Comparison of notice requirements for consent between ISO/IEC 29184:2020 and GDPR

- Harshvardhan J. Pandit
  ADAPT Centre, Trinity College Dublin, Dublin, Ireland pandith@tcd.ie
  Bio: Harshvardhan J. Pandit is a Research Fellow at the ADAPT SFI Centre in Trinity College Dublin. His PhD thesis investigated the ontological representation of activities associated with processing of personal data and consent for GDPR compliance. He currently works in areas of privacy risks, consent and its documentation, and regulatory compliance.
- Georg Philip Krog
  Cofounder, Chief of Legal Counsel, *Signatu AS, Share Oslo, Myntgata 2, 0150 Oslo, Norway georg@signatu.com*
  Bio: Georg Philip Krog is Cofounder and Chief of Legal Counsel of Signatu. His previous roles include being consultant in data protection law, copyright law and private international law, researcher at the Faculty of Law in Oslo and Max Planck Institut in Hamburg, and Fulbright Scholar at Harvard Law School and Stanford Law School.

Accepted for publicaion in Journal of Data Protection & Privacy, Volume 4, 2021 https://www.henrystewartpublications.com/jdpp

Abstract

This article analyses the ISO/IEC 29184:2020 standard and compares its requirements for notice and consent with those specified by the General Data Protection Regulation (GDPR). More specifically, it considers the extent to which the ISO/IEC 29184 standard can be applied to demonstrate compliance with the requirements of the GDPR, and to identify the additional requirements in areas where it is not sufficient. The article concludes with remarks on the potential role of ISO/IEC 29184 as a certification mechanism under GDPR for consent and notice.

Keywords: Consent, Notice, GDPR, Regulatory Compliance, Privacy, ISO

Introduction

The European General Data Protection Regulation (GDPR) permits the use of consent as a lawful basis for processing of personal data (Art.6) along with specific obligations and

requirements for the consent to be considered valid. This includes obligations regarding the provision of information that is crucial to make a choice regarding consent, and this information seems to be borne out of Art.13 and Art.14, which in the context of informed consent takes the form of a notice[1]. While the GDPR by itself along with guidelines and case law dictate which information controllers must provide to data subjects to make an informed consent choice in relation to the processing of their personal data, these obligations are binding on all practical implementations regarding notice and consent, and therefore have to be interpreted as requirements for compliance. ISO/IEC 29184:2020 'Information technology - Online privacy notices and consent' (hereafter referred to as *29184*) is a recent standard published in July 2020 that specifies requirements for online privacy notices and consent in a jurisdiction agnostic manner. The aim of 29184 is to enable individuals to understand and control through their consent the potential impact of the processing of their personal data and its consequences. Like other ISO/IEC standards, it is designed to complement existing ISO frameworks. For example, it implements privacy principles of 'consent and choice' and 'openness, transparency, and notice' from ISO/IEC 29100:2011 'Information technology - Security techniques - Privacy framework'.

GDPR defines use of standards such as 29184 to aid in the legal compliance procedures by acting as a certification mechanism (Art.42) and in the implementation of data protection by design and default (Art.25). However, unlike GDPR, 29184 is non-binding in terms of legal compliance, but its requirements must be met in order to claim conformance and its use as a certification for GDPR compliance. In this article, we therefore explore the extent to which 29184 can be used to meet the obligations of GDPR regarding notices and consent by comparing its requirements with the interpretations and guidelines provided by the GDPR and the European Data Protection Authorities. We limit our scope to the definition and requirements associated with collection of consent and the provision of notice along with information presented through it. Given that 29184 uses the ISO defined terms which are distinct and sometimes incompatible with definitions in GDPR, we use generic concepts or their equivalent terms in GDPR and offer clarifications when they are incompatible.

