

February 23, 2017

## Consent as a mechanism for justifying the process of personal data

Under the Dutch Personal Data Protection Act (the DPA) consent is one of the six legal grounds to process personal data. Without a legal ground it is not allowed to process personal data. Consent will be a legal basis of processing data under the General Data Protection Regulation (the GDPR) too. Consent is contained in different parts of the GDPR. This second Boekel GDPR update deals with the differences between (i) the legal framework of consent and (ii) the conditions for valid consent under the DPA and the GDPR.

## The legal framework related to consent

Consent under the DPA is based (word-for-word) on consent as defined in the EU Directive 95/46/EC (the Directive):

"The data subject's consent means: any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

The legal framework consists of several broadly interpretable terms creating legal uncertainties. As a consequence an independent advisory and consultative body consisting of European privacy supervisors, the Article 29 Working Party (the WP29), provided a thorough analysis of the concept of consent in July 2011. Its opinion explains certain key elements of the legal framework related to consent. These are (and remain) important guidelines on how the EU data protection regulators interpret the concept of consent. In short:

- Consent must be freely given. This means the data subject must not consent: he or she has a real choice meaning that there is for instance no risk of intimidation or perceiving deception. If the data subject is under the influence of the data controller (e.g. his/her employer or a public authority) consent is not generally considered to be freely given due to the nature of the relationship.
- Consent must be specific. Blanket consent without determination of the exact purposes is not acceptable. Consent should refer clearly and precisely to the scope and the consequences of the data processing. Specific consent clauses should be separated from general terms and conditions.
- Consent must be informed. According to articles 33 and 34 DPA, the controller has to provide the data subject with certain minimum information about the processing. The information provided needs to be sufficient to ensure that the data subject can make well-informed choices. With regard to the quality of the information, the way in which the information is given must ensure the use of language for the data subject to understand. Complicated legal

jargon is not considered appropriate.

- Furthermore, the information provided has to be clear and sufficiently conspicuous so that the data subject cannot easily overlook it. Additionally, information must be provided directly to the data subject, an indication of the place to find information (for instance 'somewhere' on the internet) is not sufficient.
- Consent should be read together with further requirements mentioned in the DPA. Processing based on consent requires consent to be unambiguous. The indication by which the data subject signifies must leave no room for ambiguity regarding its intent. There is ambiguity in case of reasonable doubt.
- According to the WP29 unambiguous consent does not fit well with procedures to obtain consent based on inaction or silence (e.g. no pre-ticked boxes).
- Consent must be explicit in case of processing special categories of data (e.g. health data). An active response of the data subject is required.

## Legal framework on consent under the GDPR

Article 4 (11) GDPR outlines consent as:

"consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

From this new legal framework it appears that the European legislator responded to certain changes proposed by the WP29 in its overall assessment of the framework. As the concept of consent under the Directive has been transposed word-for-word in the DPA, there are not many modifications from a Dutch law perspective (that is in contrast to certain other EU member states). The definition has become more prescriptive, but most of it was already required and is not new. The most significant change is that:

- Consent must be given by statement or by a clear affirmative action. Action of the data subject is actually required. Included is for instance ticking a box and choosing specific technical web browser settings. Pre-ticked boxes (in-activity) shall therefore not constitute consent.

According to the analysis of the WP29 it seemed that action of the data subject was needed for consent, now it is certain that it is needed. This requires organisations to rethink the way in which they currently obtain consent from data subjects.

## Conditions for valid consent under the GDPR

Article 7 of the GDPR stipulates conditions for valid consent, something that was not specifically stipulated in the DPA. One of the conditions for valid consent is that the controller must be able to demonstrate that the data subject has indeed consented to the processing of his or her personal data. A written declaration is not required but would be recommended, given that the burden of proof is being placed on the controller. Adequate logging of consent given online (e.g. through contact forms on websites) should be the standard.

If the data subject's consent is given in the context of a written statement which also concerns other matters, the request for consent must be clearly distinguishable hereof. The written declaration must be presented in an intelligible and easily accessible form, using clear and plain language. If the information is not provided in line with this provision,

consent may not be valid.

