

# Topics for consideration 2019

Voice assistants, constantly listening to your private life	02
Cloud computing under the GDPR	06
Data sharing: public interest issues	08
Political communication & GDPR: updating recommendations and clarifying best practices	10
The reuse of data accessible "online" by the research community: challenges and prospects	12
How is children's data protected?	14



Voice assistants are often paired with smart or connected speakers. However, it is important to note that speakers are only vectors and that assistants can be integrated into any type of appliance. In practice, voice assistants are devices with a speaker and a microphone, more or less-developed computational abilities depending on assistants and, in nearly all cases, the ability to connect to the internet.

Having appeared in mass consumption goods in the early 2010s, many voice assistants are now being rolled out. Depending on the activity carried out by the enterprises' developing them, these assistants meet very specific needs: online sales, listening to music, task planning, home automation, etc.

These products are offered by major international groups such as GAFAM (Google, Amazon, Facebook, Apple, Microsoft), BATX (Baidu, Alibaba, Tencent, Xiaomi) and even smaller enterprises (such as Snips) with different economic positions.

## How do these devices work?

Vocal assistants generally work according to five main steps. Take the example of a "smart" speaker:

### Step 1

**The user "wakes the speaker up" using a key phrase ("Hey Snips"/"Ok Google"/"Hey Alexa"/etc.)**

The speaker is always listening for this key phrase. It does not record anything and does not perform any operations until it hears this key phrase. This step is performed locally and does not require any external exchanges.

### Step 2 (optional)

**The speaker recognises the user**

Some assistant models ask the user to pre-record samples of his/her voice in order to create a voice profile and therefore recognise the user during interactions with the assistant. The purpose of identifying the user is to be able to suggest different services to the device's different users (parents, children, guests, etc.). We call this vocal biometrics. It should be noted that biometric data are considered sensitive data within the meaning of the GDPR, and as such can only be processed with the data subject's explicit consent.

### Step 3

**The user makes a request**

The phrase spoken by the user is recorded locally by the assistant. This audio request recording can then be:

- stored in the device, in order to allow the user to manage his/her data (e.g. a smart speaker with a vocal assistant from the company Snips); or
- sent to the cloud, or in other words to the company's processing servers (which is the case for example for Amazon Echo, Google Home and other speakers).

### Step 4

**The audio recording is transcribed into text and interpreted in order to provide a suitable response**

Speech is automatically transcribed into text (speech-to-text) and interpreted using Natural Language Processing technology in order to provide a suitable response. A response is then synthesized (text-to-speech) and then played and/or an order is executed (open the blinds, increase the temperature, play music, answer a question, etc.).

Whether these different processing operations are performed locally or on remote servers, the device (or its services) may store:

- a history of transcribed requests in order to enable the individual to view them and the publisher to adapt the service's features;

- a history of audio requests in order to enable the individual to listen to them and the publisher to improve its speech processing technology;
- metadata relating to the request, such as the date, time, account name, etc.

### Step 5

**The speaker returns to "stand-by"**

The assistant returns to a passive state of listening and waits to hear the key phrase before being reactivated.

## What are the stakes and what are the recommendations to protect privacy?

The voice is an essential component of human identity. As such, it is extremely personal. Personal characteristics are found both in acoustics (identity, age, gender, geographical and sociocultural origin, physiognomy, state of health and emotional state, etc.) and linguistics (meaning of the words used, vocabulary used, etc.). Thus, providing voice recordings is not an inconsequential act. Furthermore, by developing outside of telephones, vocal assistants have progressively transitioned from a "personal" status to "shared" status. They have now permeated intimate areas and areas shared by several individuals such as living rooms, bedrooms and even the insides of vehicles. These paradigm shifts raise new questions such as those relating to the collection and processing of third-party data.

Lastly, as stated above, in most cases, vocal assistants rely on the processing of speech signals on remote servers. As a result, although speech is generally associated with a certain degree of volatility, vocal requests are still recorded in the cloud as are text requests when entered into some search engines.