Consent

Definition of Consent

29184 uses the definition of consent from ISO/IEC 29100:2011 that states consent is an individual's freely given, specific, and informed agreement. It also defines 'opt-in' as a mechanism where a process of a policy requires an individual to 'take an action to express explicit consent' in order to carry out processing of personal data. 29184 combines the two definitions for 'explicit consent' as: consent where the agreement is 'unambiguous' and

1 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p. 15. See also judgment of 1st October, 2019, Planet49 GmbH, C-673/17, para 79.

'exercised through an affirmative act'. In this, 29184 defines 'freely given' as consent 'without any form of coercion or compulsion'.

Consent in GDPR is similarly defined as an individual's clear affirmative action or statement that signals agreement and is freely given, specific, informed, and unambiguous (Art.4-11). GDPR similarly obliges the controller to enable the data subject to make his or her choice by an unambiguous indication by means of a clear affirmative action or statement, which means that for consent to be valid, consent must be given by deliberate action or declaration. 'Explicit consent' in the context of GDPR means that the individual must give an express statement acknowledging their consent[2], for example by filling a form or using an electronic signature or using statements indicating action of consent such as "I consent to…". The 29184 definition of 'explicit consent' thus meets the requirements of (non-explicit) consent under GDPR. However, it does not meet the requirements of 'explicit consent' under GDPR which additionally requires an express statement or action.

Consent as Legal Basis

29184 requires the controller to request consent in situations where consent or explicit consent is appropriate, such as in the context of sensitive personal data being processed, or the potential for negative impact to the individual, or where consent is the legal basis. It notes the role of jurisdictional legislations in requiring use of consent as a legal basis in specific situations, and the existence of other legal basis for processing personal data. 29184 itself does not mandate use of explicit consent, and instead delegates the decision to controllers.

GDPR also permits use of consent alongside other legal basis for processing of personal data (Art.6), and requires the controller to utilise the most suitable one[3]. Where consent is used as a legal basis, GDPR additionally requires it to be 'explicit consent' for situations including: processing involving special categories of personal data (Art.9-2a), transfer of personal data to a third country or international organisation (Art.49-1a), use of automated individual decision making including profiling (Art.22-2c). In addition to these, consent can also be used as a lawful basis for continuation of processing after the right to restriction of processing has been exercised (Art.18-2).

Thus, while 29184 and GDPR both specify the use of consent as one of the possible legal bases, GDPR additionally specifies the situations where consent must be 'explicit'. From this, it is clear that use of 'explicit consent' in 29184 can be applied to situations where 'non-explicit' consent is used as a legal basis under GDPR. For situations where GDPR requires 'explicit consent', conformance with 'explicit consent' under 29184 is not sufficient by itself to be considered a valid legal basis.

---

2 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.20-22.

3 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.4.

Associating Identity with Consent

Where consent is associated with an account, 29184 requires the organisation to clearly indicate the specific identity or account when collecting consent in a manner they are accustomed to in context of the service. In cases where an individual does not have an account, but the organisation or service identifies the individual using an implicit account, 29184 mentions the possibility of such accounts being linked to an explicit account later.

In contrast, GDPR does not specify any requirements for associating consent with any identity or account, whereas the ePD (Art.5-3) distinguishes between a “subscriber and a “user” that consents. Additionally, GDPR encourages using an identifier so that controllers can demonstrate the individual’s given consent (Art.7-1), enable them to withdraw it (Art.7-3), and to provide them with a history of their consent events (Art.15).

Freely Given Consent

29184 requires consent to be ‘freely given’ - which means it must be obtained separately from other matters such as terms and conditions to prevent negative impacts on the comprehension of information related to consent. The action associated with consent is thus also required to be separate from actions associated with consent for other matters. In addition, 29184 also considers consent to be ‘freely given’ only when the individual does not perceive any coercion or compulsion.

Similarly, GDPR also requires consent to be ‘freely given’ (Rec.32, Rec.43, Art.4-11, Art.7-4) where the data subject is given a real choice to consent, refuse to consent or withdraw consent. This means that the data subject must not be forced to consent through coercion or compulsion, should not be tied to a contract (Art.7-4), since then consent will be presumed to be not freely given (Rec.43), must not bundle several purposes (Rec.43), and must not be caused harm or damage when refusing or withdrawing consent (EDPB p. 6-7, 9-13 and 18-19.)

