VOICE: EXPLAINED

WHAT YOU NEED TO KNOW ABOUT VOICE AND THE PRIVACY LEGISLATION

FEBRUARY 2020

1. Intro

Since Apple introduced the Siri speech assistant in 2011, speech technology has grown rapidly. The market share of the assistants of Amazon, Samsung and Google, in particular, is steadily increasing in Europe. Voice is rapidly becoming a full-grown communication channel between organisations and consumers. Innovative organisations want to start with this, and this raises legal issues. As a trade association, the DDMA sees it as its task to share the knowledge of early adopters and to remove legal obstacles as much as possible. This way we can accelerate the privacy-friendly implementation of this technology. In this manual you can read how voice works and what the most important privacy issues are.

1.1 What is voice

Voice is the collective name for all speech assistants that ensure spoken interaction between the consumer and an organisation. Examples of well-known speech assistants are Siri (Apple), Alexa (Amazon), Google Assistant (Google) and Bixby (Samsung). Users can talk to the assistant using their telephone, smart speaker, smart TV or other devices with voice functionality. The consumer can operate the provider's services with spoken instructions. This includes making agreements, operating the lighting or having a weather report read out to you.

It is an interesting development for Dutch organisations that providers open their voice channels to third-party voice applications. Providers use different names for their voice applications: Google calls them Actions, Amazon calls them Skills, Samsung has Capsules and Apple users talk about Shortcuts.

A voice application offers an organisation the opportunity to let end users talk to your organisation. The organisation has full control over the assignments that can be performed, or the questions that can be asked and the answers that the assistant offers. These make it possible, for example, to request a bank balance,

information about products or make online purchases through the voice assistant.

In addition to voice applications, we can also talk about voice searches. Where voice applications, such as an 'action', speak of a native experience that is completely designed by the organisation, voice search is about the answers that the assistant chooses on generic questions that the user asks. Think of questions such as "What is the nearest filling station?" or "How late is the supermarket open?"

1.2 How does a speech assistant work?

To be able to make a legal assessment, it is important to understand how a speech assistant works. An interaction with a speech assistant works roughly as follows:
1. The user calls up the speech assistant by calling the "keyword" as "hey Google", or using a dedicated button or some other trigger
2. The user delivers his message
3. The speech assistant uploads the message to a cloud platform
4. The audio of the message is converted into written text using automatic speech recognition, possibly with metadata such as who the speaker is. The latter is done through voice recognition.

5. The written message is analysed by the language model (natural language processing) to extract the intention of the user from the message.
6. The expected intention is matched by the provider with a possible solution or answer for the purpose of the user
7. The answer is converted from written text to spoken audio via text-to-speech (or see 9)
8. The user hears the answer through the voice assistant's voice
9. The user sees the result of the given instruction in a text display

SMART SPEAKER   ASSISTANT   ASR   NLP   TTS   INTENT MATCHING
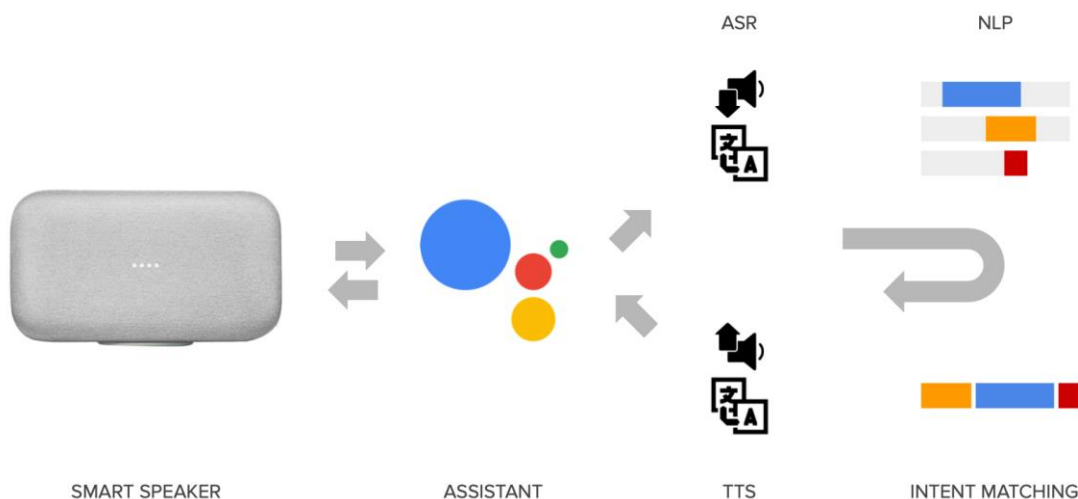
1.3 Reason for this document