The CNIL has identified three areas to be aware of, which add to the various questions that users may be faced with:

### The confidentiality of exchanges

While they are permanently on stand-by, vocal assistants can be activated and unexpectedly record a conversation when they consider that they have detected the key phrase. To better protect users' privacy and to avoid these types of malfunctions, we advise:

- favouring the use of devices with a button to deactivate the microphone;
- turn off the microphone/turn off the device/unplug the device when users do not want to be listened to. Some devices do not include an on/off button and must be unplugged;
- warn third parties/guests of the potential recording of any conversations had (or turn off the microphone when they are present);
- supervise children's interactions with these devices (stay in the same room, turn off the device when not with them);
- In this case, check that the device is configured by default to filter information targeting children.

### The lack of a screen

The purpose of vocal assistants is to provide a human-machine interface without any visual media.

However, to both configure these devices and manage data, tools such as dashboards are still necessary. Without an external screen or any display features, it is hard to see which traces are recorded, to assess the relevance of suggestions, to learn more or to have access to answers from other sources. In order to manage how such data is used, we recommend regularly visiting the dashboard (or the application) provided with the assistant to delete the history of conversations or questions asked and to personalise the device based on needs; e.g. configure the default search engine or source of information used by the assistant.

### The monetisation of intimate data

As they mainly target homes by controlling smart devices and entertainment services, devices with a voice assistant are now central to households. Users' profiles are therefore fed by the different interactions between them and the assistant (e.g., life habits: the time they wake-up, heating settings, cultural taste, purchases made, interests, etc.). To control the use of such data, we recommend:

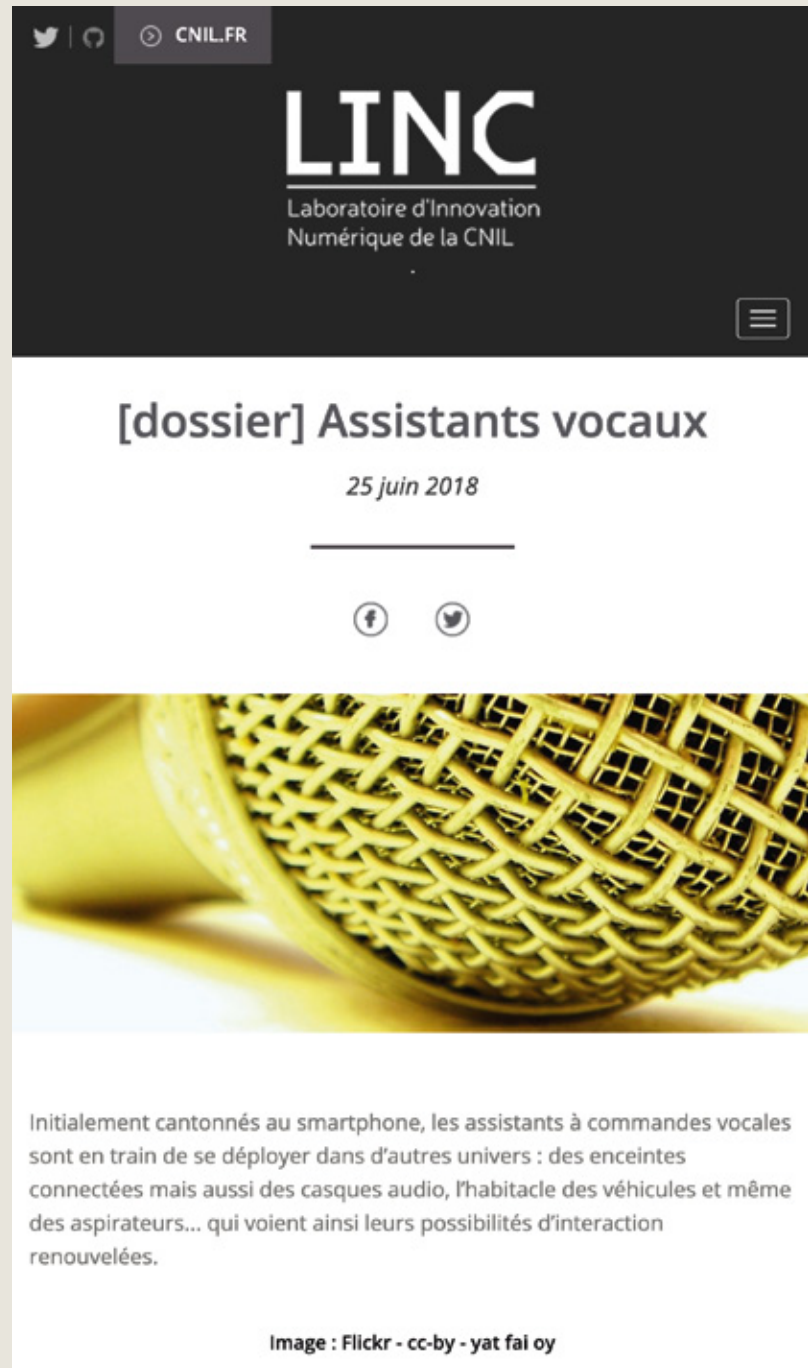
- syncing services that are actually useful to the user, while weighing the risks of sharing intimate data or sensitive features (opening doors, alarm systems, etc.);
- being aware that any speech around the device can serve to fuel marketing profiles;
- do not hesitate to contact the support service of the company providing the assistant in case of questions.