As this requirement is absent within 29184, consent considered ‘freely given’ under 29184 may not satisfy the requirements of GDPR.

Specific

29184 requires that the information the controller must provide in the consent notice must be specific.

Similarly, GDPR (A4(11)) says that consent must be specific, that personal data shall be collected for specific purposes (A5.1(b)) and that processing shall be lawful only if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes (A6.1(a)). Hence, in order to comply with this obligation, the

controller must in the consent request specify the processing purpose, ask for consent to each purpose and separate the consent request from information about other matters[4].

Timing, Frequency, and Renewal of Consent

29184 states that consent should not be obtained 'too early' and instead should be obtained in a 'timely' manner in order to avoid 'practical issues' regarding the choices made. While it does not state what 'timely' or 'practical issues' mean in practice, it requires the timing of a notice provided regarding consent to be appropriate to the collection and processing of personal data, with notices being typically provided before collection and processing of personal data takes place.

In the case of GDPR, although it does not explicitly prescribe that consent must be given prior to the processing activity, this can be interpreted following its use as a legal basis which must be established prior to processing[5].

The frequency and renewal of consent relates to the process of confirming existing consent or collecting new consent from the individual after an interval from the existing consent. 29184 deters organisations from requesting consent frequently as this can lead to the individual giving consent without understanding the consequences. It suggests considering negative impacts or risks of such impacts on the individual for determining the frequency and renewal of consent such that the individual can sufficiently understand and prepare for the risks and/or impacts.

The renewal of consent, or 're-consent', in 29184 is specified as typically being required where a change in 'condition' occurs regarding information or criteria at the time of request to which the consent was given. When such conditions change, a renewed consent from the individual is required to be obtained before the changes are implemented in processing. Examples in 29184 of changes requiring a renewed consent include changes of purpose for processing, personal data being processed, processing of personal data (including collection and transfer to third party), collection method for personal data, deletion date or period for personal data, changes to method or process for exercising revocation of consent, and substantial organisational change regarding data controller. Depending on whether a record of prior consent is available to the individual and the time elapsed since prior consent, organisations may need to reconfirm the existing consent in addition to the consent for changes.

---

4 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.13-15.

5 The wording "has given" in Art.6-1 supports this interpretation. See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.20. See also WP29 Opinion 15/2011 on the definition of consent (WP 187), p 30-31. See also judgment of 29th July, 2019, Fashion ID, C-40/17, para 102.

GDPR also obliges obtaining a new and specific consent when the conditions associated with it change[6], which includes the examples mentioned within 29184. The validity and expiry of consent is not prescribed in the GDPR, but depends on the context of processing, scope of original consent, and the expectations of the data subject. If the processing operations change or evolve considerably, the original consent is no longer considered valid. The EDPB recommends as a best practise that consent should be refreshed at appropriate intervals[7]. Thus, the 29184 requirements permit it to be used for conformance with GDPR requirements regarding timing, frequency and renewal of consent.

Withdrawal of Consent

29184 requires consent to be easily accessed, modified, and withdrawn by the data subject. The modification and withdrawal of the consent should be as easy as it was to give consent. 29184 suggests this can be achieved by providing an account or privacy settings page for the individual. In cases where a consent is being renewed, and the individual does not respond, 29184 considers this as indication that the original consent has been withdrawn. Where consent is a legal basis and revocation is required to be legally provided, 29184 also requires information on how this can be exercised by the individual.

Art.7-3 of GDPR similarly obliges the controller to provide information in the consent notice about the right to withdraw consent and how to exercise that right. GDPR obliges the controller to provide a choice for the data subject to withdraw consent to each of the purposes and says that withdrawing consent must be as easy as giving it[8].

Evidence of Consent

29184 requires organisations to inform individuals how and where they can access evidence of their ‘choice(s)’ made along with any subsequent changes and their dates, and defines ‘choice’ as the action by the individual following the principle of ‘consent and choice’ in ISO/IEC 29100:2011. It does not mention the form or manner of how this evidence should be recorded or documented.

