffice. Most controllers will employ processors. As media services use a multitude of processing services and share data across networks informing third parties about deletion requests according to Art. 17 (2) GDPR becomes very relevant. This is not to say that the third party, being a controller himself, does not have a legitimate basis to process said

---

31 Expectations: Art. 5 (1) (a) GDPR.

32 LG Berlin 16 O 341/15.

33 Wolff, in: Schantz/Wolff, Neues Datenschutzrecht, point 523.

34 Gola, in: Gola, DS-GVO, Art. 7 point 44.

35 Literature example of most to least information to be provided: wp259, 19; Ernst, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, 110 (113); Voigt/von dem Bussche, The EU General Data Protection Regulation (GDPR) (2017), 96.

36 Ernst, in: Paal/Pauly, DS-GVO^2 (2018), Art 4 point 83; Ernst, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, 110 (113).

37 Buchner/Kühling, in: Kühling/Buchner, DS-GVO^2, Art 7 point 59.

38 Schild, in: BeckOK DatenschutzR^{25} (2018), Art 4 point 129; Voigt/von dem Bussche, The EU General Data Protection Regulation (GDPR) (2017), 96.

39 wp259, 15.

personal data. Only a «best effort» to inform is required.[40] In the case of joint controllers, according to Art. 26 (1) third sentence GDPR, a contact point for data subjects may be designated.[41] Rec. 43 GDPR is referencing to Directive 93/13/EEC.[42] Austrian rulings on such consumer contracts have been interpreting «factual knowledge in a specific case» quite «strictly».[43] Therefore, just informing about «third parties» in general is not sufficient.[44]

Once consent has been revoked stations see themselves confronted with deletion. Overlap between legal basis of Art. 6 (1) GDPR is largely possible with constraint regarding consent: «In other words, the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent.»[45] Therefore, «*if a controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent*.»[46] The commentary literature is unanimous regarding the interaction of Art. 6 (1) (a) GDPR and other legal basis in stating that «at least one» must be fulfilled, therefore enabling consent to be taken as a first choice regardless of other grounds of processing that might have taken its place.[47] Whereas *Buchner/Petri* argue that, concerning public institutions, an illusion of choice might be suggested to the data subject, the informational provisions of Art. 12 seq. GDPR still apply to the controller and suggest no detriment to the interests of the data subject; furthermore, the lawmaker did not intend a suspensory effect.[48]

Concerning the use of chatbots and alternative means of automated communication another problem arises for a radio station: «*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1* [of Art. 5] *(‹accountability›)*.» This framework guarantees a degree of transparency to the data subject and ensures that such voluntary act is being recorded properly, independent of the text of the notion of consent itself.[49] This implies that such demonstration should be sufficient to show that the intended legal basis indeed has been consent.[50] The modality of such demonstration has not been specified by Art. 7 GDPR. As implicit consent is possible within the framework of the GDPR[51] the literature argues, that such will be a valid basis[52] alongside Art. 6 (1) (c) as processing to comply with a legal obligation to save data for demonstration.[53] This in understanding that according to Art. 5 (1) (b) GDPR such purpose is sufficiently specified.[54] Fundamental questions arise if a system will only collect an extremely limited amount of information rendering identification of data subjects hard and costly, being in no relation to the service provided:

- What data will be required to comply with Art. 7 (1) GDPR to sufficiently demonstrate consent?
- Will the data subject have to be identified?

---

40 Paal, in: Paal/Pauly, DS-GVO^2 (2018), Art. 17 point 32.

41 The Privacy Policy shall contain more information concerning the respective roles and relationships: Rec. 58 GDPR; Spoerr, in: BeckOK, DS-GVO^{25} (2018), Art. 26 point 35.

42 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L 95, 21.4.1993, p. 29-34.

43 RIS-JUSTIZ, RS 0115216.

44 Kastelitz/Hötzendorfer/Tschohl, in: Knyrim, DatKomm (2018), Art 6 point 30.

45 WP29, Guidelines on Consent under Regulation 2016/679 wp259 (rev.01) (2018), 23.

46 Ibidem.

47 Buchner/Petri, in: Kühling/Buchner, DS-GVO^2, Art. 6 point 22; Albers/Veit, in: BeckOK DS-GVO^{24} Art. 6 point 27.

48 Albers/Veit, in: BeckOK DS-GVO^{24} Art. 6 point 27; Schulz, in: Gola, DS-GVO (2017) Art. 6 point 11; Art. 17 (1) (b) GDPR.

