Push Notifications under E-Privacy Law: A Review and Outlook on the Interplay between Data Protection Law, E-Privacy Law and other Legal Acts

by **Tristan Radtke** *

Abstract: Push notifications are widely used to inform users directly about messages, news and offers. Although the opt-in mechanisms implemented by all providers of push notifications might suggest straightforward compliance with e-privacy law, this popular phenomenon is a good example to discuss the current and future challenges under European e-privacy and data protection law. The use of push notifications raises intriguing legal questions under the e-privacy directive, the General Data Protection Regulation (EU) 2016/679 (GDPR) and the law of unfair commercial practices. The focus here is on questions related to the interaction of these different legal acts, the requirements for legal bases as well as the relationship between a consent requirement and the push notification permissions granted through system permission prompts on the devices. A closer look is necessary for the requirements of the e-privacy Directive with regard to the storage of information on the device, unsolicited communication and the question of whether push notifications constitute electronic mail or other forms of communication. Against this background, this article explores the complex legal landscape surrounding push notifications, addresses these legal challenges, and provides standards for push notifications using different scenarios. Finally, the article concludes with a discussion on how the current legal framework handles such an important phenomenon and considers what to expect from a potential e-privacy Regulation in this regard.

Keywords: Push Notifications; E-Privacy Directive; Consent Requirement, Data Protection Law

Recommended citation: Tristan Radtke, Push Notifications under E-Privacy Law: A Review and Outlook on the Interplay between Data Protection Law, E-Privacy Law and other Legal Acts, 16 (2025) JIPITEC 107 para 1

A. Introduction

1 Push notifications are brief, alert-style messages sent by app providers, including websites, to user devices such as smartphones or personal computers. These notifications are designed to inform users about updates and reminders, provide promotional content, or prompt users to an action, even when the app is not actively in use. Push notifications address individual users directly by delivering content to their devices. The combination of these phenomena raises challenges under data protection law and the law of unfair commercial practices.

I. Data flows

2 The specifics of the data flow vary according to the device and the operating system in use. However, the data flow involved in the delivery of a push notification can be summarized as follows:[1] The app of

* Dr. Tristan Radtke, LL.M. (NYU) is a research assistant (Akademischer Rat a.Z.) at the Chair for Law and Regulation of the Digital Transformation (Prof. Dr. Boris P. Paal, M.Jur. (Oxford)), TU Munich – School of Social Sciences and Technology, Department of Governance. The author would like to thank Prof. Dr. Boris P. Paal, M.Jur. (Oxford) for his valuable comments on a previous version of this article and fruitful discussions on this topic.

1 See 'Setting up a remote notification server' (*Apple*

the app provider is installed and launched on the device by the users. Once the app is launched, the app provider can ask users to allow push notifications through an operating system permission prompt. Users can change the format of the push notification in the operating system settings, but not the content or frequency of the notifications.

3 The launch of the application initiates the registration process with a push notification provider, which generates a unique token for the specific application on the particular device. The push notification provider depends on the device and its operating system. For iOS and other Apple devices, it is the Apple Push Notification (APN)[2] service, for Android devices, it is often Firebase Cloud Messaging,[3] for web push notifications in Firefox, it is the Mozilla Web Push[4] service. However, there might be additional service providers in the middle between the app provider and the push notification provider in order to facilitate the process and provide a framework for sending push notifications on different platforms.

4 Once the device token has been generated, it is the responsibility of the app provider to transmit this token to its own servers and link it with other identifiers (e.g., with the user's account information).

5 When the app provider wishes to issue a push notification via their servers, the server of the app provider requests the push notification provider to initiate the process by submitting the message, the modalities and the app's device token. Such modalities may include information about the expiration of the notification after a certain period of time during which the device was offline and the notification could not be delivered (e.g., 30 days).[5] Furthermore, the app provider could specify the priority of a notification.[6]

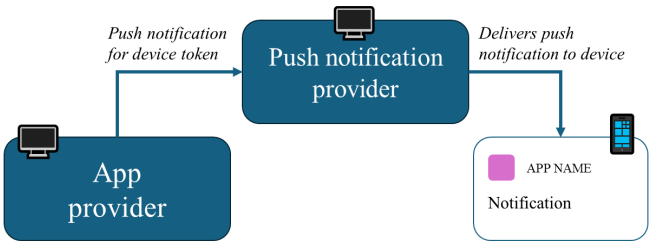

Figure 1: Process of initiating a push notification from the server of the app provider to the user's device (simplified)

6 This analysis focuses on the initiation of the push notification process from the perspective of the app provider. As the push notification provider is only responsible for delivering the content *provided by the app provider*, the role and obligations of the latter under applicable law will not be considered in this article.

II. Analysis based on three Scenarios

7 To illustrate the lawfulness of push notifications, this article focuses on three specific scenarios in the context of connected cars:

(1) An app is connected to a vehicle and can be used to view certain metrics about the vehicle's condition. The push notification informs the user that a new software update for the software of the vehicle is available.

(2) As in Scenario 1, but the push notification informs the user of an available update for the mobile app.

(3) As in Scenario 1, but the push notification contains promotional advertising on a discount available for a vehicle software upgrade.

8 These Scenarios will be used to analyze the legal challenges posed by device access under the e-privacy Directive (see below B. I.), communication with the user under the e-privacy Directive (see below B. II.) and the processing of personal data in general under the GDPR (C.). Further requirements arising from the UCP and ecommerce Directive will then be addressed (see below D.).

Developer) <https://developer.apple.com/documentation/usernotifications/setting-up-a-remote-notification-server> accessed 15 November 2024; 'Registering your app with APNs' (*Apple Developer*) <https://developer.apple.com/documentation/usernotifications/registering-your-app-with-apns> accessed 15 November 2024.

2 'Registering your app with APNs' (*Apple Developer*) <https://developer.apple.com/documentation/usernotifications/registering-your-app-with-apns> accessed 15 November 2024.

3 'Firebase Cloud Messaging' (*Google Firebase*), <https://firebase.google.com/docs/cloud-messaging> accessed 15 November 2024.

4 'Web push notifications in Firefox' (*Firefox Support*, 9 February 2023) <https://support.mozilla.org/en-US/kb/push-notifications-firefox> accessed 15 November 2024.

5 'Sending notification requests to APNs' (*Apple Developer*) <https://developer.apple.com/documentation/usernotifications/sending-notification-requests-to-apns> accessed 15 November 2024.

6 *Apple Developer* (n 5).

