Conditions for Explicit Consent in Web Forms

Bud P. Bruegger, ULD <uld613@datenschutzzentrum.de>

Purpose

This document contributes to project-internal discussion.

Objective

While the requirements for valid consent are already high in the GDPR, situations as those described in Articles 9 and 22 require an even more demanding form of consent called "explict consent". In its Guidelines on Consent[1], the Article 29 Data Protection Working Party uses the term "regular consent" to refer to a form of consent that is valid according to Articles 4(11) and 7 but fails to reach the level of "explicit consent". The same guidelines also discuss the conditions of how to reach the level of "explicit consent" in section 4 "Obtaining explicit consent".

While the conditions for reaching regular consent according to the GDPR are relatively clear, the present paper attempts to further clarify the considtions necessary to reach the level of explicit consent.

Approach

The paper takes a partly differential approach, assuming that the conditions for a valid consent according to the GDPR are already met and focusing on the additional conditions that are necessary to reach the level of explict consent.

Scope

While the Working Party's guidelines provide examples of explicit consent using various media including phone conversations and written consent, this paper focuses exclusively on web forms.

Proposed Conditions

The paper proposes that the following additional conditions are necessary and sufficient to achieve a level of explicit consent:

(1) The dialog that confirms consent is **separated** from other dialog such that it exclusively deals with the collection of consent and refrains from serving any other function.

(2) If consent is asked for multiple independent purposes, multiple **separate** consent dialogs for a single purpose are used.

(3) The dialogs are **explicitly marked as "consent"**.

(4) The consent dialog shall state **who** processes **what data** for **what purpose**. If the processing entails automatic decision making, this has to be clearly indicated. When

1 Article 29 Data Protection Working Party, WP259 rev.01, Article 29 Working Party Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, last Revised and Adopted on 10 April 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (last visited 14/03/2019).

processing entails transfer of data to a third country without adequate level of protection, the potential risks and the taken appropriate safeguards need to be described.

(5) The dialog element that captures the user's consent has **three states**: ['yes', 'no', 'unfilled'] with default setting being "unfilled".

(6) The right to withdraw consent must be stated. The information on how users can withdraw consent should be available at least as as a link or pop-up window.

(7) Optionally, the consent dialog captures confirmation or evidence that the user who provides the consent meets the conditions that are required in order for the consent to be valid.