GDPR similarly obliges the controller to document consent, which means that the controller has a duty to demonstrate a data subject’s consent and has the burden of proof to demonstrate that consent (Rec.42). Although the GDPR does not prescribe the form or manner of such evidence, a controller must be able to demonstrate evidence that all required information was provided to

6 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.20.
7 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.23.
8 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.15.

the individual, such as through a notice, and that the subsequent choice made by the individual satisfies the requirements of valid consent under GDPR.

As an example of record for documenting consent, the 29184 mentions the Consent Receipt[9] with further elaboration on its potential role as a record of consent provided in Annex B. The Consent Receipt captures consent as machine-readable data that can also be visualised as a human-readable 'transaction', and consists of relevant information such as parties, purposes, and recipients. Comparison of the Consent Receipt with the requirements of GDPR and 29184 shows that it lacks several important fields of information which makes it unsuitable for use in documenting consent for legal compliance.

Notice for Informed Consent

Function

The notice and consent requirements in 29184 are defined with the aim that an individual can "give consent freely, specifically, and on a knowledgeable basis; and easily access, modify and/or withdraw that consent." In order for the given consent to be considered as 'informed', 29184 requires provision of a notice containing information regarding the processing of personal data. Such notices must be provided appropriate to the context of the product or service to enable individuals to easily find and access them - such as through links on a website's homepage or landing pages, captive portals, and online forms.

GDPR considers consent to be informed where, at minimum, the data subject is aware of the identity of the controller, the purposes of processing intended personal data, what type of data will be collected and used, the existence of the right to withdraw consent, information about the use of the data for automated decision-making (in accordance with Art22-2c), and on the possible risk of data transfers due to absence of an adequacy decisions and appropriate safeguards[10] (Rec.42, Rec.60, Art.46) which will be presented below.

Understandable

A notice as per 29184 must be provided in a clear and easily understandable manner for the targeted individuals, must be easily legible, and must use 'concise language that a person without any legal or technical training can comprehend' based on the individual's expectations. 29184 mentions the possibility of implementing multilingual notices by providing options for

9 Lizar M, Turner D. Consent Receipt Specification v. 1.1. 0. Kantara Initiative Technical Specification. 2018.
10 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.15-16.

selecting languages or through the web-browser's preferences. 29184 also requires information in the notice to be understandable in terms of relations between them, in particular regarding purposes and personal data.

GDPR similarly requires information to be provided in clear, precise, concise and plain language to enable an average person, or minors where applicable, to easily understand the information in their own language[11] (Rec.39, Rec.42, Rec.58). Similar to 29184, GDPR requires the information to clearly indicate the relation between purpose and personal data.

29184 requires the notice to be made accessible based on the technologies used to provide it. Where individuals are expected to have accessibility issues, the notice should enable them to understand the information through features such as text-to-sound. It mentions the use of ISO/IEC 40500 for designing accessibility into a service. Similarly, GDPR (Rec.39, Rec.58) also obliges the provision of the notice in a language and design that is "easily accessible for vision impaired end users"[12].

Form of Notice

29184 requires the interface or 'screen' providing the notice and collecting consent through an affirmative action to be one and the same. It states that separation of interfaces can lead to confusion for individuals regarding their action for consent. Where a single interface is not feasible, 29184 requires organisations to summarise the key points of the notice on the interface obtaining consent in order for the individual to "clearly understand what they are consenting to". Where a notice is 'layered', 29184 requires the first layer to provide information considered unexpected or regarding significant impact to the individual and provide information intended for quick comprehension using measures such as summarisation and links to further information.

GDPR similarly obliges the use of interfaces that enable the individual to be informed and make a choice regarding consent through the same interface. GDPR (Art.7-2) obliges the controller to provide the consent notice in an easily accessible form[13] (Rec.32). GDPR also states that notice should not be unnecessarily disruptive to the use of the service for which consent is requested and provided. Thus, it may be necessary that a consent request interrupts the use of the service with an action by which consent is given that is clearly distinguished from other actions.