## What future developments and CNIL works are yet to come?

Manufacturers are very active in improving voice assistants' abilities and security. Although some are increasingly interested in putting an end to the use of a key phrase to wake assistants, others are working to carry out processing operations to separate sound sources in order to improve systems' listening capacity - for example, to reduce TV volume, to separate one person's speech from another's, etc. Lastly, professionals are also looking into new places where these systems can be used, such as in hotels and workspaces, thereby reviving questions relating to the effective use of data.

The topic of vocal assistants was identified as an area for works to be carried out by the CNIL in 2017. The latter quickly made contact with various stakeholders in order to gain a perfect understanding of the systems deployed. It has led important discussions within the CNIL's digital innovation laboratory (LINC), its structure dedicated to experiments and studies on emerging digital use trends. As such, a thematic dossier comprised of articles and interviews with professionals was published on its website.

In 2019, the CNIL plans to pursue these works, by continuing to exchange with the industrialists and academics working on these topics, but also by continuing tests on these devices. In particular, the aim is to study how we can guarantee that users are well informed of the data collected, the uses made of such data and the means at their disposal to exercise their rights of access, modification, erasure and portability, as well as to assess the security of the data processed and how the artificial intelligence algorithms that are inherent to these devices learn.









# LINC

Laboratoire d'Innovation Numérique de la CNIL

[dossier] Assistants vocaux

25 juin 2018

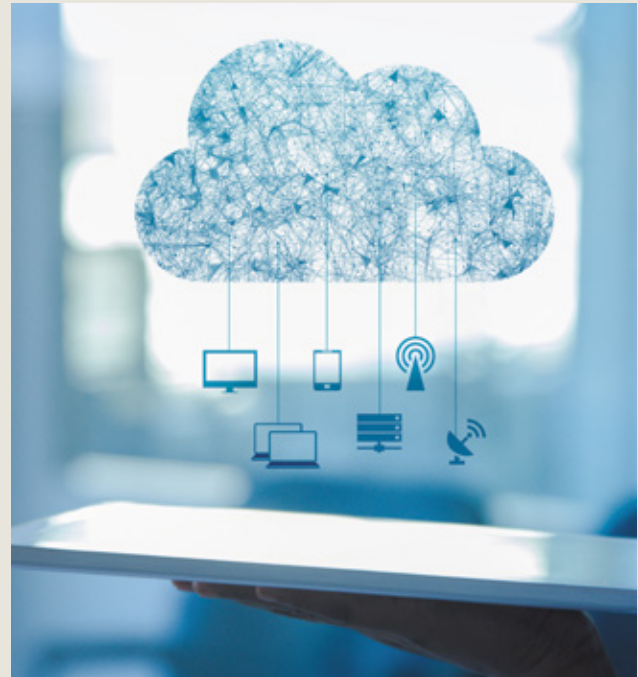
Initialement cantonnés au smartphone, les assistants à commandes vocales sont en train de se déployer dans d'autres univers : des enceintes connectées mais aussi des casques audio, l'habitacle des véhicules et même des aspirateurs... qui voient ainsi leurs possibilités d'interaction renouvelées.