As under the DPA, the data subject has the right to withdraw his or her consent at any time. It shall be as easy to withdraw consent as it is to give consent. What is new, is that the data subject must be informed of its right of withdrawal prior to giving consent. In addition, the data subject must also be informed about the fact that withdrawal does not affect the processing of personal data based on consent before withdrawal. This requires not only the rewriting of privacy policies but may also require organisations to change their internal processes ensuring that the withdrawal of consent is as easy as giving it.

## Consent of children

Specific rules on consent apply to children in relation to information society services (in short: all services offered online, whether for free or paid, including social media). The rationale behind this is that children should be given additional protection because they are generally less aware of risks, safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should apply to the use of personal data of children for the purposes of marketing or creating personality/user profiles, and the collection of personal data of children when using services offered directly to a child. Any information and communication should be in such a clear and plain language that the child can easily understand.

Processing on the basis of consent shall only be lawful where the child is aged over 16 years. If the child is below this age processing on the basis of consent shall only be lawful if consent is given (or authorised) by the holder of parental responsibility over the child. Individual EU member states are allowed to provide for a lower age thresholds, but not below 13 years. The Netherlands will not provide for a lower age (according to the legislator there is no reason to change the current situation). Organisations operating throughout the EU which process personal data of children on the basis of consent should be aware of individual EU member state legislation in this respect.

With regard to other data subjects lacking legal capacity, the Dutch Implementation Act on the GDPR (the Implementation Act) stipulates that data subjects placed under guardianship (curatele) or under a protection order (mentorschap), also require consent from their legal representatives (and consent can be withdrawn by the legal representative).

The controller shall make reasonable efforts to verify that consent is actually given or authorised by the legal representatives, taking into consideration available technologies.

## Organisations currently relying on consent to process personal data

Recital 171 of the GDPR states that:

"Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. (...)"

The main rule is that it will not be necessary for organisations to reobtain consent when consent has been obtained in line with the conditions of the GDPR. However, it is not entirely clear whether or not consent obtained under the DPA,

which is not obtained in conformity with the GDPR, will be no longer valid beyond 25 May 2018. It can be argued that the European legislator values the continuity of processing most: “so as to allow the controller to continue such processing after the date of application of this Regulation”. On the other hand, the specific wording of Recital 171 (“Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after” and: “if the manner in which the consent has been given is in line with the conditions of this Regulation”), points towards the conclusion that consent should be reobtained.

As part of the consultation of the Implementation Act questions on this point were posed to the Dutch legislator. Further clarification might be included in the next version of (the explanatory memorandum to) the Implementation Act.

## Practical recommendations

Organisations relying on the consent of data subjects as a lawful basis for processing activities are recommended to check if the current consent is obtained in line with the requirements of the GDPR. If not internal processes should be aligned with these requirements and the controller should consider requesting renewed consent in accordance with the GDPR requirements (to avoid the risk that consent will no longer be valid after 25 May 2018). Additionally, organisations should put in place mechanisms to demonstrate valid consent, and to ensure that consent can be easily withdrawn.

Organisations could further consider if other (perhaps more appropriate) legal grounds of processing are available and desirable.

Organisations failing to comply with the new obligations, risk severe administrative fines from the Dutch data protection supervisory authority (de Autoriteit Persoonsgegevens), and other regulators in EU countries where they are active.

## Overview of subjects

January 2017	Territorial scope of the GDPR (Dutch)
February 2017	The Concept of Consent
March 2017	Sensitive Data
April 2017	Accountability, Privacy by Design and Privacy by Default
May 2017	Rights of Data Subjects (information notices)
June 2017	Rights of Data Subjects (access, rectification and portability)
July 2017	Rights of Data Subjects (erasure, restriction, object and automated individual decision-making)
August 2017	Data Processors
September 2017	Data Breaches and Notifications
October 2017	Data Protection Officers
November 2017	Transfer of Personal Data (outside the EEA)
December 2017	Regulators (competence, tasks and powers)
January 2018	One Stop Shop
February 2018	Sanctions
March 2018	Processing of Personal Data in Employment Context

## Your Key Contacts



**Marc Elshof**

Partner, Amsterdam

D +31 20 795 36 09

M +31 6 46 37 61 08

[marc.elshof@dentons.com](mailto:marc.elshof@dentons.com)



**Celine van Es**

Associate, Amsterdam

D +31 20 795 31 22

M +31 6 11 16 30 45

[celine.vanes@dentons.com](mailto:celine.vanes@dentons.com)