Example

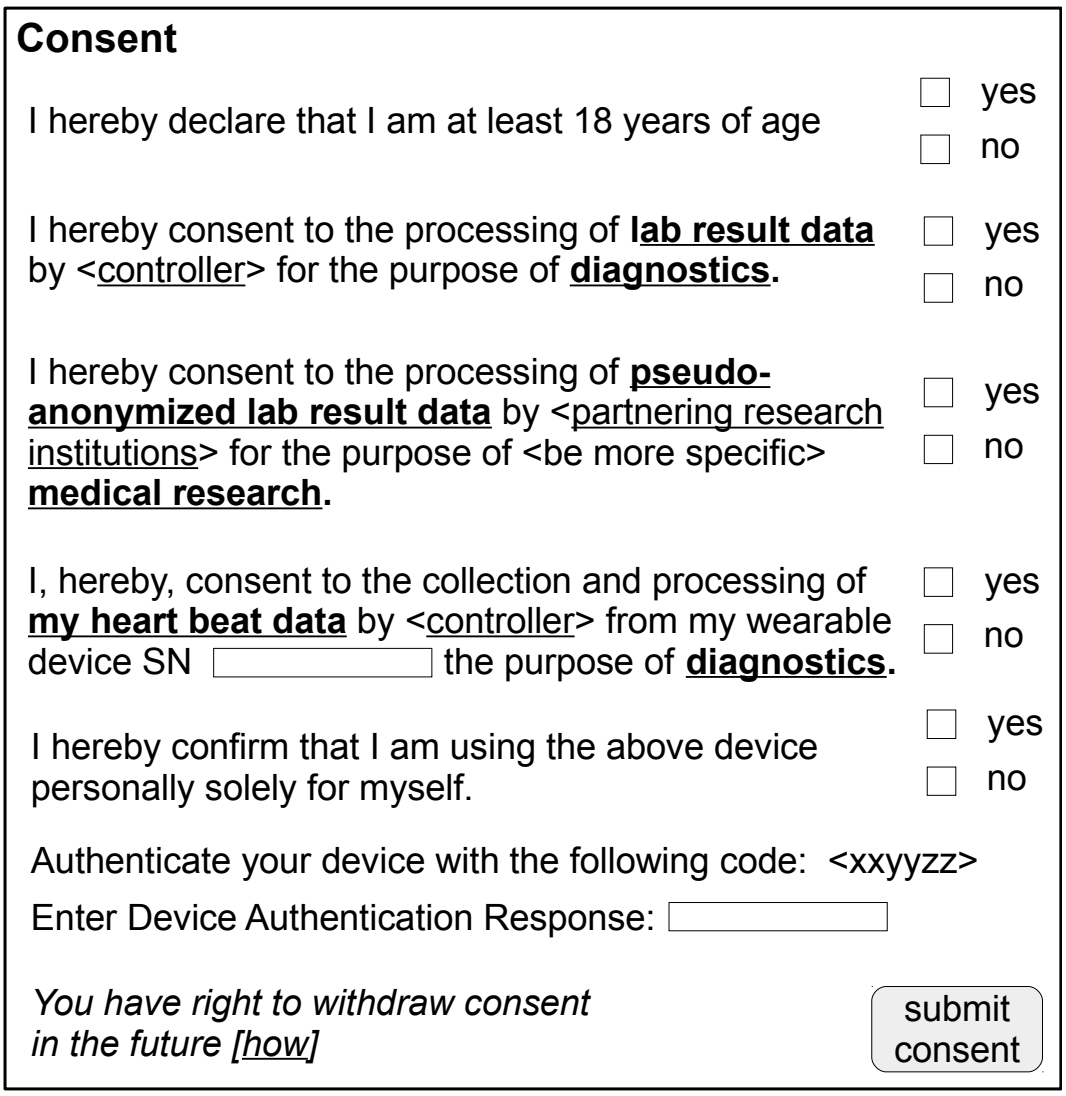

Figure 1: An example for an explicit consent form.

If the web page contains other input fields, the "submit button" shown in Figure 1 would be outside of the consent section.

Discussion

The following provides details and rational for the proposed conditions.

(1) The separation of the consent dialog from other input areas and functionality renders the consequences of input clearer to users and avoids any interference from other aspects of the web page.

This is also consistent with the requirement stated for consent in general in the Working Party's guidelines on page 14: "*Likewise, if consent is requested by electronic means, the consent request has to be **separate and distinct**, it cannot simply be a paragraph within terms and conditions, pursuant to Recital 32*". (Highlighting added by the author).

It is particularly important to clearly separate user actions that express consent from those that are used to control the workflow and navigation of pages. If a user action serves for both, giving consent and advancing to the next step of the workflow, it cannot be clear whether the user really gave consent or solely wanted to move ahead.

(2) To ask consent for each purpose individually is mandated in recital 32(5) of the GDPR: "*When the processing has multiple purposes, consent should be given for all of them*". The separation of consent for independent purposes creates the clarity to users necessary to express their consent. A possible bundling of independent purposes into a single consent decision would constitute a manipulation XXXX.

The separation of consents is also clearly required by the guidelines in section "3.1.3. Granularity": "*A service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR*".

(3) Making explicit that consent is requested brings the necessary clarity about the consequences of their actions to users. This is stated in the Working Party's guidelines in [Example 17] on page 19: "*..provided that the text clearly indicates the consent, for instance '**I, hereby, consent to the processing of my data**', and not for instance, '**It is clear to me that my data will be processed**'*". (Highlighting added by the author).