B. E-Privacy Directive

9 The e-privacy Directive 2002/58/EC, as amended by Directive 2009/136/EC, addresses primarily privacy concerns with respect to electronic communication services and "particularise[s] and complement[s]" the GDPR insofar (cf. art. 1(2) e-privacy Directive, art. 94(2) GDPR). In light of the stipulations set forth in art. 95 of the GDPR, which establishes that the provisions of the e-privacy Directive prevail over the general GDPR,[7] this analysis will initially focus on the e-privacy Directive and subsequently address the GDPR requirements.

10 However, despite the e-privacy Directive being *lex specialis* to the GDPR, the e-privacy Directive takes a slightly different approach. As the name of the Directive suggests, the e-privacy Directive is primarily concerned with the protection of privacy with regard to devices and the confidentiality of communications (arts. 7, 8 EU Charter of Fundamental Rights, hereinafter Charter), rather than merely data protection (art. 8 Charter).[8] The here relevant arts. 5(3) and 13 e-privacy Directive are primarily concerned with the protection of the private sphere, including users' devices in the context of electronic communication.[9] The national provisions implementing the e-privacy Directive have to be interpreted in accordance with the Directive.

11 In the near future, the e-privacy Regulation, which has not yet to be agreed upon,[10] could replace the e-privacy Directive. Although the precise details of the successor provision to art. 5(3) remain uncertain, there are indications that the e-privacy Regulation will adopt a provision similar to art. 13, potentially with only a few modifications.[11]

I. Access to the User's Device under Art. 5(3) E-Privacy Directive

1. Scope of Art. 5(3) E-Privacy Directive

12 According to art. 5(3) e-privacy Directive, the storage of information and the access to information on the terminal equipment of the user (e.g., a smartphone) is subject to limited specific legal bases: (1) the consent of the user, (2) the necessity for transmissions or (3) the necessity for the provision of a requested service. This applies to information on any type of device medium including the RAM for temporary storage.[12] The ECJ places emphasis on the language "information" and interprets art. 5(3) e-privacy Directive broadly to cover both personal and non-personal data.[13]

13 Delivering a push notification involves temporarily storing its content on the device, which constitutes storing information on the user's terminal equipment under art. 5(3) of the e-privacy Directive. As with

7 Recital 173 GDPR; Christoph Werkmeister in Frenz Jürgen Säcker and Torsten Körber (eds), *TK – TTDSG* (4th edn, dfv 2023), s 25 TTDSG para 40; Daniel A Pauly in Boris P Paal and Daniel A Pauly (eds), *DS-GVO BDSG* (3rd edn, CH Beck 2021), art. 95 DS-GVO para 2.

8 cf. art. 1(1), recital 12 e-privacy Directive; Achim Klabunde and Martin Selmayr in Eugen Ehmann and Martin Selmayr, *DS-GVO* (3rd edn, CH Beck 2024), art. 95 DS-GVO para 10; Alexander Golland in Jürgen Taeger and Detlev Gabel (eds), *DSGVO – BDSG – TTDSG* (4th edn, dfv 2022), art. 95 DSGVO para 9; Vagelis Papakonstantinou and Paul De Hert in Indra Spiecker gen. Döhmann and others (eds), *General Data Protection Regulation* (CH Beck and Nomos 2023), art. 95 para 2. On the terms privacy and data protection Lee A Bygrave, 'Privacy and Data Protection in an International Perspective' (2010) 56 Scandinavian Stud L 165.

9 cf. Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH*, Opinion of AG Szpunar, ECLI:EU:C:2019:246, para 107; recital 24 e-privacy Directive; EDPB, 'Opinion 5/2019 on the interplay between the e-privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities' (12 March 2019), paras 25-28; Werkmeister (n 7) 1; Carlo Piltz, 'Das neue TTDSG aus Sicht der Telemedien' [2021] CR 555, 560; Hanloser, 'Telekommunikation-Telemedien-Datenschutz-Gesetz' [2021] ZD 121, 121.

10 The e-privacy Regulation was originally intended to come into force at the same time as the GDPR in 2018. Due to different views on the proposal within the EU institutions, probably also and especially with regard to tracking, no agreement has been reached to date and the proposal has just been withdrawn. For an overview, see e.g. Martin Selmayr and Eugen Ehmann in Ehmann and Selmayr (n 8) Introduction 130.

11 See the draft of the e-privacy Regulation, Council of the European Union, '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)' 6087/21 (10 February 2021); providing an overview Christina Etteldorf, 'A New Wind in the Sails of the EU e-privacy-Regulation or Hot Air Only? On an Updated Input from the Council of the EU under German Presidency' (2020) 6 Eur Data Prot L Rev 567; Louisa Specht in Louisa Specht and Reto Mantz (eds), *Handbuch Europäisches und deutsches Datenschutzrecht* (CH Beck 2019), s 9 para 13.

12 EDPB, 'Guidelines 2/2023 on Technical Scope of Art. 5(3) of e-privacy Directive' (14 November 2023), para 37.

13 Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH* (ECJ, 1 October 2019), ECLI:EU:C:2019:801, paras 69-70.

cookies, the fact that they are automatically deleted after a certain period of time does not preclude the presumption that information is being "stored".[14] It may be argued against an interpretation of art. 5(3) e-privacy Directive, which covers temporary storage of a displayed information, that such a broad interpretation would cover any website that is stored on a user's device in order to display its content. This was probably not the intention of the legislator. However, storing such information initiated directly by the user does not constitute provider-initiated storage as required under art. 5(3) of the e-privacy Directive.

14 Furthermore, information originating from the device such as the device token or the version of the installed app, could be accessed in order to deliver a push notification, which would also be considered access to information on the device.[15]

2. Exceptions from Consent Requirement

15 Art. 5(3) e-privacy Directive provides two exceptions to the principle that access to or the storage of information on the user's terminal equipment is prohibited. Where these exceptions apply, providers are not required to obtain the user's consent.

a.) Necessity for Transmission of a Communication

16 The first exception permits storage or access if it is necessary "for the sole purpose of carrying out the transmission of a communication over an electronic communications network" (art. 5(3)(2) (alt. 1) e-privacy Directive).

17 This is the case for device identifiers, without which communication could not be delivered.[16] If the service provider were to access the device token on the device before delivering a particular push notification in order to enable the delivery of the push notification at hand, that access would be covered by the exception.

18 However, it is not considered necessary to access the device to *store* the content of the push notification on the device in order to carry out the *transmission*. Art. 5(3)(2)(alt. 1) e-privacy Directive must be read restrictively in order to leave some room for the exception of the service explicitly requested by the user (alt. 2, as discussed under b.).[17] If the storage of any information were covered by the exception for transmission, there would be no need for the exception for the service requested by the user or for a consent requirement.