29184 mentions notices can be provided in various forms such as textual, visual, or graphical, and can include design and interface elements such as layered notices, dashboards, icons, and

11 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.16.
12 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.16.
13 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.18.

just-in-time notices based on the technology and medium of provision. 29184 also mentions the possibility of using machine-readable notices (e.g. as XML and JSON standardised formats) that can be used to select the graphics or icons shown to the individual.
GDPR (Rec.60, Art.12-7, Art.12-8) similarly says it is permitted for the controller to combine the information that is required in consent notices with machine-readable standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing.

Indicating Choice for Consent

29184 requires the 'choice' for 'explicit consent' to indicate unambiguously the individual's intentional and affirmative action, and provides examples which include checkboxes, buttons, and slide bars. GDPR similarly requires a clear affirmative act indicating the individual's unambiguous agreement, and provides examples such as checkbox, and choosing technical settings[14]. Both 29184 and GDPR consider inaction, silence, and pre-ticked boxes as invalid mechanisms for indicating choice of consent. The application of 29184 regarding choice of consent differs from two of GDPR's requirements regarding explicit consent which requires the choice to be 'explicit' or be associated with an express statement of consent[15], and regarding ability to provide separate and independent consent for different purposes or elements which necessitates separation of choice associated with them[16] (Rec.43). Both 29184 and GDPR require withdrawal of consent to be as easy as giving consent. Interpretation of GDPR's right to withdraw consent indicates the withdrawal must be the same or as easy as the choice or element used to give consent - such as a checkbox or a button[17].

Record of Notice and Consent

As per 29184, organisations must retain the specific notice (i.e. 'version') used to collect consent so that individuals can access them at a later date. In addition to this, the most recent relevant version of the notice must also be made accessible to the individual. Such versions are to be kept as long as the relevant personal data is being retained. While GDPR does not directly specify that consent notices must be preserved, the requirements for the consent to be demonstrable (Rec.42) and where it is used as a legal basis (Art.6-1a) requires such notices and records of given consent to be maintained by the controller as part of evidence for demonstrating given consent. For cases where personal data is collected without prior

14 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.18-20.
15 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.20.
16 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.12.
17 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.23.

interaction with relevant individuals and where it is difficult for individuals to identify who is processing their data, 29184 suggests using a 'publicly accessible common repository' to provide access to the required information. To the best of our knowledge, and as of October 2020, no such repository currently exists or is in operation, nor does any law or regulation mandate its creation and operation.

Information provided through the Notice

Both the 29184 and GDPR require provision of a notice with specific information in order for the consent to be considered informed and specific[18]. In the following, we will present the minimum information that is required for obtaining valid consent.

Identity of Data Controller

29184 requires notices to provide relevant information regarding the controller, which typically includes the name of the controller along with contact details for inquiries regarding processing of personal data. 29184 also requires notices to provide information regarding the right to lodge a complaint with the supervisory authority. GDPR similarly requires the identity of the controller to be provided along with contact details for inquiries[19] (Rec.42, Art.5-1b), but does not require provision of information related to lodging complaints with the supervisory authority. It instead permits the data subject to lodge a complaint with another supervisory authority which is then responsible for cooperating with the 'lead' supervisory authority (Rec.130).

Purpose

29184 requires the notice to include information regarding the purposes for which personal data will be processed. Purpose descriptions are based on the processing it requires, the personal data categories involved, the existence of third party transfers, and the possibility of risks and impact to the individual. Purposes can be shortened to a name or a short phrase for conciseness, which are then associated through means such as hyperlinks with additional information so as to enable 'meaningful consent'. Each element or category of personal data being collected should be justified with a purpose where the association between purpose and personal data required for it is clearly indicated. Further to this, 29184 requires the purposes to be ordered according to the assessment of plausible risk.