The DDMA has had a Voice Taskforce since 2019, which has the leading Dutch voice experts at the moment. They have experience in guiding and executing voice trajectories at large organisations, and thereby point out that there is still much uncertainty in the area of privacy. A lot is possible, but it is important that legal colleagues are involved in the project in time. Those legal experts also need information. How does voice work, and what are the most important privacy issues? With this document from the Explained series, a collaboration between the Voice Taskforce and the legal counsels of the DDMA, we want to take the sector further with the use of voice as a marketing channel and to remove potential obstacles.

Note: the development of channel voice is in full swing, which may mean that the information in this document is out of date. We will do our best to keep the document up-to-date, but make sure you also check the date on the front page.

1.4 What will the voice landscape look like in 2020?

Some of the well-known speech assistants are Siri (Apple), Alexa (Amazon), Google Assistant (Google) and Bixby (Samsung). At the time of writing, the Google Assistant is by far the largest one in the Netherlands. This is mainly due to the availability of the Dutch language since July 2018. The competitor, Alexa, is not yet available in Dutch. See an overview of the most relevant parties for voice in 2019 below:

Brands

Agencies
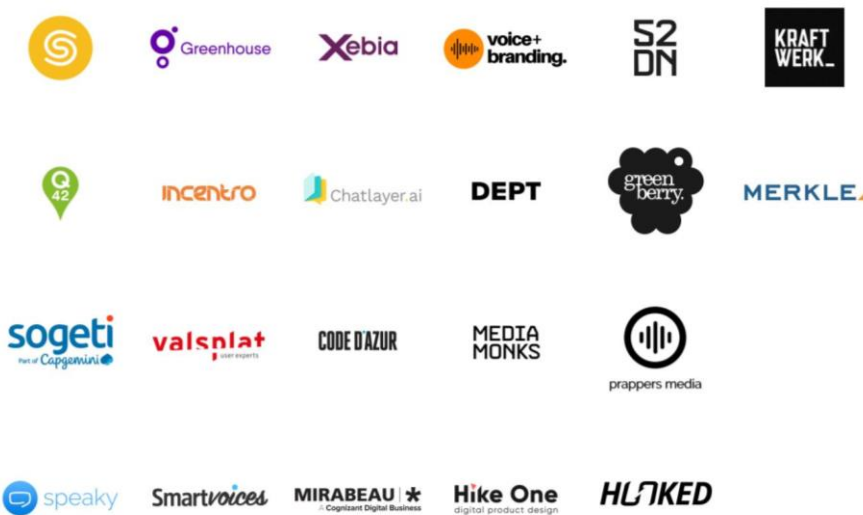
1.5 The scope of this manual: Google Assistant

As Google is by far the largest in the Netherlands, we have decided to only look at the Google Assistant in this manual for the time being. This way we prevent this document from becoming a general description for all services, which is not specific enough to make the provider-specific points of interest clear. Here we focus on the Voice Applications aspect (Google: Google Actions) of the Voice landscape. As the market continues to develop and other voice assistants develop a position on the Dutch market, we will update this manual.

1.6 Abbreviations and terms

Providers – Platforms that offer a voice assistant. *Amazon, Apple, Google, Samsung.*
Organisation – parties that communicate with their target group via the voice channel. *For example Centraal Beheer, Philips, KLM, Rabobank.*
Agencies – Service providers who assist with the realisation of voice applications or the presence of Providers' platforms. *For example 52DN, Greenhouse Group, Merkle, Nodes, Q42.*

2. This way you involve legal personnel in a voice trajectory

2.1 This is how you involve the legal department in time

To involve colleagues from your legal department, it is important that the legal experts know what voice means. They must be able to assess how compliance must be regulated with relevant legislation, including the GDPR. That is only possible if the legal experts understand how it works. Involve your legal colleagues in time. Make sure that they join in with the first meetings and that they are aware of why you want to introduce voice.