Image : Flickr - cc-by - yat fai oy



# Cloud computing under the GDPR

In 2012, the CNIL and the G29 published recommendations on cloud computing. Since then, use of the cloud has only increased: Gartner<sup>1</sup> recently estimated that public cloud revenue had grown by 21.4% in 2018, and that this revenue would rise to \$300 billion by 2021. At the same time, Eurostat<sup>2</sup> stated that 55% of enterprises used the cloud for critical functions (finance, accounting, CRM or business applications). With the advent of the GDPR – which modernises the obligations of data controllers and subcontractors alike – a situational analysis of how the cloud is used within organisations is necessary. Have the 2012 recommendations been applied? Is personal data protection guaranteed when migrating data to the cloud?



## Concentration of risks and limited bargaining power

In December 2018, a survey<sup>3</sup> published by the Independent Oracle Users Group estimated that one quarter of all enterprises' data were now stored on the cloud. Of course, such data includes industrial data, but it also includes a large amount of often-sensitive personal data, which are usually hosted and processed within the infrastructures of a very limited number of major cloud computing providers. Yet, opposite these players, those who wish to use the cloud actually have very limited contractual bargaining power.

The movement of data within these infrastructures can increase systemic risks, even when the enterprises providing these services – whether data controllers or subcontractors – fall within the material scope of the GDPR.

Furthermore, in 2018, the adoption of the Cloud Act by the United States – which provides American authorities with a legal framework enabling them to access data beyond their borders – and the European proposal for a regulation on terrorist content online, present the

challenge of finding a balance in terms of privacy when using these services.

The stakes in terms of data protection, and more widely in terms of economy and strategy, are high. It is therefore vital that the CNIL carries out a technical and precise situational analysis of these infrastructures and services.

### 1/4 of enterprises' data stored on the cloud

(according to the Independent Oracle Users Group)

<sup>1</sup> <https://www.gartner.com/en/newsroom/press-releases/2018-04-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-21-percent-in-2018>.

<sup>2</sup> [https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud\\_computing\\_-\\_statistics\\_on\\_the\\_use\\_by\\_enterprises](https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises)

<sup>3</sup> « 2019 IOUG databases in the cloud survey » par Joseph McKendrick, produit par Unisphere Research, division de Today, Inc. Décembre 2018 <https://www.ioug.org/d/do/8551>



## FOCUS

### Recommendations relating to the cloud:

1. Map data and processing in the cloud
2. Set out technical and legal requirements
3. Carry out a PIA or at least a privacy risk analysis
4. Identify the relevant type of cloud for each processing operation
5. Choose a service provider offering sufficient guarantees
6. Update the internal security policy
7. Monitor development over time

### The CNIL and the cloud, an old story

The CNIL has been working on this topic since the early 2010s, alongside other European data protection authorities. After a broad consultation, in June 2012, the CNIL published its first recommendations relating to cloud computing, which were followed by the WP29 one month later. The concept of joint responsibility therefore entered CNIL doctrine. Today, this concept is also provided for in the GDPR, and processors - who up until now had no legal responsibilities with regard to the Data Protection Act -, now have responsibilities.

### The future of the cloud examined by the CNIL

The CNIL would first like to delve further into the technical aspects of the cloud to better understand the infrastructures used by the main cloud service providers and, more generally, this ecosystem. As a second step, it will analyse the constraints and risks which client companies are actually faced with today. Lastly, these works will allow the CNIL to update its recommendations and to identify new levers to regulate this sector which should be mobilised.

In this context, the aim will be to develop the following lines of focus:

- **Clauses between data controllers and processors**

For cloud services considered processors, what margins for negotiation are clients afforded in terms of security and privacy protection? What clauses govern the relationships between data controllers and processors? Do these clauses cover all items set out in Article 28 of the GDPR?

- **The impact of legislation**

What impact do some specific laws - and particularly those with an anti-terrorist purpose - have on cloud contracts and on privacy protection? Whether as regards the Freedom Act and the Cloud Act in the United States or the draft regulation "on preventing the dissemination of terrorist content online" proposed by the European Commission in September 2018.