19 In all three Scenarios, the access to the identifiers stored on the device is covered by the exception laid down in art. 5(3)(2)(alt. 1) e-privacy Directive. For the storage of the content of the push notification, the provider has to rely on another exception.

b.) Information Society Service Explicitly Requested by the User

20 Second, any storage or access "strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service" is permitted (art. 5(3)(2)(alt. 2) e-privacy Directive). Information society services are defined in art. 1(1)(b) Directive (EU) 2015/1535 as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". This covers any app-related services and push notifications, regardless of whether they are actually provided for remuneration.[18] Since an *explicit* request for each communication is not required for a service to be considered an information society service, the installation of an app may be generally sufficient for the purposes of the definition with respect to future push notifications.[19]

21 Any interpretation of art. 5(3)(2)(alt. 2) e-privacy Directive has to give sufficient consideration to the elements "strictly necessary", "explicitly requested" and the determination of the respect service and its scope.[20] The test for the "strictly necessary" prong is whether the specific service could not be provided at all without the storage of or access to the information.[21] The element of an explicit request of the service is met if the user has the reasonable expectation that information will be stored or accessed on his device, if this part of the service is used and thus "requested".[22] In order not to undermine the general consent requirement under art. 5(3)(1) e-privacy Directive, the part of the

14 cf. *Planet49 GmbH* (n 13) 75.

15 cf. EDPB (n 12) 55.

16 WP29, 'Opinion 04/2012 on Cookie Consent Exemption' (7 June 2012), 3.

17 cf. WP29 (n 16) 2-3.

18 Case C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* (ECJ, 15 September 2016), ECLI:EU:C:2016:689, paras 41-42; Stefan Ernst in Paal and Pauly (n 7), art. 4 DS-GVO para 143.

19 cf. Ernst (n 18) 147.

20 cf. WP29 (n 16) 5.

21 Recital 66 Directive 2009/136/EC.

22 Adrian Schneider in Simon Assion (ed), *TTDSG* (1st edn, Nomos 2022), s 25 para 40; cf. WP29 (n 16) 8; recital 47 GDPR.

service must be considered granularly in terms of its function.

22 In the first and second Scenario, there may be some doubt as to whether the user explicitly requested the specific update information service. While it can be assumed that the user has requested the vehicle connection service, the user has not explicitly requested to be informed via push notifications on available updates. However, there is a closer link to the provision of the vehicle connection service in the case of essential updates, where the use of the service would be disrupted if not installed on time. In such cases, the sending of a push notification is covered by art. 5(3)(2)(alt. 2) e-privacy Directive.

23 In addition, the permission given through the system prompt can be considered as a request for the respective service. By authorizing push notifications for the app, the user expects to receive such push notifications. The question of whether the respective notifications can still be considered "explicitly requested" in accordance with the user's legitimate expectation depends on the scope of the notification's purposes pursued with the app and the frequency with which notifications are sent. If, as in Scenarios 1 and 2, a vehicle connectivity app only sends relevant connectivity notifications, these are still covered by the explicit request. However, supplementary advertising messages as in Scenario 3 may be assessed differently.

24 In Scenario 3, the small-scale analysis requires that the information on discounts for additional vehicle features be considered as a separate service or as a separate part of the same service. The discount notification promotes a service that is subject to a separate contract. The information on the option to conclude another contract is not expected by the user when the app is installed and the vehicle connection features are activated or when the user gives permission to receive push notifications in general.

3. Consent Given by the User

25 In the absence of any applicable exceptions, the service provider may rely on the user's freely given and informed consent (art. 5(3)(2), recital 17 e-privacy Directive).[23] The consent required under the e-privacy Directive generally adheres to the same principles as those set out in the GDPR.[24] The operating system's permission prompt for allowing push notifications could potentially function as a consent prompt, which will be assessed below.

23 *Planet49 GmbH* (n 13) 50-65.

24 *Planet49 GmbH* (n 13) 60 et seqq.

a.) Standards in Comparison to the GDPR

26 Art. 5(3)(2) e-privacy Directive requires that the user "has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing". This could be interpreted as adopting the consent requirements as provided for under the Data Protection Directive 95/46/EC and, nowadays, the GDPR (art. 94(2)(1) GDPR) without any modifications. However, an alternative interpretation of the language in art. 5(3)(2) e-privacy Directive could be that it refers only to the general *information* requirements of processing (e.g., arts. 4(11), 13-14 GDPR).

27 The different interpretations are relevant with regard to the information about the right to withdraw the consent (art. 7(3)(3) GDPR). If the reference is limited to specific information and does not encompass the information on the right to withdraw the consent under art. 7(3)(3) GDPR, the requirements for the consent could be met more easily by the system permission prompts (see below b.). Nevertheless, several aspects indicate that the reference includes the information on the right to withdrawal under the GDPR: the language employed in art. 7(3)(3) GDPR ("inter alia") as well as the interest of the user in withdrawing the consent and being informed about it and the need for a unified standard under GDPR and e-privacy Directive, which can seamlessly interlock in their application.[25]

28 Accordingly, this consent is subject to the same standards set out in the GDPR, including information on the right of withdrawal.

b.) Operating System's Permission Prompt

29 The push notification permission prompt triggered by the app provider as in Figure 2 and Figure 3 constitutes a valid consent if the GDPR requirements are met. According to art. 6(1)(a) GDPR, the controller is not required to obtain the consent directly; rather, any party, including push notification or app store

25 Stefan Hanloser in Sibylle Gierschmann and Ulrich Baumgartner (eds), *TTDSG* (1st edn, CH Beck 2023), s 25 TTDSG para 79; Peter Schmitz in Martin Geppert and Raimund Schütz (eds), *Beck'scher Kommentar zum TTDSG* (5st edn, CH Beck 2023), s 25 TTDSG para 46; LfD Niedersachsen, 'Handreichung: Datenschutzkonforme Einwilligung auf Webseiten' (November 2020), p 3 <https://lfd.niedersachsen.de/startseite/themen/internet/datenschutzkonforme-einwilligungen-auf-webseiten-anforderungen-an-consent-layer-194906.html> accessed 15 November 2024; Diana Ettig in Taeger and Gabel (n 8) s 25 TTDSG para 34; cf. *Planet49 GmbH* (n 13) 60-64; Schneider (n 22) 32.

service providers such as Apple and Google, can obtain the consent for the specific purpose on the controller's behalf.[26]

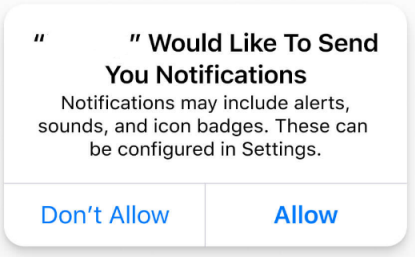

Figure 2: Example of a previous iOS push notification permission prompt.