2.2 Share documents with explanations

There are several documents that you can share with your legal colleagues to explain to them how voice works. Share these documents in time so that they can delve into it before a legal assessment has to take place. Think of:

Google Enterprise agreement

If you publish your action with Google, you fall under the Google Cloud Agreement by default. To prevent the data from being used by Google for advertising and optimisation purposes, it is recommended for you to conclude an Enterprise Agreement. In many cases this is also a must from a legal point of view and reviewing this (framework) agreement takes a lot of time.

Roadmap

Share a roadmap with your legal department. Where do you start and what is the point on the horizon that you are working towards? And why are you doing this? Do you see it as a pilot programme or as a full replacement of your current channels? A roadmap helps to make your future plans transparent. This way you ensure that the legal assessment becomes clearer.

**2.3 Provide a process description**

Before your legal department can assess what needs to be arranged, it is important that the voice process is clear. The End User also has an agreement with the Provider, and in many cases also uses a device from the Provider for this. For example the Google Home smart speaker.

As an organisation, you also make agreements with the Provider yourself. You communicate with customers through the Provider's channel. As a result, personal data is processed by the Provider, which often involves sensitive information such as bank or health data.

Because of the applicable privacy legislation, it is important that it is clear:
- what is the role of the Provider's GDPR and of your own organisation
- whether the Provider also processes the data for its own purposes
- where the data is stored, and whether it is outside the EU
- which storage periods the Provider applies
- where the consumer can go for inspection, removal and other GDPR rights

3. What you need to know about voice and privacy legislation
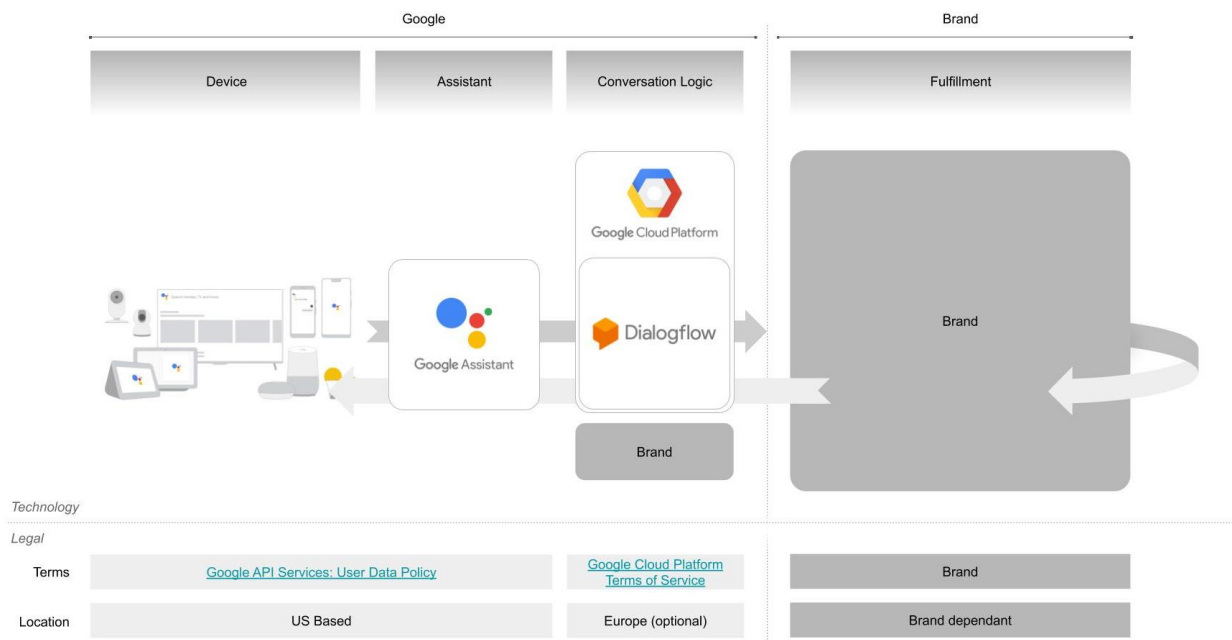
3.1 Applicable legislation

In order to know which privacy rules apply to voice, it must first be determined which legislation applies. Every organisation must comply with European and national legislation. For some sectors, additional obligations may apply from sectoral legislation or self-regulation.