(4) **Who** processes which **data** for which **purposes** covers the three most important pieces of information that are necessary to render the consent "informed". This corresponds directly to the following three pieces of required information stated in the Working Party's guidelines in section "*3.3.1. Minimum content requirements for consent to be 'informed'*": "*(i) the controller's identity, (ii) the purpose of each of the processing operations for which consent is sought, (iii) what (type of) data will be collected and used*".

The additional information elements listed there either don't apply to an individual consent element or are necessary only in specific cases.

In particular, "*(iv) the existence of the **right to withdraw consent***" applies to multiple consents and doesn't require any decision on part of the user.

Similarly, "*(v) information about the use of the data for **automated decision-making** in accordance with Article 22 (2)(c) where relevant*" and "*(vi) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46*" have to be stated only for matching kinds of processing.

Since this information has to be presented "in an intelligible and easily accessible form" (Art. 7(2) GDPR), the consent declarations need to be kept short. Consequently, the controller can only be named without providing details such as address or contact points (like the DPO); the data can only be described with a few words, without possibility to state individual data elements; and also the purposes are restricted in size to a few words without possibility to providing details. In all these cases, a fully informed consent decision by the data subject may require additional detail. This is discussed in the following.

There are different methods of providing additional detail of the **data** that is processed. Where the data is not collected on the same web page that includes the consent dialog, this can be achieved by a pop-up dialog and/or a link to an additional page. The additional information can for example list the individual data elements. In other cases, such as the "pseudo-anonymized data of lab result data" in Figure 1, an explanation of the used term "pseudo-anonymized" and a description of the possible risks of re-identification are necessary.

Where the data is collected with form input fields on the same page, and if different subsets are used in different consent decision dialogs, the input fields could for example be grouped in named sections to permit the use of those names in the consent dialog.

While not strictly required for explicit consent, a pop-up dialog for the data would be also a good place to provide information about the storage period and when the data will be deleted.

Providing additional detail on the **controller** can again be achieved through pop-up dialogs and/or links. In addition, contact e-mail addresses of DPOs could be rendered clickable[2].

In the case where categories of recipients are named as controllers, the detail should include every individual controller. While Art. 13 and 14 GDPR require only to provide "categories of recipients", the example in Figure 1 asks the users to provide consent for the processing by those recipients. Consent is only informed if the data subject is informed about the controller.

Pop-up dialogs and links can also provide additional information about **purposes**. In addition to a longer and thus more precise description of the purpose itself, it would also be possible to justify why the collected data are indeed necessary to achieve them.

(5) The Working Party's guidelines, in [Example 17] describe an explicit consent dialog that has both, a *Yes* and a *No* check box. Compared to a solution with only a *Yes* check box, this makes it explicit that it is possible to chose *No* and thus withhold consent. Leaving both check boxes unchecked as default avoids to influence the choice in any way and present both options on an equal footing[3].

(7) In the cases where the subject who consents to the processing needs to fulfill certain conditions in order for the consent to be valid, this should also be integrated in the consent dialog.

This topic hasn't been discussed in the Working Party's guidelines. More feedback from legal specialist is necessary here. One key question is for example, what level of non-repudiation is required to make declarations legally meaningful.

The following lists some examples:

2 Through the use of mailto: ULRs.

3 Obviously, if *Yes* was checked by default, it would fail to constitute valid consent since it is then given without an affirmative action.

(i) According to Art. 8(1), a minimal age is required from a persons in order for their consent to be lawful.

(ii) According to Art. 8(1), an adult can give consent for a child only if that person is the holder of parental responsibility.

(iii) m-health devices typically collect personal data of their wearer. In the cases where the device itself is incapable of conducting a consent dialog itself, another channel such as a web page can be used to collect consent. In this case, the consent is only valid if the person providing the consent is the person wearing the device. Devices that operate in such scenarios may offer technical means to provide proof (or at least evidence) that the person filling in the consent dialog has physical control over the device. In Figure 1 this situation was represented by a challenge and response dialog.