30 It is possible that details of the design of the permission prompt window may have an impact on the validity of the consent. For example, the display of the prompt in a previous iOS version (Figure 2), highlights the "Allow" option in bold. This highlighting of the option to give consent could arguably be considered stirring[27] as part of a dark pattern, potentially[28] impairing the voluntariness of the consent (art. 4(11) GDPR) and violating the principle of fairness (art. 5(1)(a) GDPR).[29]

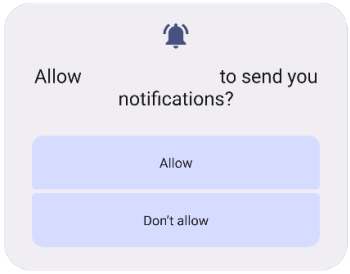

Figure 3: Example of Android push notification permission prompt.

31 The prompt in the most recent iOS versions and the Android prompt as in Figure 3 does not highlight one of the options. Aside from this issue, there are two additional challenges that need to be considered in order for the permission granted via the system prompt to be considered a valid consent under the e-privacy Directive and the GDPR.

32 Firstly, the system permission prompt does not distinguish between different categories of push notifications such as information on available updates (see Scenarios 1 and 2), reminders, and advertising (see Scenario 3). The access to device data or the storage of data for the purpose of sending push notifications with such entirely different content is subject to different purposes within the meaning of art. 6(1)(a) GDPR. A general consent to all such notifications is incompatible with the "specific" prong in art. 6(1)(a) GDPR and the "freely given" prong in art. 4(11) GDPR.[30]

33 Secondly, it is evident from Figure 2 and Figure 3 that the system permission prompts often fail to sufficiently inform users on the right of withdrawal and the implications for the processing. While users are able to change the settings for push notifications through the operating system's permission settings, they must be informed of this option prior to providing their consent (art. 7(3)(3) GDPR).

34 It could be argued that a general reference to the settings, as illustrated in Figure 2, suffices ("These can be configured in Settings"). However, the language in art. 7(3) GDPR clearly requires (explicit) information on the right to withdrawal and that it does not affect the lawfulness of the processing prior to the withdrawal. Such information is typically not provided in the system permission prompts.

35 Furthermore, one could argue that the majority of smartphone users are aware of the option to change their push notification settings. However, other than

26 Tristan Radtke, *Gemeinsame Verantwortlichkeit unter der DSGVO* (Nomos 2021) 395-397; Richard Jansen and Fabian Kreis, 'Herausforderungen bei der Datenverarbeitung im Rahmen der NEVADA Share & Secure Strategie der Automobilindustrie' [2020] RAW 19, 24; cf. Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* (ECJ, 29 July 2019), ECLI:EU:C:2019:629, paras 99-102.

27 EDPB, 'Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them – Version 2.0' (14 February 2023), paras 50-53.

28 Taking the view that the consent would still be valid in such cases Schneider (n 22) 30. On the issue in general, Ettig in Taeger and Gabel (n 8) s 25 TTDSG para 30.

29 EDPB (n 27). See also for online platforms art. 25, recital 67 of the Digital Services Act; Pascal Schumacher, Lennart Sydow and Max von Schönfeld, 'Cookie Compliance, quo vadis? Datenschutzrechtliche Perspektiven für den Einsatz von Cookies und Webtracking nach TTDSG und e-privacy-VO' [2021] MMR 603, 608 with further references.

30 EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679 – Version 1.1' (4 May 2020), paras 42-45, 55-61.

art. 13(4) GDPR, art. 7(3) GDPR does not provide an exception in cases where the data subject has already been provided with the necessary information. Instead, it requires that the information be provided in any case.

36 It can be reasonably concluded that the system permission prompt does not satisfy the conditions for valid consent under the GDPR. In such cases, the responsibility for obtaining the user's consent, with the exception of the transmission process and the explicitly requested service, lies with the respective app provider.

c.) Separate Consent by the App Provider

37 If the app provider wants to rely on the user's consent as the legal basis, the app provider could implement a separate process initiated subsequent to the permission prompt, which complies with the information requirements and allows users to choose between the push notifications for different purposes.

4. Summary

38 The exceptions laid down in art. 5(3)(2) of the e-privacy Directive cover identifiers for the transmission process as well as notifications on some essential updates for the vehicle software or the mobile app. The permission obtained through the system permission prompt does not constitute a valid consent given that those prompts do not address the specific purposes and often lack sufficient information on the right of withdrawal. However, depending on the design of the app and the services offered, the general permission given by the user through the system permission prompt, could be considered an explicit request of such service and would thus be the basis for push notifications. In other cases, the app provider is required to obtain the consent of the user separately, in accordance with the consent standards set forth in the GDPR.

II. Unsolicited Communications under Art. 13 E-Privacy Directive

39 Art. 13 e-privacy Directive does not focus on the user's device per se, rather, it focuses on messages as unsolicited communications reaching the user's sphere.

1. Scope of Art. 13 E-Privacy Directive

40 Art. 13 e-privacy Directive establishes a consent requirement for communication via means such as electronic mail for the purposes of direct marketing, with the exception of the promotion of similar products or services following a sale (art. 13(1),(2) e-privacy Directive). With regard to other forms of unsolicited communication and means other than electronic mail, the Directive leaves the concrete approach to the Member States (art. 13(3) e-privacy Directive). Member States may elect to implement either an opt-in or a mechanism for excluding users who do not wish to receive the communications. However, as apparent from the draft of the e-privacy Regulation from 2021, under a future e-privacy Regulation, the distinction between electronic mail and other forms of electronic communication may become almost obsolete.[31]

41 With regard to push notifications, it has to be determined whether they, firstly, constitute a form of direct marketing within the meaning of art. 13 e-privacy Directive. If this were not the case, art. 13 e-privacy Directive would not apply to push notifications. Secondly, it has to be assessed whether push notifications are considered either as electronic mail (art. 13(1),(2) e-privacy Directive) or as other forms of communication (art. 13(3) e-privacy Directive).

a.) Direct Marketing

42 The e-privacy Directive does not provide a definition of the term direct marketing. The definition of the similar term of advertising under art. 2(a) Directive 2006/114/EC addresses traders only.[32] However, the definition in art. 2(d) UCP Directive considering direct marketing as form of commercial

31 See art. 16 of the draft of the e-privacy Regulation, Council of the European Union (n 11).

32 Helmut Köhler in Helmut Köhler, Joachim Bornkamm and Jörn Feddersen (eds), *Gesetz gegen den unlauteren Wettbewerb* (42nd edn, CH Beck 2024), s 7 UWG para 149.

communication, an ECJ judgement[33] and guidelines by the authorities[34] suggest that direct marketing means the communication addressed directly and individually to a person in connection with the promotion, sale or supply of a product or service.