GDPR: When using voice as a communication channel between your organisation and the customer, the processing of personal data is inevitable. A device (telephone or smart speaker) is linked to an individual through an account login. It is also often possible to deduce from conversations who are concerned. The GDPR applies as soon as your personal data is processed.

Telecommunications Act: The provisions on spam may apply once unsolicited text or voice messages with commercial content are sent to the end user. Reading the peripherals can also ensure that the rules for cookies apply.

Sectoral legislation: Some sectors have their own legislation, such as the E-commerce Directive,

which includes rules on informing consumers. This legislation can also apply to voice when this channel is used to communicate about products or services, or to conclude agreements.

Self-regulation: There is currently no specific self-regulation for the channel voice. As soon as it is required, the DDMA shall initiate the process.

3.2 Data processed

The personal data processed may be different with each organisation. You can determine yourself which functionality is linked to the assistant. Every situation involves a Google account and the associated account details. With a Google Home, a Device ID will also be linked.

In addition, you can, for example, choose to link customer data to the voice assistant such as the bank balance or the purchase history of the End User.

Personal data of the End User are also shared. Call logs of every conversation are saved. These

logs are personal data when the content can be traced to individual users. This is what it looks like in the Google Cloud platform:
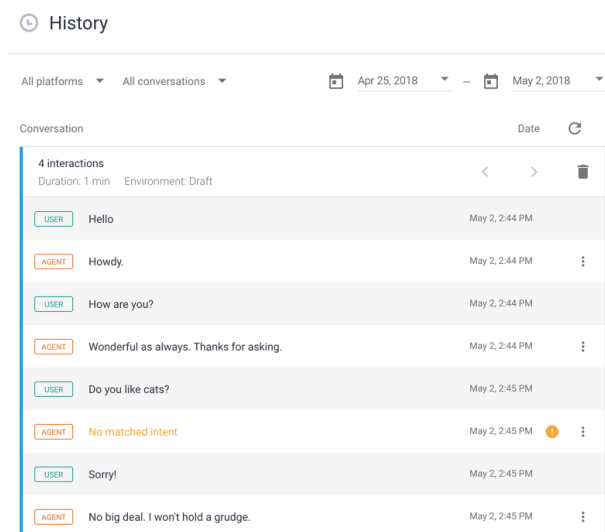
1

No sound recordings (voice logs) are currently available for the Organisation. Recent media coverage shows that Google still does keep them, to allow its employees to analyse them to improve its assistant. Capturing sound recordings is not unimportant, because voice data can be used as biometric data to determine the identity of the end use.

Authentication takes place on a personal level, but a smart speaker can be used by several people in one household. For this, Google uses voice recognition. Based on that, the identity of the speaker is determined, and this determines which actions are available. For privacy data, extra privacy provisions apply from the GDPR.

3.3 Determine the GDPR roles of all parties
In order to know to whom the GDPR obligations apply, the role of the parties involved must be determined.

As a rule there will be three parties:

End User: customers or prospects who communicate with the Provider and Advertiser through their voice assistant. If personal data relating to them is processed, the End User is, in GDPR terms, the *data subject.*

Provider: this is the party offering the speech assistant, they are the link between the Advertiser and the End User. It is not possible to say for the entire service whether the Provider is 'responsible' or 'processor' in the sense of the GDPR. That must be assessed per processing and depends on the agreements between the Organisation and the Provider.

Organisation: this is the organisation that wants to communicate with the End User via the voice assistant. This is done in an extra 'layer' of actions, in addition to the regular options between the Provider and the End User.

