ICTRECHT

Legal assessment of CAcert / Oophaga

CAcert.org is a community-driven certificate authority that issues certificates to the public at large for free. CAcert is incorporated in Australia as CAcert Inc. Some servers that support the CAcert operation are owned and operated by the Dutch Oophaga Foundation. Oophaga is owner of the equipment and provides hosting for CAcert services. CAcert has sole access to the data stored on this equipment. This data is secret to Oophaga.

Below, a legal analysis is presented of the applicable legal obligations for Oophaga and CAcert to comply with Dutch and European privacy regulations, in particular the Dutch Data Protection Act and how to address these.

European privacy framework

The European legal framework for privacy is built around the Data Protection Directive 95/46/EC of 24 October 1995. This Directive was incorporated into Dutch law as the Data Protection Act of 6 July 2000. While the Directive by itself is not binding law, Dutch law must be interpreted in accordance with the Directive.

Are certificates "personal data" under European privacy law?

First, some definitions from the Dutch Data Protection Act (DDPA) regarding the purpose of the privacy framework.

> Article 1(a): "personal data" shall mean: any information relating to an identified or identifiable natural person;
>
> Article 1(b): "processing of personal data" shall mean: any operation or any set of operations concerning personal data, including in any case the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure or destruction of data;

The first two definitions in particular are extremely broad and this is explicitly the point. The Directive was designed to cover any processing of any kind of data about natural persons. It does not matter whether an actual name or government ID is included. Data becomes personal as soon as there is any kind of trace back to the natural person behind it.

What personal data is present in certificates?

CAcert collects identifying information of its community members and stores this data to issue and manage certificates. The CAcert Community Agreement provides the following definitions:

> "Community" means all of the Members that are registered by this agreement and other parties by other agreements, all being under CAcert's Arbitration.
>
> "Member" means you, a registered participant within CAcert's Community, with an account on the website and the facility to request certificates. Members may be individuals ("natural persons") or organisations ("legal persons").

To obtain a certificate, a community member has to fill out CAcert's Identity Verification Form (CAP) form. This form calls for the person's exact full name as given on government-issued ID or IDs, an e-mail address and the person's date of birth. The data in the form must be confirmed by a CAcert Assurer.

A certificate as issued by CAcert includes the person's full name as assured in the CAP form and e-mail address. These items can be traced back to the entity to whom the certificate relates. Indeed, that is the very point of a certificate: it provides a person's name as well as assurance administration to bind a person to this name. In the case of CAcert certificates, this administration is based on government-issued ID presented by the person to a CAcert Assurer. It is also possible to obtain a CAcert-issued certificate without a full name.

Some certificates may be issued only in the name of a legal entity which is not a natural person. Such certificates are not "personal data". However, those certificates that identify a natural person, even if only by pseudonym, are covered under the definition of "personal data" under the Directive and the DDPA. The same goes for the data that is stored in the community member database managed by CAcert.

Is CAcert subject to Dutch privacy law?

The DDPA further provides this definition:

> Article 1(d): "responsible party" shall mean: the natural person, legal person, administrative body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal data;

CAcert is a legal person (legal entity). It determines how certificates are issued, managed and made available and therefore is the "responsible party" according to this definition.

As CAcert is incorporated outside the European Union, it would seem this Directive nor the Dutch Act applies to it. However, the involvement of Dutch foundation Oophaga changes things. The Dutch Act puts non-EU entities under Dutch jurisdiction under certain circumstances:

> Article 4(2): This Act applies to the processing of personal data by or for responsible parties who are not established in the European Union, whereby use is made of automated or non-automated means situated in the Netherlands, unless these means are used only for forwarding personal data.

The Oophaga servers store personal data regarding CAcert community members, such as their names and dates of birth, together with the serial numbers of their certificates. This personal data is stored on behalf of CAcert and is encrypted so that Oophaga personnel cannot access it. CAcert uses this data for certificate issuance for community members and for dispute resolution.

These actions fall under "processing" in the broad definition given above. The processing in question is physically done on servers that reside in the Netherlands. Hence these automated means situated in the Netherlands do more than only forwarding personal data. This puts CAcert under Dutch jurisdiction with regards to the data it stores and processes using the Oophaga servers.

Oophaga is providing these means, but is not actually processing the data itself. In fact it cannot process the data as it is encrypted and all operations are performed by CAcert

operatives. Hence Oophaga is not a “processor” in the sense of article 1(e) of the DDPA (a person or body which processes personal data for the responsible party, without coming under the direct authority of that party).

What obligations does CAcert have under Dutch privacy law?

CAcert has several obligations under the DDPA. The most important obligations have to do with notification to the authorities.