43 The direct marketing prong hinges on the content of the push notification and whether this direct communication promotes products or services. While in Scenario 3, the content itself constitutes direct marketing, for push notifications in other Scenarios the classification depends on the link to the supply of services. However, mere information without any connection to the promotion of services (as it is the case with regard to editorial information)[35] or the fact that the push notification reminds the user of the app – which is already installed – is not sufficient to constitute direct marketing.[36] Furthermore, information that the provider is legally obliged to provide may lack the promotional intent required for the marketing requirement (e.g., on necessary updates).[37]

44 However, strong indicators of a link to the supply of an *additional* service include: advertising for third parties in the app, if the app allows users to subscribe to additional services (e.g., subscription to over-the-air-updates, in-car internet access, battery capacity upgrade) or if the app is used to gain commercial advantage by analyzing user behavior – regardless of whether the user has given his or her consent under data protection law. If one of these non-exhaustive factors is present and there is a strong link to the content of the push notification, the push notification could be interpreted as relating to the promotion of (additional) services. This is because the direct marketing requirement must be interpreted broadly in line with the above definition.[38]

33 Case C-102/20 *StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH* (ECJ, 25 November 2021), ECLI:EU:C:2021:954, para 47.

34 DSK, 'Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO)' (February 2022), 3.

35 cf. Köhler (n 32) s 2 UWG para 2.70.

36 cf. Köhler (n 32) s 2 UWG para 2.36.

37 Hans-W. Micklitz and Martin Schirmbacher in Gerald Spindler and Fabian Schuster (eds), *Recht der elektronischen Medien* (4th edn, CH Beck 2019), s 7 UWG para 173; but see Köhler (n 32) s 2 UWG para 2.52, in particular for misleading information.

38 E.g., Christian Alexander in Peter W Heermann and Jochen Schlingloff (eds), *Münchener Kommentar zum Lauterkeitsrecht* (3rd edn, CH Beck 2020), s 5a UWG para 106; Köhler (n 32) s 2 UWG para 2.42; Case I ZR 57/05 (BGH, 19 April 2007), para 27; cf. *StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH* (n 33) 47-48.

b.) Electronic Mail and other Forms of Communication

45 Push notifications could be considered either as electronic mail with a strict consent requirement or as other forms of communication with opt-in or opt-out requirement depending on the legislation of the respective Member State.

46 The term "electronic mail" is defined as "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient" (art. 2(2)(h) e-privacy Directive). In recital 67 of the amending Directive 2009/136/EC, it is stated that the term "electronic mail" should be interpreted in a broad sense and that it should also apply to SMS, MMS, and similar means of electronic communication.[39] From these sources and the comparison with SMS and MMS, it can be concluded that mail requires an inbox as a local or online collection of received messages. This inbox typically prompts the user to go through the messages as a list, which makes it more likely for advertising to be noticed by the user than it is the case for other means of communication.[40]

47 Push notifications do not utilize an inbox in the same way as email or SMS; both of which may be the subject of a push notification. The respective operating system does indeed collect the push notifications and provides the user with an overview of the notifications received. However, this categorized overview does not adhere to the conventional rules of an inbox and is instead selective and temporal in nature.

48 For example, limits might apply to an app or website sending multiple push notifications to a user,[41] the app provider could suppress the notification from being displayed beforehand[42] or the push notification could be discarded before delivery if the user's device is offline for a long time.[43] Unlike emails, a notification is often deleted as soon as the corresponding app is opened. The notification might not even be stored until retrieval by the user's device. In addition, push notification providers have

39 *StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH* (n 33) 38-39.

40 cf. *StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH* (n 33) 41.

41 E.g., *Firefox Support* (n 4).

42 E.g., 'com.apple.developer.usernotifications.filtering' (*Apple Developer*) <https://developer.apple.com/documentation/bundleresources/entitlements/com_apple_developer_usernotifications_filtering> accessed 15 November 2024.

43 E.g., *Apple Developer* (n 5); 'About FCM messages' (*Google Firebase*) <https://firebase.google.com/docs/cloud-messaging/concept-options> accessed 15 November 2024.

announced summaries of push notifications, and it remains to be seen whether the system may further filter push notifications in this context.[44]

49 Overall, push notifications do not follow the typical inbox and list procedure but are rather selectively and temporarily stored for the user. Instead of being relevant until the user reacts by replying, forwarding or deleting the message, the push notification is usually only relevant for a short time frame and serves as a reminder in connection with the respective app.

50 At first sight, the ECJ's finding that the display of randomly generated and only temporarily stored advertising within an inbox suffices[45] could support the view that any temporarily stored message nevertheless falls within the scope of art. 13(1) e-privacy Directive. However, the ECJ did primarily contest the fact that the temporarily stored advertising was displayed as part of the inbox for electronic mail.[46] As push notifications are displayed separately and not as part of an inbox, this argument cannot be applied to push notifications.

51 Thus, push notifications do not constitute electronic mail.[47]

2. Requirements

52 As push notifications fall within the scope of art. 13(3) e-privacy Directive,[48] providers are obliged to comply with the applicable implementation at the level of the Member State. This entails either obtaining consent or refraining from sending push notifications to users, who do not wish to receive the notifications. The latter may be indicated, e.g., by the app's settings, which allow users to specify the types of notifications they wish to receive, or to indicate whether they wish to be informed about previous notifications. This is subject to the condition that the tracking of such reactions is permissible under data protection law.

53 Insofar as the push notification provider allows users to choose an interruption level (e.g., "passive", "active", "time sensitive", and "critical" for iOS users),[49] the selection of an inappropriate interruption level has to be considered when assessing the compliance with the user's wish. This is because the language in art. 13(3) e-privacy Directive considers the specific unsolicited communication ("these communications"), which allows for the consideration of the specific circumstances of such a message. The general classification of different means of communication (e.g., art. 13(1) e-privacy Directive) and the consideration of a certain *circumstance* in art. 13(2) e-privacy Directive supports this finding.

C. GDPR

54 The GDPR lays down requirements for the processing of personal data and sets requirements for push notifications to the extent personal data is processed.