Who determines the goal and the means?
In order to determine who is responsible in the sense of the GDPR, the actual influence of the parties on the processing must be considered. The actual situation precedes the written agreements among the parties. In practice, this has already led several times to a large technology party - irrespective of the written agreements - designated as responsible. Therefore, make sure you watch out for the actual relationships and not just look at the contracts. In its Google Cloud Platform agreement (GCA), Google emphasizes that it is a processor. [2] This concerns the data that Google, *commissioned by* the Advertiser, processes to deliver Dialogflow Enterprise services. Among the same conditions, Google states that it will not use customer data for its own purposes, except where this is necessary to provide the requested services and technical support. [3]

3.4 Determine your basis
A basis (also a legal basis) is required for every processing of personal data. The GDPR offers six possible bases, three of which are relevant to voice:

The agreement: Google has a user agreement

---

[1] Images via:
https://cloud.google.com/dialogflow/docs/history

[2] In Art. 1.4 of the Google Cloud Agreement (hereinafter: the GCA), Google considers itself a processor: "Under this Agreement, Google is merely a data processor."
[3] GCA: 5.2 Use of Customer Data

with the end user. For example, for conversations someone makes with the Google Assistant on a smart Google speaker. The processing of personal data is necessary for the implementation of the agreement.

The agreement can serve as a basis for processing voice recordings. An Organisation that wants to communicate with the End User through the voice assistant cannot rely on this basis because the processing within an action is not necessary for the implementation of the agreement between the Provider and the End User. The basis can offer a solution for an Advertiser when voice communication is necessary for the implementation of an agreement between the Organisation and the End User.

Consent: Just as Google processes end user data based on consent, it is also possible for an advertiser to request consent. This is highly recommended when it comes to sensitive data. For example, if a bank links financial data to an individual user of the Google Assistant. Bear in mind that the law sets high standards for valid consent, and that the consent must also be verifiable. Often there is a case of a consent because a customer indicates to the advertiser that they want to communicate through voice. Google emphasises in its user agreement that the Organisation must ensure that, if necessary, consent is requested from the End User.[4]

Legitimate interest: If the agreement and consent offer no solution, you can assess whether the legitimate interest can serve as a basis for processing, for example for the analysis of conversations. Weight up the importance of your organisation (being able to communicate with the customer via voice) against the impact this has on the person concerned.

3.5 Determine the location of your data

In a time of cloud computing and storage, location of data is an abstract concept. It is nevertheless relevant to be able to comply with the GDPR. Additional requirements have been set for the transfer of personal data outside the European Union. The responsible person must ensure that data outside the EU remains just as well protected as in the EU. The GDPR offers a number of options for this. Some countries have

been declared 'safe' by means of an 'adequacy decision' by the European Commission. The Privacy Shield certification mechanism has been established with the US to help US organisations can confirm that they offer an adequate level of protection. Google is an American company, and has been certified for the Privacy Shield. When your organisation shares (customer) data for voice conversations with Google US, the Privacy Shield certification does not require additional safeguards. Data that data subjects themselves share with Google falls outside the scope of the GDPR rules on transfer. In the Google Cloud user agreement, Google emphasises that the customer (read: your organisation) can choose where the data is stored. Those who do not make a choice give Google itself the freedom to make a decision about it. [5]

3.6 Storage periods

For the processing of personal data, the GDPR obliges responsible organisations to ensure that it does not last longer than necessary for the specified purposes. A storage period must be communicated to the data subject before the data is recorded. As an alternative to mentioning a specific period, the method by which that period is determined is also sufficient. The most obvious place to provide information about this is the privacy statement on the website of your organisation. Ensure that a storage period is also set for less obvious personal data such as voice logs. If these are linked to unique identifiers or contain identifying information, a storage period must also be used for this.

3.7 Extra

US Cloud Act

Since the introduction of the Cloud Act in the United States, much criticism has been levelled against the EU-US Privacy Shield. The European Commission has expressed its concerns, and there are various lawsuits from privacy organisations. It is therefore not inconceivable that the regulation will be declared invalid. This can immediately make the storage of personal data in the US a

---

[4] GCA: 3.2 Privacy

[5] GCA: 1.4 Data Location

violation of the GDPR. It is therefore recommended to store data in Europe whenever it is possible.