- **Encryption**

Encryption is one of the most powerful methods for ensuring data confidentiality: how is this method used and applied in practice in the new cloud architectures? How can we comply with best practices in the field whilst managing keys in a secure manner? For example, when virtual machines are randomly restarted, what means are put in place to ensure the secure sharing of keys between the client's Hardware Security Module (HSM) and the new entity?

- **The end of the contract**

During its previous works, data controllers informed the CNIL of significant difficulties in retrieving their data at the end of a contract and of the complexity of ensuring that data are properly erased. Has management of account closures improved? At first glance, it appears that progress has been made in this field, but is such progress enough to enable data controllers to effectively meet their obligations?

- **Information on data localisation**

Several improvements have been noted in the information provided to clients and to data controllers as regards data localisation. But, how do data localisation clauses take account of exceptional situations such as cases of force majeure or hardware connections by administrators or remote support?

- **Data breach notifications**

How have cloud suppliers set-up personal data breach notifications? Particularly when such suppliers are regarded as processors, what means are provided to their clients, data controllers, to meet their obligations (whether for a breach detected by the service provider or for a breach notified to the client by a third party)?

Lastly, in a time in which trust has become vital for cloud service providers, standards, codes of conduct and other frameworks are multiplying. Their relevance must therefore be assessed in terms of data protection. A map of these frameworks would allow suppliers and their clients to choose those that are most relevant to them.

# Data sharing: public interest issues

In its IP5 report, *“la plateforme d’une ville”*, the CNIL explored four data-sharing scenarios to attempt to find a new balance between public and private stakeholders using data. Since then, the topic of data sharing has entered the public debate, presenting as a possible solution to several vital societal needs, and particularly in terms of regulation and research.



Since 2017, in keeping with the open data movement and the notion of public-interest data, several works have advocated for a wider sharing of data. The President of the Republic made this point during his speech on artificial intelligence in March 2018. In particular, the Villani Report *“Pour donner un sens à l'intelligence artificielle”* (“For a meaningful artificial intelligence”) recommended:

- “encouraging economic stakeholders to pool data”;
- “providing for the opening of certain data held by private entities, on a case-by-case basis”;
- “implementing portability with a citizen-based approach”;
- “facilitating dialogue between AI stakeholders and regulators”, thereby picking up on some of the topics developed by the CNIL.

The topic of data sharing has also been the subject of works in the framework of the General Situation of the New Digital Regulations, launched in July 2018.

The spectrum of data concerned by such sharing initiatives extends to all or part of personal data, and these initiatives must be undertaken in compliance with individuals’ rights. For this reason, the CNIL considers that developing an effective and sustainable data-sharing model, with a strong ethical component and based on compliance with fundamental rights - which naturally includes personal data protection and privacy - should be encouraged.

## Sharing initiatives already identified

Several data sharing initiatives have already been developed: for example, in la Rochelle where inspiration has been drawn from the principle of citizen portability to access certain data held by private operators. A different approach has been taken by the CASD (the Secure Access Data Centre) which has extended its service offer to hosting private data (banks, services, transport, private health, etc.) and to their availability to researchers or private operators, on a purely voluntary database, in order to develop value added services.



The “Health data hub”, containing suggestions regarding organisation arrangements for operating platforms and the sharing of health data, was also provided to the Minister of Solidarity and Health. In early 2019, this fuelled the submission of the draft act on organising and transforming the health system, which the CNIL provided an opinion on in January 2019. On an international scale, private stakeholders have designed data-sharing models: e.g. the city of Toronto and Sidewalk Labs are considering developing a locally controversial civic data trust to manage urban data.

## Setting out a framework rather than a unique sharing model

The GDPR was established to reconcile both technological innovation and the protection of individuals’ rights, with the belief that the former would become stronger and more sustainable if the latter is complied with and promoted.

In this respect, in itself, the sharing of data between public and private stakeholders is not contrary to the right to personal data protection, especially when the clearly defined general interest purposes are involved. However, these initiatives do call for more clarity in terms of applicable framework and for the accompaniment of project leaders as from the early stages.