---

18 Providing the consent notice and the information in Art.13 and Art.14 may lead to an integrated approach, however, valid informed consent can exist, even when not all elements of Art.13 and Art.14 are mentioned in a consent request. See also EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p. 16. See also the separately issued WP29 Guidelines on transparency under Regulation 2016/679, as last revised and adopted on 11 April 2018.

19 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.15-16.

GDPR similarly requires provision of information about purposes that are specific[20] (Rec.42, Art.5-1b), but does not require it to be associated or accompanied with additional information such as in 29184. GDPR does however require the purpose to not be vague or generic in order for it to be considered specific[21], with “improving users experience” provided as a non-compliant example. The order of purposes or its presentation are not specified by the GDPR as in 29184.

Personal Data

29184 requires notices to provide information about specific categories of personal data being collected, including where the collection “is obvious” and where generic such as ‘we collect your personal information’ is used. It suggests using the actual value of personal data at the time of collection and where feasible or to provide examples otherwise in order to assist the individual in understanding the collection of personal data and determining their choice in consent. GDPR similarly obliges the controller to provide specific information in the consent notice about the categories of personal data that are collected and processed for each purpose[22] (Rec.42).

29184 specifies that it must be possible for an individual to recognise the necessary and optional categories of personal data for each identified purpose, and to consent separately for the necessary and optional categories. It defines ‘necessary’ personal data as that without which the required processing operations cannot be carried out. The provision of personal data categorised as optional is taken to indicate given consent. In the case of GDPR, separation between ‘necessary’ and ‘optional’ concepts is not present since personal data is instead tied to one or more purpose(s) whose processing is then permitted through consent. Information regarding personal data is encouraged by 29184 to be grouped under categories and ordered according to the highest potential impact to privacy. GDPR does not specify any such requirements on the grouping or ordering of personal data categories.

Data Collection and Source

29184 requires notices to provide clear explanations of the collection methods used to collect each element or category of personal data. 29184 distinguishes between direct (from the individual), indirect (through a third party), observed, and inferred as separate collection methods. Where the same method is applicable to multiple elements or categories, they can be

20 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.13-16. See judgment of 29th July, 2019, Fashion ID, C-40/17, para 89; judgment of 1st October, 2019, Planet49 GmbH, C-673/17, paras 46, 56, 58, 64, 73, 75 and 77. This is also the opinion of Article 29 Working Party Guidelines on consent under Regulation 2016/679, p. 13.
21 See WP 29 Opinion 3/2013 on purpose limitation (WP 203), p. 16.
22 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.15. See also WP29 Opinion 15/2011 on the definition of consent (WP187) p19-20. See also judgment of 1st October, 2019, Planet49 GmbH, C-673/17, paras 51, 61 and 79.

grouped together under a common method - unless one of the categories of personal data has a higher risk of impact regarding privacy. 29184 requires this information regarding when and where the personal data is collected to be provided in the notice, except when the data subject themselves provide the data. Personal data can be provided directly by the data subject (such as responses to a questionnaire), can be observed about the data subject (such as location data collected via an application), can be derived or inferred data such as a profile of the individual that has already been created (e.g. a credit score) and can be made with or without profiling. 29184 requires the controller to include in the consent notice the source from which the controller collected personal data e.g. whether the personal data is directly collected from the data subject or collected from a third party.

Although the GDPR (Art.14-2f) obliges the controller to inform the data subject about the source from which the personal data are collected, and if applicable, whether it came from publicly accessible sources, there are so far no legal sources that explicitly support that the controller is obliged to declare this in the consent notice. It does not oblige providing information about categories of personal data that are inferred or derived from existing ones.

Data Retention Period

29184 requires notices to provide information regarding the retention period and/or the schedule for erasure (mentioned as ‘disposal’) regarding collected personal data. The retention period can be based on: date of collection, occurrence of events, a specific date, or some criteria used to determine the period or schedule. The retention of personal data may be specific to the purpose, and can therefore also be specified per-purpose within the notice. GDPR similarly obliges the controller to provide in the consent notice the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period[23], and further obliges the controller to delete personal data when consent has been withdrawn or invalidated and there is no further lawful basis for processing[24].