Processor agreement
Written agreements must be made with processors about, among others, the security measures and the purposes for which the processor may use the data. Make sure that you also make the agreements required by Article 28 of the GDPR with Google. Check if the Google Enterprise Agreement contains the required agreements, and make additional written agreements where necessary.

Applicable law
Please note that article 16.10 (c) of the Google Cloud Platform Terms of Service states that the California Law applies to disputes between Google and customers. If this is not acceptable for your organisation, an additional agreement must be made with Google.

Data of children
Voice assistants are also available for children. That is why it is good to pay special attention to the additional protection that the GDPR offers to children. In the Netherlands it is possible to create a Google Account from the age of 16. That is also the age at which a child can give GDPR consent. Under 16 it is possible if the account is linked to the account of a parent through the 'family link'. Please note that your organisation does not provide personal data for children under 16 without parental consent. Read the additional measures that Google takes for Google Assistant <mark>here</mark>.

Identification
When you link personal data to a voice assistant, it is important to take measures that prevent unauthorised persons from gaining access. It is not complicated when using Google Assistant on a telephone. A mobile phone contains built-in security methods and the device is usually tied to one person. The situation is different with smart speakers like Google Home, which other family members or guests can also use. For example, when a bank account or a web shop account is linked

to a Google ID, it does not mean that the information may be freely accessible to all users of Google Home. Voice recognition is the most obvious option for this, but this technique has not yet been fully developed at the time of writing.

Certainty
As a provider of its voice technology, Google has control over the parties that use their services. For both free and paid Dialogflow users, Google can choose, without giving any reason,[6] to cancel the agreement without liability. Conversely, the advertiser can also opt to do so at any time. This offers flexibility, but also brings uncertainty. There is a possibility that your organisation will be removed from the channel. As the Google Assistant becomes a more important part of customer contact, it is good to take this into account.

Special points
Depending on what you want to use the interaction with the Google Assistant for, there may be additional legal issues. For example, when the Assistant is used to make a sale. Who is liable if the Assistant makes a mistake as a result of which the purchases are not legally valid? In the standard version of the user agreement, Google excludes any liability for this. If this risk is significant for your organisation, it is recommended for you to make additional agreements with Google about this.

3.8 Rights of data subjects
As with any processing of personal data, the data subject can invoke all rights arising from the GDPR, including:
- Inspection
- Removal
- Objection

What can you arrange yourself and what can you arrange through Google? For all processes where your organisation is responsible, the obligation to comply with these articles lies with your organisation. That does not mean that the implementation may not be delegated to another organisation. As all end users have a

---

[6] GCA: 9.4 Termination for Convenience.

direct relationship with Google, it is obvious that users will be offered all general information and rights with regard to the Google Assistant in this way. Google has set up a privacy portal for this purpose.[7]

However, this does not relieve you of your obligations as a controller. The user must also be able to contact your organisation. For example, to ask what is in the call logs that you keep in Dialogflow. As the controller, you are also obliged to provide information about the processing 'when obtaining' personal data. A lot of information must be provided, which is usually stated in the privacy statement. Make sure that everyone who chooses to communicate with your organisation through the speech assistant is advised of your privacy statement. That privacy statement must explain, among others, which data is processed for this and whether the data is provided for this purpose to countries outside the EU. Attention should also be given to rights such as inspection, removal and complaints. It may be possible to inform the customer in the dialogue with the speech assistant that a spoken version of the privacy information is available. Google has guidelines that describe how they think advertisers should communicate about the deployment of their channel.

About the DDMA

The DDMA is the industry association for data and marketing. Its objective is to raise the industry to a higher level. The members of the DDMA, who number over 300, input and share knowledge about how data and techniques can be used to communicate with their target groups in a way that is relevant to these groups. The DDMA organises research projects and network and knowledge meetings with its members and for its members. Its team of legal counsels advises members and the industry on changes in legislation. The DDMA also gives the industry a voice in stakeholders in The Hague and Brussels on the development of a sustainable data economy.

Would you like to know more about the privacy rules concerning voice? Send an e-mail to legal@ddma.nl or call 020 4528413.

---

[7] https://safety.google/privacy/privacy-controls/