Internally, the CNIL has already launched works to clarify the legal framework applicable to data sharing, by addressing the major cross-cutting issues relating to compliance with the GDPR (legal ground for the provision of data, modalities for the exercise of individuals’ rights throughout the share chain, etc.), in order to provide support with securing projects from a legal point of view. However, such a legal framework can only be very general, as the topics of respecting rights, governance, and sharing arrangements (directly or through a third party) can only be studied in light of concrete projects. Yet, in general, beyond strict compliance with texts, the CNIL strongly encourages the integration of necessary personal data protection as from the creation of sharing approaches, both on a legal and ethical basis.

The CNIL will continue its work on frameworks and will combine these works with a pro-active policy of providing prior accompaniment for given sectoral projects, including experiments, as part of its role to advise public authorities and assist professionals. For all of its tasks, it will ensure that the safeguards set out in terms of personal data protection are effective and, where necessary, will suggest changes or corrections to frameworks.

## Capitalising on and furthering works already started

The CNIL’s experience in regulating data sharing platforms demonstrates that there is no unique model but rather several possible and desirable options. In particular, the scenarios set out in the IP5 report for the reuse of private data by public stakeholders could be completed and detailed, especially should it be decided to open certain personal data belonging to private stakeholders to other private stakeholders.

Depending on the sector or the project, the data sharing scenarios available must therefore be adapted and combined. In some cases, recourse to intermediaries (platforms, data department) in charge of providing access to data and, where necessary, other functions in the general framework, could be particularly suitable, particularly in cases in which several stakeholders pool their data. However, recourse to these intermediaries does not seem suited to all sharing frameworks, particularly when data comes from only one stakeholder and are made accessible to one or more entities. In this case, simple sets of legal (licence) and technical (API) rules, without any intermediary, could be quite suitable and sufficient to ensure that the framework complies with data protection rules.

It is by approaching these systems as from their creation that stakeholders will be able to produce virtuous and sustainable data sharing models which place the citizen and his/her rights at the centre of processes and of data governance for general interest purposes. In this respect, the regulator has a role to play, by committing to promoting innovative models and ensuring the highest level of protection of individuals’ rights.



“The sharing of general interest data is an opportunity to implement a European ethical innovation model.”

# Political communication & GDPR: updating recommendations and clarifying best practices

The CNIL assists all electoral process stakeholders, whether they be electoral candidates or their parties, elected representatives or voters, both in the context of bringing the processing implemented into compliance and to enable data subjects to exercise their rights. Following the entry into force of the GDPR and in a context of European and municipal elections, the CNIL intends to continue the works started on this topic and plans to update its 2012 recommendation.



Determining which rules are applicable in terms of political communication is one of the CNIL's long-standing tasks, with its first recommendation in the field of political communication having been adopted in 1991. In recent years, this task has taken on a particular dimension with the development of digital tools and the use of social networks. We are now witnessing a complex overlapping of relations between stakeholders from various backgrounds: individuals who, due to their activity, produce a large amount of data and voluntarily provide such data to certain stakeholders, platforms whose economic model relies on the processing of such data, consultancy firms and research structures, political parties likely to use such data.

In addition, several scandals, and particularly the Cambridge Analytica

scandal, have made the general public aware of the stakes relating to the use of their data and, in particular, of the need to prevent the misuse of personal data during political campaigns. Over the last year, complex legal challenges in particular have appeared around the notions of profiling, data localisation and around the means that should be implemented to ensure the security of data. Lastly, in addition to the legal stakes, these different cases highlight significant ethical issues, in particular by touching on the fairness of elections.

In this context, **the CNIL's role in the field of political communication is to accompany innovation whilst ensuring that individual freedoms are respected in an environment in which new technologies are now among the instruments frequently used during political campaigns.**

**The impact of the implementation of the GDPR on political communication: principles to observe and best practices.**

While regulations on data protection have evolved since 25 May, the new legal framework has not resulted in any changes as regards the qualification of political opinions as sensitive data, the principle of prohibition from collecting and processing such data, and the exceptions that the data controller may raise to circumvent this prohibition (Article 9 of the GDPR).