55 In light of the e-privacy Directive's status as *lex specialis* and the GDPR's as *lex generalis* (art. 95 GDPR),[50] the GDPR does not impose additional requirements pertaining to the legal basis for accessing a user's device and storing information including potential unsolicited communication on the user's device.[51] However, the sending of a push notification entails the processing of personal data prior to and subsequent to the access to the user's device. In such instances, the GDPR, and in particular art. 6 GDPR, applies.[52]

44 'Introducing Apple Intelligence, the personal intelligence system that puts powerful generative models at the core of iPhone, iPad, and Mac' (Apple, 10 June 2024) <https://www.apple.com/newsroom/2024/06/introducing-apple-intelligence-for-iphone-ipad-and-mac/> accessed 15 November 2024.

45 *StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH* (n 33) 63.

46 *StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH* (n 33) 46.

47 Taking a different view Julia Höltge, 'Werbung über mobile Push-Dienste' [2015] ITRB 223, 223.

48 For art. 13 in general, EDPB, 'Guidelines 8/2020 on the targeting of social media users – Version 1.0' (2 September 2020), 17.

49 'Managing notifications' (*Apple Developer*), <https://developer.apple.com/design/human-interface-guidelines/managing-notifications> accessed 15 November 2024.

50 Papakonstantinou and De Hert (n 8) 1.

51 EDPB (n 9) 40; Tilman Herbrich and Elisabeth Niekrenz, 'Privacy Litigation Against Real-Time Bidding Data-driven online marketing: Enforcing the GDPR by protecting the rights of individuals under civil law' [2021] CRi 129, para 50; Carlo Piltz in Peter Gola and Dirk Heckmann (eds), *Datenschutz-Grundverordnung* (3rd edn, CH Beck 2022), art. 95 DS-GVO para 23; Golland (n 8) 23. Taking another view Maximilian Becker, 'Consent Management Platforms und Targeted Advertising zwischen DSGVO und e-privacy-Gesetzgebung' [2021] CR 87, para 55.

52 EDPB (n 9) 40-41; Herbrich and Niekrenz (n 51) 65; Wolf-Tassilo Böhm and Valentino Halim, 'Cookies zwischen e-privacy und DS-GVO – was gilt? – Anforderungen an die Verwendung von Cookies nach der aktuellen Rechtsprechung' [2020] MMR 651, 653; cf. Ettig in Taeger and Gabel (n 8) s 25 TTDSG para 12.

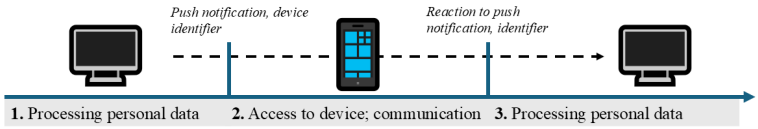

Figure 4: Underlaying technical steps for the interplay between the GDPR (1. and 3.) and the e-privacy Directive (2.).

I. Scope of the GDPR

56 Pursuant to art. 2(1) GDPR, the GDPR applies to any processing of personal data, which is broadly defined as any operation which is performed on "any information relating to an identified or identifiable natural person ('data subject')" (art. 4(1), (2) GDPR). According to the case law of the ECJ, the information constitutes personal data from the perspective of the controller as defined in art. 4(7) GDPR, if the controller has available "means likely reasonably to be used either by the controller, [...] or by any other person, to identify that person, without, however, requiring that all the information enabling that person to be identified should be in the hands of a single entity".[53]

57 In all Scenarios, the push notification is sent to a specific device of a data subject. The processing of the push notification in order to transmit and deliver it to the device entails the processing of personal data, including the device token and the content of the notification. In general, the app provider links the device token to account data or other user data on its servers. Even if the respective app provider does not have access to the device tokens but is nevertheless able to trigger a general push notification to all registered devices, the natural person in question can be identified by the app provider through the use of reasonable means. In fact, the app provider can request further information about the specific device and potentially the user at any time.

58 Thus, the GDPR applies to the process of sending and receiving a push notification except for the final step of the storage on the user's device. In light of the fact that the app provider determines the purpose and means of the processing by initiating the processing,[54] including the decision on the user as the data subject, the content, and other modalities, the app provider is to be regarded as controller under art. 4(7) GDPR. However, if another person or entity exerts influence in its own interest over the push notification (e.g., extensive filtering by the push notification provider or a third party pays for advertising), such person or entity might be considered the controller or joint controller under art. 26 GDPR.[55] This applies even in cases where such person or entity lacks access to personal data.[56]

II. Legal Basis

59 Pursuant to art. 6 GDPR, any processing activities must be supported on a legal basis. In the context of push notifications, the following legal bases are particularly relevant: the data subject's consent (art. 6(1)(a) GDPR), the necessity for the performance of a contract (art. 6(1)(b) GDPR) and the balancing of interests (art. 6(1)(f) GDPR).

1. Consent

60 In order to obtain consent in accordance with arts. 4(11), 6(1)(a) GDPR,[57] the standards and requirements set out above apply (see B. I. 3.). Consent under the e-privacy Directive and for the upstream and downstream processing operations under the GDPR can be jointly[58] obtained if all operations serve similar, specific purposes[59] within the meaning of arts. 4(11), 5(1)(b), art. 6(1)(a) GDPR.

2. Performance of a Contract

61 Nevertheless, the processing is also lawful if it is "necessary for the performance of a contract to which

53 Case C-319/22 *Gesamtverband Autoteile-Handel eV v Scania CV AB* (ECJ, 9 November 2023), ECLI:EU:C:2023:837, para 45; Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* (ECJ, 19 October 2016), paras 42-43.

54 cf. *Fashion ID* (n 26) 75, 78.

55 cf. Case C-25/17 *Tietosuojavaltuutettu, Jehovan todistajat - uskonnollinen yhdyskunta* (ECJ, 10 July 2018), ECLI:EU:C:2018:551, para 68.

56 Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (ECJ, 5 June 2018), ECLI:EU:C:2018:388, para 38.

57 See *Planet49 GmbH* (n 13).

58 cf. Björn Steinrötter, 'Anforderungen an die Einwilligung des Internetnutzers beim Setzen und Auslesen von Cookies' [2020] GPR 106, 109.