49 Frenzel, in: Paal/Pauly^2, DS-GVO Art 7 point 6.

50 Frenzel, in: Q, DS-GVO Art 7 point 7.

51 Stemmer, in: BeckOK DatenschutzR^{24} DS-GVO Art. 7 point 81-82.

52 Ingold, in: Sydow, DS-GVO, Art 7 point 53.

53 Frenzel, in: Paal/Pauly^2, DS-GVO Art 7 point 9.

54 Rossnagel/Nebel/Richter, Was bleibt vom europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455 (458).

– Is the processor in need of gathering more identifying data than needed for the performance of his service and his individual purposes?

To answer the first question concerning the threshold of being able to identify the data subject in recording and storing his notion of consent it is imperative to consider the operations of the controller and the context, the scope and the expectations of the data subject regarding the consent itself. The bare minimum of stored information should therefore consist of:

– Which relationship does Art. 7 (1) enter to with Art. 11 GDPR?
– The processing the subject consented to;
– An identifying object such as IP, e-mail or full name of the subject;
– An integer value as timestamp.

The literature suggests that, as the consent should be able to be proven by the controller as long as the respective legal basis lasts, only an e-mail address confirmed of being under control of the data subject should be used (double-opt-in-procedure).[55] However, in regards to question two, the principle of data minimisation says otherwise. The WP29 argues, that showing only «a link» to the processing should be of sufficient nature[56] while the previously cited literature at least acknowledges that certain evidence of the identity of a data subject will be challenging to provide in online environments.[57] This wording allows the deduction that the data subject does not necessarily have to be identified to give consent for the reasons of mail addresses not necessarily stating a clear name, leaving the data subjected merely identifiable. Another point *pro* can be found in Art. 12 (6) GDPR allowing the controller to request additional information of the data subject to confirm his identity. *Stemmer* also remarks, that electronically checking a box before using a service as a technical precondition will not be sufficient to demonstrate consent.[58] He also notes that an «electronic protocol» is a viable option of documentation.[59] Art. 11 GDPR says that a controller should not be held responsible to collect additional data not required for the performance of his service only to comply with the GDPR itself. The *telos* can be elucidated in two points being that the controller should not be obliged to identify every subject using a potentially not identifying service therefore protecting the controller from undue cost of identification and protecting the basic human rights of the data subject.[60] Should a controller be in need to collect more data about a subject just to demonstrate a compliant and therefore valid notion of consent, Art. 11 (1) as well as Art. 5 (1) (c) GDPR, the general principle of data minimisation, may be violated.

This leads to the conclusion that a controller shall only be held responsible to demonstrate a notion of consent with data of a higher level of identification if he himself is already collecting it. Web services analysing user behaviour and sharing tracking information with third parties should therefore not store a (dynamic) IP and a timestamp but the tracking ID itself as well as cookies and metadata from browser fingerprinting methods which require consent according to Art. 5 2002/58/EC.[61] This as such storage would prove to be more concise than an additional IP address and would not violate the principle of Art. 5 (1) (c) GDPR as the data in question to demonstrate consent is being collected either way by the controller.

---

55 Frenzel, in: Paal/Pauly, DS-GVO[2], Art 7 point 6; Plath, in: Plath, DS-GVO, Art 7 point 4; Schulz, in: Gola, DS-GVO, Art 7 point 63; Dienst, in: Rücker/Kugler, New European General Data Protection Regulation (2018), 99.

56 Art. 29 Working Party, WP259, 20.

57 Dienst, in: Rücker/Kugler, New European General Data Protection Regulation (2018), 99.

58 Stemmer, in: BeckOK DatenschutzR[24] DS-GVO Art. 7 point 88.

59 Ibidem.

60 Wolff, in: BeckOK DatenschutzR[24] DS-GVO Art. 11 point 8.

61 Wiebe, Datenschutz in Zeit von Web 2.0 und BIG DATA – dem Untergang geweiht oder auf dem Weg zum Immaterialgüterrecht?, ZIR 2014, 35 (42); Art. 5, 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.