Processing of Personal Data

29184 requires the notice to specify information regarding processing of personal data (referred to as ‘method of use’), such as whether the data is used as is or it undergoes processing operations such as derivations, inference, anonymisation, combining with other data, and the use of automated decision-making techniques such as profiling and classification. 29184 recommends inclusion of information regarding transformations applied to personal data before its use. GDPR similarly obliges the controller to provide specific information in the consent notice about the categories of processing of personal data, including information about the use

23 See Judgment of 1st October, 2019, Planet49 GmbH, C-673/17, paras 75, 79 and 81.
24 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.25.

of the data for automated decision-making in accordance with Art.22-2c, the technology or method that is used to process a data subject's personal data as well as a description of the technology, its function and the entity that owns or controls the technology[25].

Whereas 29184 only suggests informing about the existence of automated decision making and profiling, GDPR further requires identifying where such processing produces legal effects for a data subject or similarly significantly affects the data subject (Art.22-2c, Rec.60, Rec.63); and obliges the controller to provide in the consent notice meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject[26].

Data Transfers to Third-Party

29184 requires the notice to specify whether the personal data will be transferred (including disclosure and communication) to a third party 'in the ordinary course of business'. It does not consider a 'processor' to be a third party and does not require information about processors to be provided within the notice. Where personal data is transferred to a third party, the notice should provide the following information 'directly or indirectly': identity of individual or group of recipients, geo-locations of the transfer and whether this entails a change in legal jurisdiction, purposes of transfer, negative impact or risk of impacts caused by the transfer, and safeguards for the transfer.

Although GDPR (Rec.61, Art.13, Art.14) requires providing information regarding recipients or categories of recipients for personal data, it only obliges controllers to provide in the consent request the names of the joint controllers or other controllers that rely on the original consent. GDPR requires providing information regarding recipients or categories of recipients for personal data (Rec.61, Art.13, Art.14). Where such recipients are third parties or act as controllers or joint-controllers, they are required to be named[27]. Similar to 29184, GDPR does not require providing information about processors within a consent notice. Thus, the requirements of 29184 and GDPR regarding data transfer to third parties are compatible with each other. 29184 considers situations regarding third parties and third countries should be

25 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.15. See also WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), paragraph IV.B, p. 20 onwards. See also judgment of 29th July, 2019, Fashion ID, C-40/17, para 77.

26 See Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01), Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018, p. 13, 25 and 26.

27 See judgment of 29th July, 2019, Fashion ID, C-40/17, paras 75, 77, 80 and 81. See judgment of 1st October, 2019, Planet49 GmbH, C-673/17, paras 75, 77, 80 and 81. See also EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 pg. 16.

specified within the same set of requirements regarding the notice, whereas GDPR specifically differentiates between third countries by specifying additional obligations (Rec.101, Art.46).

Transfers to Third Country

29184 requires the notice to specify the geo-location(s) where personal data will be stored and processed, and to specify the legal jurisdictions applicable. which also means that the notice must indicate whether data will be transferred from one geo-location to another geo-location. Organisations are required to determine the appropriate granularity of geo-locations and can consider privacy safeguarding requirements in ISO/IEC 29100:2011.

In contrast, GDPR specifies that when consent is required for personal data to be transferred to a third country or international organisation (Art.49-1-a), the consent notice must provide the names of the countries or the name of the international organisation[28]. Compared to 29184, GDPR does not require providing information about storage locations for personal data when it is located within the jurisdiction of the EU/EEA but requires information when personal data is transferred across legal jurisdictions for third countries, whereas 29184 requires providing information regarding changes in legal jurisdictions only in the context of third party transfers.