59 cf. Marion Albers and Raoul-Darius in Heinrich Amadeus Wolff, Stefan Brink and Antje v. Ungern-Sternberg (eds), *BeckOK Datenschutzrecht* (48th edn, CH Beck, 1 May 2024) art. 6 DS-GVO para 32; Giovanni Sartor in Spiecker gen. Döhmann and others (n 8), art. 6 para 19.

the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (art. 6(1)(b) GDPR). Necessity must be determined from an objective perspective and has to take into account the main obligations under the contract as mutually agreed by the parties.[60] Features that are merely useful for the performance of the contract, such as personalized advertising in a social network rather than non-personalized advertising, are thus not covered by art. 6(1)(b) GDPR.[61]

62 In the first Scenario, there are likely several contractual relationships depending on the individual circumstances. For example, the user may have bought the vehicle and thereby concluded a consumer contract for the sale of a good (cf. Directive (EU) 2019/771). The user may have entered into a separate contract for the use of connected vehicle services and a contract for the downloading and utilization of the smartphone app (cf. Directive (EU) 2019/770). In order to determine the contractual relationships in question, it is crucial to ascertain whether such vehicle network and smartphone app services form an integral part of the contract for the purchase of the vehicle (cf. art. 3(4) Directive (EU) 2019/770).[62]

63 In the case of security updates, the vendor of the vehicle or the app provider may be under a contractual obligation to provide such updates (e.g., art. 8(2) Directive (EU) 2019/770). Providing information on these updates via push notification is a secure and admissible way of notifying the user of the available update. In this case, it could be considered that the processing is necessary for compliance with the legal obligation deriving from art. 8(2) Directive (EU) 2019/770 and within the meaning of art. 6(1)(c) GDPR. However, in accordance with art. 6(3)(1) GDPR, the specific purposes of the processing must be clearly outlined in the legal basis.[63] The national implementation of art. 8(2) Directive (EU) 2019/770 does not provide for a *notification* obligation and also presupposes a contractual relationship. Therefore, recital 38(1),(2) Directive (EU) 2019/770 refers particularly to the legal basis of the necessity for the performance of the contract as laid down in art. 6(1)(b) GDPR.

64 However, the necessity of processing for the performance of the contract depends on whether the data subject is not sufficiently informed by other means. For example, the notification may not be considered necessary if the vehicle or, in the case of Scenario 2, the app store automatically provides and installs the app updates in due time and the connection to the vehicle in the meantime is maintained (i.e., the update is not urgent).

65 Assuming that this requirement is met, the installation of updates is often linked to the continuous provision of the vehicle connection services. As a result, the processing is necessary for the performance of the respective contracts.

66 With regard to Scenario 2, similar considerations apply. Updates that are essential for maintaining the connection to the vehicle, which form the main purpose of the app and the respective contract, and the information conveyed via a push notification may be covered by art. 6(1)(b) GDPR, provided that there are no more effective means of installing the update.

67 In the third Scenario, the information on the availability of the discount could be considered useful for the user. However, such an upgrade is not part of the same contract (see above B. I. 2. b., and the vehicle connection services can be provided without the information on the upgrade. Therefore, processing for a push notification in Scenario 3 would not be considered necessary.

3. Balancing Interests

68 In particular for the third Scenario, art. 6(1)(f) GDPR could be considered the applicable legal basis. Art. 6(1)(f) GDPR permits processing which "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". Accordingly, the ECJ requires (1) a legitimate interest, (2) for which the processing is necessary, and (3) the interests and rights of the data subjects must not override the legitimate interest.[64]

60 Case C-252/21 *Meta Platforms Inc. and others v Bundeskartellamt* (ECJ, 4 July 2023), ECLI:EU:C:2023:537, para 98; EDPB, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects – Version 2.0' (8 October 2019), paras 30-32.

61 *Meta Platforms* (n 60) 102.

62 See Tristan Radtke, 'Das Recht des Streamings im Vergleich mit dem herkömmlichen Kaufrecht' in Gregor Albers and Hanjo Hamann (eds), *Vertrieb und Vertrag auf der Schwelle zur Dienstleistungswirtschaft* (Mohr Siebeck, forthcoming).

63 Marion Albers and Raoul-Darius in Wolff, Brink and v. Ungern-Sternberg (n 59) art. 6 DS-GVO para 48; for examples for legal obligations see EDPB, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' (8 October 2019), paras 44 (example 4) and 47 (example 6).

64 Case C-597/19 *Mircom International Content Management*

69 Any economic interest fulfils the requirement of the legitimate interest (cf. recitals 47, 48 GDPR). This is particularly the case where there is a contractual relationship between the controller and the data subject (recital 47(2) GDPR). The reasonable expectation of the data subject (cf. recital 47(3),(4) GDPR) is an important factor in determining the weight of the interests of the data subject.

70 In Scenarios 1 and 2, the legitimate interest of the app provider in informing users of software updates to maintain the services is particularly strong if the information on the update is necessary to maintain the security of the vehicle and the app (cf. recital 49 GDPR). From the user's perspective, there is an interest in the protection of their personal data (art. 8 Charter) and the right to be protected against unsolicited communications on their devices, including the processing prior to delivering such communications (cf. art. 7 Charter). In light of the aforementioned considerations, it is reasonable to conclude that the rights and interests of data subjects do not prevail in Scenarios 1 and 2, contingent on the design of the app and the user expectations shaped by it (see above under B. I. 2. b.), as well as the frequency of processing (i.e., the frequency of notifications).

71 The processing of personal data for marketing purposes, including direct marketing, can also serve a legitimate interest (recital 47(7) GDPR).[65] Nevertheless, data subjects have the right to object to the processing at any time, without giving reasons (art. 21(3) GDPR). In the light of the aforementioned, even the occasional dissemination of information via push notifications regarding discount offers within the app, as in Scenario 3, may be justified as form of direct marketing on the basis of art. 6(1)(f) GDPR.

72 However, the interests of data subjects may prevail if the content and timing of the advertising is personalized in such a way that it is based on excessive behavioral targeting in the form of profiling[66] (arg. art. 35(3)(a), recital 60(3),(4) GDPR) or if third parties process personal data in connection with push notification advertising for third party services.

4. Summary

73 Consent appears to be a practical way forward under the GDPR, as it can be combined with the consent required under the e-privacy Directive. However, the processing of personal data for necessary and urgent updates, as potentially in Scenario 1 and 2, may be necessary for the performance of the contract. Notifications in those Scenarios regarding less urgent updates might be based on the balancing of interests. In Scenario 3 and other scenarios, under certain conditions, the balancing of interests or, in any case, the consent obtained by the app provider allows for the processing to prepare the delivery of a push notification and for post-delivery processing.

III. Further Requirements

74 In addition to its existing obligations, the controller is subject to further requirements under the GDPR. It is important to note that such requirements pertaining to push notifications are interlinked with those discussed above. For instance, controllers must comply with the data processing principles under art. 5 GDPR, including the lawfulness under art. 5(1)(a) GDPR, and must inform data subjects pursuant to arts. 13, 14 GDPR. Default settings for push notifications within an app (e.g., for fine-tuning the content and frequency of notifications) must be designed in compliance with data processing principles such as data minimization (art. 25(1),(2), art. 5(1)(c) GDPR).