In addition, the GDPR does not change the main principles governing personal data protection, compliance with which should define the conditions for the use of data relating to political opinions

## Respecting the golden rules of data protection

### Illustrated through a few key principles:

- **Determine the purpose of the processing carried out:** precisely identifying the purpose pursued by the processing of data relating to political opinions is essential.
- **Ensure the proportionality of the data collected:** only data which is strictly necessary for the identified purpose must be processed.
- **Securing the data collected:** the particular nature of the data processed requires that further measures be taken to ensure their security (setting out appropriate storage measures, access management measures, etc.).

These principles are more relevant than ever in order to prevent any misuse of personal data during electoral campaigns.

The evolution of applicable regulations in terms of personal data protection has also led to the application of new provisions contained in the regulation, and particularly those relating to the rights of individuals whose data is processed.

The wide range of information that could be considered a political opinion means that the data collected must be processed in a transparent manner. Sufficient and easily accessible information must therefore be provided to data subjects.

The appearance of new rights (right to the restriction of processing, to portability, etc.) must also be taken into account in practices such as political prospection in order to guarantee their effectiveness. Similarly, more general discussions must be held on the conditions under which such prospection may be carried out, particularly when it relies on files initially created for another purpose (such as commercial files).

With the entry into force of the GDPR resulting in the disappearance of most prior formalities and the improved protection of each citizen by creating new rights and obligations for political stakeholders, **the CNIL has launched an**

## Electoral campaign and use of personal data: main principles and areas for vigilance

The CNIL has drafted an article for the AJCT journal (Actualité Juridique Collectivités territoriales) to be published in February 2019 within a dossier devoted to "The Internet, social networks and electoral campaigns".

### in-depth analysis which will soon lead it to adapt its recommendations and to set out best practices in this field.

At the same time, the CNIL intends to continue its works on new tools and uses mobilised for political communication with a view to improving and solidifying its doctrine on the topic during a period marked by the organisation of both European and national campaigns. In particular, through the works launched on electoral prospection software, the aim is to specify under which conditions data from social networks can be used and the role of each of the stakeholders involved in electoral campaigns.

## Personal data, social networks and democracy: on the 2019 agenda for French-speaking authorities

On 19 October 2018, the CNIL hosted the annual meeting held by the French-speaking association of personal data protection authorities (Association francophone des autorités de protection des données personnelles, AFAPDP). French-speaking authorities were invited to a morning of discussions centred around the topic of "Personal data, social networks and democracy". This topic was a natural result of the revelations of the "Cambridge Analytica" case, but falls within the much broader scope of the discussions which have been carried out by the AFAPDP on electoral issues for several years now. In particular, the association took part in the creation of a practical guide on the consolidation of the civil registry, electoral lists and the protection of personal data<sup>4</sup>, published by the Organisation internationale de la Francophonie (OIF) in 2014.

During this session, the AFAPDP decided to promote a cross-cutting approach, which goes beyond the mere framework of personal data protection. To do so, the AFAPDP called on the complementary expertise of the French-speaking network of electoral competencies (Réseau des compétences électorales francophones, RECEF), the French-speaking network of media regulators (Réseau francophone des régulateurs médias, REFRAM) and Reporters without borders (Reporters sans frontières, RSF). All of these actors are questioning their respective roles with the appearance of new digital tools, media and social networks, at different stages of the electoral process.

While relevant legal principles already exist, these either completely or partially ignore social networks and, more generally, the digital sphere. This legal coverage, which can only be qualified as partial, could be improved with new legislative provisions. A multi-regulator approach could also consolidate the reliability and fairness of electoral processes under the digital era, and for this purpose a multi-network working group is already being put in place by the AFAPDP, the RECEF and the REFRAM, with support from the OIF.

<sup>4</sup> [https://www.francophonie.org/IMG/pdf/oif\\_guide-pratique\\_etatcivil-27-11-14.pdf](https://www.francophonie.org/IMG/pdf/oif_guide-pratique_etatcivil-27-11-14.pdf)

# The reuse of data accessible “online” by the research community: challenges and prospects



Recent revelations and scandals have illustrated the potential abuses arising from the exploitation of data that is freely accessible on the internet for research purposes: misuse or uncontrolled dissemination of results resulting in data protection breaches. More generally, given the interest of using data accessible “online” for research purposes, the CNIL has decided to look into the conditions under which these operations are carried out.