Notification of Dutch proxy

The primary obligation for CAcert is given in article 4(3) of the Act:

> The responsible parties referred to under (2) are prohibited from processing personal data, unless they designate a person or body in the Netherlands to act on their behalf in accordance with the provisions of this Act.

In other words, CAcert has to designate a proxy. The most logical person or body to designate is Oophaga, although this is not strictly necessary. The only legal requirement is that the proxy is physically residing in the Netherlands.

Notification of goals and methods of processing

In addition, CAcert has to comply with the basic rule of notice regarding goals and methods of processing. To this end, the Dutch person designated by CAcert must notify the Dutch Data Protection Commission (article 27 and 28 DDPA) of the following particulars:

a) the name and address of the responsible party;

b) the purpose or purposes of the processing;

c) a description of the categories of data subjects and of the data or categories of data relating thereto;

d) the recipients or categories of recipients to whom the data may be supplied;

e) the planned transfers of data to countries outside the European Union;

f) a general description allowing a preliminary assessment of the suitability of the planned measures to guarantee the security of the processing, in application of Articles 13 and 14.

Although article 29 DDPA provides a number of exceptions for types of processing that do not have to be notified to the DDPC, none of these exceptions apply to CAcert’s processing.

General obligations

Of course CAcert also has to ensure that its processing of certificate data (at least that data processed using Oophaga servers) complies with the general obligations on lawful data processing.

The general rule is, according to article 7 DDPA, that personal data may only be collected for specific, explicitly defined and legitimate purposes. This rule can be satisfied by providing an explicit privacy policy that spells out what happens with personal data that natural persons provide as part of the certificate application and assurance process, and what happens with the certificates containing some or all of this personal data. However, at this time CAcert does not have such a privacy policy. It is strongly recommend to introduce one as soon as possible.

Article 8 DDPA further specifies that the subject (the person to whom the certificate is issued) must have unambiguously given his consent for the processing. This consent is obtained during the CAcert application process: when a person requests a certificate from CAcert, he has to sign the Application Programme form (CAP) which states that the provided information (full name as taken from a government-issued identification document and birth date) is correct and the person agrees with the CAcert Community Agreement (CCA).

Related obligations are spelled out in articles 9-15 of the DDPA. It would go too far in the context of this assessment to discuss these in detail.

What happens if CAcert fails to comply with these obligations?

If CAcert fails to appoint a person or legal entity as its proxy in the Netherlands, it is forbidden from processing any data. In practice, this means that the Dutch Data Protection Commission (DDPC) can demand that Oophaga takes the relevant servers offline or removes all CAcert data from it. If necessary, the DDPC can impose a penal sum or performance bond to enforce its demands.

For failure to notify the DDPC of the processing undertaken by CAcert, a fine of EUR 4500 can be imposed (article 66 DDPA).

Regarding the general obligations of lawful processing of the personal data, there are little to no legal sanctions available for the DDPC. As with failure to appoint a proxy, the DDPC can demand that CAcert ceases certain kinds of processing, on penalty of a performance bond. See article 65 of the DDPA:

> The Commission is authorised to apply administrative measures of constraint pursuant to the obligations laid down by or under this Act.

As part of these administrative measures the DDPC can demand information from CAcert to e.g. explain how the personal data is secured against unauthorized access. The DDPC can however not demand copies of this data or access to the security systems or to force CAcert to grant Oophaga access to the data.

In particular, there is simply no provision in the Data Protection Act to make a request for access to the private signature keys. An inspection of the Oophaga systems might include a request for information about the procedures and security protocols surrounding the personal data stored on these systems, but this request only needs to be fulfilled insofar as is necessary to reassure the DDPC that the security is sufficient (article 13 DDPA).

The private signature keys have nothing to do with the security of the personal data on the Oophaga servers. Handing over a copy of the private signature keys is out of the question.

Bottom line

CAcert collects identifying information of its community members and stores this data to issue and manage certificates. This information qualifies as personal data under European privacy laws. CAcert is responsible for the processing of this personal data and the consequences thereof.

CAcert is bound by Dutch law with regards to the personal data that is processed using the Oophaga servers. In practice, this means CAcert must appoint a Dutch proxy and notify the

Dutch Data Protection Commission about the goals and methods of processing certificates. In addition, CAcert must draft an explicit privacy policy that details the processing of personal data and publish this on its website.

Should at some point in time the DDPC find that CAcert's processing somehow violates Dutch or European privacy laws, then it can force CAcert or Oophaga (only if CAcert does not cooperate) to cease such processing or adapt the processes.

There is no basis in law for the DDPC to demand opening up of its secure systems, let alone for access to the private signature keys.

Arnoud Engelfriet, Dutch IT lawyer – 20090607