D. Further Regulation

75 In regard to push notifications and their content, the relevant legislation, such as the UCP Directive and the ecommerce Directive (both as amended), provides less specific provisions.

I. UCP Directive

76 The amended UCP Directive 2005/29/EC subjects commercial practices to additional requirements. The term "commercial practice" refers to "any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers" (art. 2(d) UCP Directive). Consequently, the requirements set forth in the UCP Directive apply to push notifications that are directly connected to the promotion of the app and the provided services

& Consulting (M.I.C.M.) Limited v Telenet BVBA (ECJ, 17 June 2021), ECLI:EU:C:2021:492, para 106; case C-13/16 *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA „Rīgas satiksme"* (ECJ, 4 May 2017), ECLI:EU:C:2017:336, para 28.

65 See also Becker (n 51) 66.

66 Article 29 Data Protection Working Party, 'WP251rev.01' (6 February 2018), 14-15.

(cf. above under B. II. 1. a.).[67]

77 For example, art. 7(2) UCP Directive considers the absence of an indication of commercial intent within a commercial practice to be a misleading omission. This is the case where the commercial intent is neither apparent from the context nor identified. The commercial link between the push notification and the promotion of the app is typically apparent from the name and icon of the app as included in the push notifications. However, in instances where an additional commercial intent is not apparent from the context, as may be the case in Scenario 3, the app provider is required to identify this commercial intent, e.g., by declaring the push notification as "advertising".[68]

78 The misleading use of app name and icon to mislead users into believing that another provider is responsible for the notification and the app may be prohibited under art. 5(1),(5), Annex I(13) UCP Directive without prejudice to claims under intellectual property law. This is particularly relevant for apps under less strict scrutiny of app store providers, e.g., third party apps provided on alternative app distribution platforms.[69]

79 The sending of persistent and unwanted solicitations is prohibited under art. 5(1),(5), Annex I(26) UCP Directive. This practice is of less relevance for push notifications, as users are able to indicate their wish regarding push notifications and, furthermore, to prevent an app and its provider from sending the user push notifications by means of the operating system settings. However, if the app provides for finer adjustments to notifications and does not respect the indicated settings, this prohibition could apply.

II. Ecommerce Directive

80 The amended ecommerce Directive 2000/31/EC applies to information society service providers within the meaning of art. 1(1)(b) Directive (EU) 2015/1535. Such services include apps and sent push notifications (see above B. I. 2. b.).

81 In accordance with art. 5 ecommerce Directive, app providers are obliged to make information such as the name of the provider easily, directly and permanently accessible. In the case of push notifications, this requirement is satisfied if the relevant app interface allows for the information to be accessed with ease.[70]

82 However, in addition to the attribution of the push notification to a particular application and its associated interface, the identification requirement set forth in art. 6(b) of the ecommerce Directive also necessitates the assignment of a unique and distinctive combination of an app name and app icon.

83 Similar to art. 7(2) UCP Directive, commercial communication has to be clearly identifiable as such under art. 6(a) ecommerce Directive.

E. Conclusion

84 Push notifications have become an important means to inform users directly. Although sending push notifications might appear straightforward given the permissions obtained by each app, these notifications raise complex legal issues, particularly under the e-privacy Directive and potentially under a future e-privacy Regulation.

85 Despite the impression the system permission prompts for push notifications might give, such permissions do not constitute a valid consent under art. 5(3) e-privacy Directive for the temporary storage of the notification on the user's device. In this respect, push notifications clearly demonstrate the requirements for consent in the interaction between the e-privacy Directive and the GDPR.

86 Nevertheless, contingent on the configuration of the app and the scope of services it offers, as well as the frequency of notifications, such permission may be construed as an explicit request for the notification service, in accordance with art. 5(3) (2) of the e-privacy Directive. Accordingly, the interpretation of the concept of a service, whether narrow or broad, is crucial for the application of art. 5(3) of the e-privacy Directive. Push notifications with marketing and advertising content, by contrast, regularly require consent under the e-privacy Directive.

67 Micklitz and Schirmbacher (n 37); cf. Boris Paal and Dominik Nikol, 'Spendenwerbung durch E-Mail-Direktmarketing zwischen UWG und DSGVO' [2023] GRUR 781, 784 for the relationship between commercial practice and direct marketing.

68 In detail Tristan Radtke, 'Disclosure Requirements for Influencer Marketing in the U.S. and Germany' (2022) 12 JIPEL 141, 147-154. See also art. 5(5), Annex I(11) UCP Directive for advertorials, which is of less relevance for push notifications.

69 See recently for Apple devices 'About alternative app distribution in the European Union' (*Apple*) <https://support.apple.com/en-us/118110> accessed 15 November 2024.

70 cf. Case I ZR 228/03 (BGH, 20 July 2006).

87 In light of the case law of the ECJ and the meaning and purpose of the characteristic of electronic mail, push notifications are not to be considered as electronic mail within the meaning of art. 13(2) e-privacy Directive. Thus, app providers must comply with the requirements of art. 13(3) e-privacy Directive as implemented by the Member States when sending push notifications. In instances where Member States have elected to implement an alternative approach that excludes users who do not wish to receive communications, as opposed to opt-in, a relative approach is applied, allowing for consideration of the circumstances of the individual communication. The specific purpose of the communication, the frequency and the application settings have been identified as such relevant circumstances. As things stand at present, an e-privacy Regulation may abandon special provisions for electronic mail and establish uniform standards for electronic communication.

88 The GDPR applies to the processing of personal data both before and after the delivery of the push notification. Consequently, the e-privacy Directive and the GDPR are complementary and require a clear distinction between the individual storage of information and processing activities. For such processing activities, the legal basis under the GDPR is often the necessity for the performance of a contract under art. 6(1)(b) GDPR or the balancing of interests under art. 6(1)(f) GDPR. With regard to contracts for connected products, the different contracts need to be assessed carefully taking into account regulations such as the Directive (EU) 2019/770. The balancing of interests requires consideration of factors similar to those under the e-privacy Directive. Forms of direct marketing might fall within art. 6(1)(f) GDPR. For other cases, the processing can be based on the consent under art. 6(1)(a) GDPR, which can often fulfil the consent requirements under the e-privacy Directive at the same time.

89 This complex interplay of e-privacy and data protection is further compounded by other legal acts, such as the UCP Directive. The resulting transparency requirements assume particular significance with regard to apps that are downloaded via unofficial app stores, a phenomenon that has only recently become possible on Apple devices.