3.3. Performance of a Contract

The service radio stations are providing consists in rending individual engagement with subjects possible by automated means making it easier to either share content and stories with editors or receive information and recommendations about the program and even personalised content. The literature remains relatively silent concerning the definition of «contract» which, of course, shall be interpreted autonomously according to union law. This imposes significant concern for a processing party if it remains unclear whether or not another lawful basis can be applied as a subsidy as denied by the WP29 in the initial publication of WP259.[62] This interpretation has been highly questionable as the verbatim expression of the regulation, «*no other legal ground for the processing*»[63] and «*at least one of the following* [legal basis] *applies*»[64], points in the opposite direction. However, as outlined above, Art. 5 (1) (a) GDPR may be violated concerning the application of other legal basis as a subsidy for consent. According to the E-Commerce-Directive,[65] a contract is a legal transaction or obligation similar to a legal transaction.[66] A quasicontractual relationship can therefore be designated as a contract if they are based on a voluntary decision of the data subject.[67] Quasi-contractual relations on a goodwill basis are seen as being included by Albers[68] as well as Buchner/Petri[69] while Schulz[70] and Frenzel[71] uphold a different opinion as free services shall not be included, as the term «*enter* […] *into a contract*» shall be interpreted strictly. According to the latter, unilateral contracts may be also included (e.g. «Auslobung» in Germany).[72] 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.[73] This leads to a situation where users «pay» for a service with personal data. However, in the case of the aforementioned purposes, users receive the service of easily obtaining program information and personalised content or receive a chance to broadcasted live while at the same time editors may benefit by creating additional content for a radio program out of submitted media and stories.

3.3.1. Mobile Applications

Most mobile applications are being provided 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[74] 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.[75] Following the opinion of Lachenmann, the Apple App-Store would be the contracting partner, on the contrary to Google Play. Regardless of the conformity of

62 WP29, Guidelines on Consent under Regulation 2016/679 (2017), WP 259, 22.
63 Art. 17 (1) (b) GDPR.
64 Art. 6 (1) GDPR.
65 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 July 2000, 1-16.
66 Albers/Veit, in: BeckOK DatenschutzR[23] (2017) DS-GVO Art. 6 Point 31.
67 Albers/Veit, in: BeckOK DatenschutzR[23] (2017) DS-GVO Art. 6 Point 32.
68 Albers/Veit, in: BeckOK DatenschutzR[23] (2017) DS-GVO Art. 6 Point 32.
69 Buchner/Petri, in: Kühling/Buchner, Datenschutz-Grundverordnung (2017) Art. 6 point 27-29.
70 Schulz, in: Gola, DS-GVO (2017) Art. 6 Point 31.
71 Frenzel, in: Paal/Pauly, DS-GVO[2] (2018) Art. 6 Point 13.
72 Schulz, in: Gola, DS-GVO (2017) Art. 6 point 27; dissenting: Buchner/Petri, in: Kühling/Buchner, Datenschutz-Grundverordnung (2017) Art. 6 point 28.
73 Buchner/Petri, in: Kühling/Buchner, Datenschutz-Grundverordnung (2017) Art. 6 point 59; Zankl, E-Commerce-Gesetz (2016) § 3 point 63.
74 Lachenmann, in: Solmecke/Feldmann/Taeger, Mobile Apps (2013), Chapter 3, point 339.
75 Bisges, Schlumpfbeeren für 3000 Euro – Rechtliche Aspekte von In-App-Verkäufen an Kinder, NJW 2014, 183.

such statement to domestic laws and consumer provisions, terms of service shall be presented and agreed to by the subject, designating the user and the service provider (radio station) as parties.[76]

3.3.2. Websites

Some stations allow users to access an embedded chat interface. A contract requires affirmative or at least conclusive action by one party; this shall be a declaration of intention. However, no affirmative action will be required on the user side. The subject is able to access the feature by simply entering and sending text. However, the user is 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. Therefore, no personal data should be processed under the legal basis of performance of a contract. 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. Else, as outlined above, legitimate interest shall be an alternative.