Risks of Processing Personal Data

29184 requires organisations to assess the potential risks to the individuals regarding impact to their privacy through mechanisms such as risk assessments and privacy impact assessments, and to identify suitable mitigations and safeguards. Where the potential for the risks is high even after mitigations and safeguards, notices should provide information regarding the risk to individuals where it cannot be (reasonably) inferred from other information already provided to the individual. 29184 recommends placement of risks with related information such as purposes or personal data categories in some cases so as to better understand the impacts of the risk. The assessment of risk is also utilised in the purpose specification and description within the notice, and the ordering of elements according to the potential risk associated with it.

In the case of GDPR, where (explicit) consent is used as the legal basis for data transfers to a third country or international organisation, and where there is an absence of adequacy decisions (Art.45) or appropriate safeguards (Art.46), the consent notice is required to provide information about the possible risks arising from such transfers[29] (Art.49-1-a). Although GDPR considers

---

28 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.16. See Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems Adopted on 23 July 2020, p. 4.

29 This means the data subject should also be informed of the specific risks resulting from the fact that their data will be transferred to a country that does not provide adequate protection and that no adequate safeguards aimed at providing protection for the data are being implemented. See also EDPB Guidelines

risk awareness a principle of data protection (Rec.39) and requires controllers to undertake risk assessments, such as data protection impact assessments (Art.35), it does not require this information to be provided to the data subject within the consent notice. Compared to GDPR, the requirements of 29184 thus make it more pragmatic in making the individual more aware by providing information about potential risks.

Existence of Rights

29184 requires notices to inform individuals, whether directly or indirectly, regarding the rights available to them regarding accessing, rectifying, and deleting their personal data. For rights regarding personal data, the notice should include the method for requesting access, specific categories of personal data that can be accessed, method for challenging accuracy and completeness of data and amending it, information required to authenticate the identity of the individual as authorisation, time limits for completing the request, and the existence of fees charged for the request (if any). The notice is also required to list circumstances where personal data cannot be altered or deleted. Where consent is used as a legal basis and its revocation is feasible or required by law, the notice must provide information regarding the revocation or withdrawal of consent. In comparison, although Art.13 and Art.14 of the GDPR obliges the controller to provide the data subject information about data subjects' rights as provided under Articles 15 to 22, there is so far no legally binding requirements or guidelines that require this information to be provided directly in a consent notice, except for the right to withdraw consent at any time and how this right can be exercised[30].

Conclusion

The comparison shows that 29184 and GDPR have similar requirements, and that 29184 meets these in several cases. However, 29184 fails to meet two important requirements in GDPR regarding 'freely given' consent and use of 'explicit consent' as a legal basis. We therefore conclude where 29184 is used to demonstrate conformance with many of GDPR's requirements regarding notice and consent, organisations using it must additionally also ensure that they meet the other requirements and obligations regarding GDPR not covered by 29184. If these drawbacks are addressed, the use of 29184 can aid in the demonstration of compliance with the requirements of GDPR and can also act as a certification mechanism for organisations.

05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p. 16. See also Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 Adopted on 25 May 2018, p. 7. See also Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems Adopted on 23 July 2020, p. 4.

30 See EDPB Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020 p.18-20.

At the same time, it is also important to note that apart from the above mentioned drawbacks, the requirements in 29184 go beyond those of the GDPR in several areas, such as providing specific requirements regarding the understandability of notice and ordering of information within it based on impact to the individual. 29184 also has additional requirements involving comprehension and provision of risks to the individual as compared to GDPR. Apart from these, 29184 provides novel suggestions regarding use of machine-readable notices and a public repository for providing access to information, as well as the use of a standardised format for documenting consent with the example of the Consent Receipt standard.

Funding Acknowledgements

Harshvardhan J. Pandit is funded by the Irish Research Council Government of Ireland Postdoctoral Fellowship Grant#GOIPD/2020/790, by European Union's Horizon 2020 research and innovation programme under NGI TRUST Grant#825618 project "Privacy as Expected: Consent Gateway", and by the ADAPT SFI Centre for Digital Media Technology, which is funded by Science Foundation Ireland through the SFI Research Centres Programme and is co-funded under the European Regional Development Fund (ERDF) through Grant#13/RC/2106.