4. Information Provisions

Especially regarding social media monitoring, several questions regarding to Art. 14 GDPR have to be dealt with. 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»[77]) as long as they carry personal data.[78] This can either happen through the privacy policy statement as outlined above or directly through a banner. According to the WP29, cookies must conform to two criteria[79] in being either strictly necessary for communications or being requested by the user and required to perform a service of the information society. Cookies from social plugins such as the Facebook login will not match the first criterion if the user is not already logged in.[80] The user is therefore required to opt in beforehand. As it is impossible to inform a data subject using the designated hashtag of a radio program that invites users to share content via Twitter, the provision of information would involve a disproportionate effort. It shall be considered to therefore include links in a stations social media profile pointing to data protection statements as a subsidiary measure.

4.1. Social Media

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.[81] 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.[82] 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.[83] Wille suggest a «*double-click solution*» in order to gain the user's consent.[84] This can be achieved by letting users enable social plugins themselves or

[76] Peschel/Schwamberger, Der Vertragspartner beim App-Erwerb, ZIIR 2016, 413.
[77] Art. 5(3), Directive 2002/58/EC.
[78] Christoph Berdenich, Datenschutz online: Analytics & Tracking-Cookies, Dako 2016/51 (81).
[79] WP29, Opinion 04/2012 on Cookie Consent Exemption, 00879/12/ENWP 194, 2-4 (2012).
[80] WP29, Opinion 04/2012 on Cookie Consent Exemption, 9 (2012).
[81] Oberlandesgericht Düsseldorf: EuGH-Vorlage zur datenschutzrechtlichen Verantwortlichkeit eines Internetanbieters für Einbindung eines Social Plugin – Like-Button, GRUR Int. 2017, 466 (467).
[82] Wille, in: Rücker/Kugler, New European General Data Protection Regulation (2018), 277.
[83] ECJ 5 June 2018, C210/16 Schleswig-Holstein, Rec. 33-37.
[84] Wille, in: Rücker/Kugler, New European General Data Protection Regulation (2018), 277.

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.

4.2. Profiling and Automated Decision-making

Online personalisation and user privacy need to go hand in hand as personal attributes and preferences are often strongly correlated and therefore of high value in big data industries.[85] According to Art. 13 (2) (f) GDPR, such additional information would include the information about the existence of automated decision-making, including profiling, referred to in Art. 22 (1) and (4) GDPR. The former 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. Does the selection for a prize game already fall under the scope of «legal effects»? Looking at Rec. 71 GDPR, it might appear that only negative and restricting legal consequences fall under the scope. With regards to the wording of Art. 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. While every translation of the text of the directive is equally valid and is therefore of the same importance as the English version, there is still some discussion in the literature regarding the necessity of said negative impact since the GDPR does not define the threshold of «similarly significant […] effects». The WP29 states, however: «*similarly significant effects may be positive or negative*.»[86] Ultimately, this depends on how the radio station designs its systems. The general consequences should therefore be balanced with considerations to the precision of the methods, excluding trivial operations.

5. Conclusion

Radio stations face several hurdles if they want to efficiently engage an audience as large as possible and enabling personalisation features whilst supporting many platforms of choice to communicate such as Twitter.

Radio broadcasters shall be allowed to skim public media for the purpose of journalistic tasks. Processing of public data, regardless of the application of either Art. 6 or 9 GDPR, should not be detached from the original purpose of publishing. For processing additional information which will neither fall within the framework of weighing of interests, consent from the data subject is the obvious choice. However, the provisions concerning consent, identification and withdrawal of consent must be observed. Further, information provisions must be complied with.

As a large quantity of users engage with a radio station, it is of importance to consider the special rules on automatic processing of data. In most cases, the processing by radio stations will not produce legal effects.

6. Acknowledgement

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 761802, MARCONI.

[85] Kosinski/Stillwell/Graepelb, Private Traits and Attributes Are Predictable from Digital Records of Human Behavior, PNAS (2013).

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