## Research and use of personal data: inextricable links

The pools of data created by use of the Internet and social networks attract many stakeholders with the intention of exploiting them and drawing added value from them for their activities. The use of such data presents significant challenges and risks in terms of data protection. The “Dinsinfo Lab” scandal illustrated the sensitivity of issues relating to reuse of data that is accessible “online” for research purposes; the revelations of the Cambridge Analytica scandal showed how data initially collected for research purposes could be ultimately misused for other purposes.

Researchers are some of the actors using this wealth of data. As such, from time to time, research projects using such data are referred to the CNIL to ensure that these projects comply with applicable regulations on personal data protection.

It can be difficult to articulate some of the principles arising from these regulations with the aims of research. In terms of referrals to the CNIL, it was noted that some stakeholders either considered that the Data Protection Regulation did not apply to their works, or that the corresponding legal principles either prohibited or went against most of these works. Indeed, carrying out research most often requires the collection of a large amount of data, for which setting a precise data retention period in advance can be difficult.

As such, the compilation of datasets that may be useful for other studies, and access to said datasets to ensure that research can be reproduced are issues that must be reconciled with the requirement of complying with the Data Protection Regulation.

It is against this backdrop that the CNIL has begun to think about the legal conditions under which data that is accessible online can be reused for research purposes. This reflection must also serve to clarify which regulations are applicable in a political and social context marked by several “scandals” concerning the reuse of data accessible “online” by researchers. It appears vital that personal data protection reflexes are included in research projects as from their creation, at the risk of these projects being carried out without taking them into account.



“Carrying out research requires the collection of a large amount of data, for which it can be difficult to precisely set a data retention period beforehand.”

## A Data Protection Act serving the research sector

In a time in which the regulations applicable to personal data protection are being strengthened, the CNIL recalls that many provisions can be mobilised to favour the processing of data for research purposes. For example, under certain conditions, the GDPR sets out exceptions to the prohibition from processing sensitive data, to the obligation of informing the individuals whose data is collected, and to the exercise of the rights to erasure and to object.

The GDPR differentiates between scientific research, historical research and statistical research. It states that scientific research must be understood in the broad sense and must include “for example technological development and demonstration, fundamental research, applied research and privately funded research”, but also “studies conducted in the public interest in the area of public health” (recital 159 of the GDPR).

As such, it appeared necessary that the CNIL launch works to present and more clearly define the applicable legal framework, both prior to and after the entry into force of the GDPR. These works must therefore accompany both public and private stakeholders from the research community in their compliance efforts. In particular, the aim is to further explain the conditions under which the planned processing operations can be implemented - whilst recalling that consent is only one of the legal grounds that can be invoked, alongside, for example, the performance of a task carried out in the public interest or the legitimate interests pursued by the data controller -, to verify the

fairness of the collection of data carried out and to check that data subjects have been provided with the necessary information.

As regards information in particular, one of the difficulties raised by the application of the provisions contained in the GDPR resides in the balance that must be found between the requirement of delivering sufficient information and that of encouraging participation in a study or in research.

Similarly, these works must clarify the relations that may exist between the different fields of research (public research, private research) and any potential differences that must be made depending on which field is concerned. Each of the stakeholders involved must be able to understand what can and cannot be done with the data collected, depending on the context in which they find themselves. This clarification appears all the more important given that some researchers are, for example, likely to move from one field to another during their career.

These works, which will be carried out in collaboration with research stakeholders, must also determine which appropriate safeguards must be implemented to govern the collection, use and reuse of data accessible “online” by the research community.

In particular, the aim is to determine under which conditions researchers may access online data on social network platforms, for example to avoid situations in which only some researchers may access such data or to avoid that only research serving

platforms in terms of marketing or commercial effectiveness is able to rely on access to the data possessed

**The approach set out by the CNIL therefore aims to:**

- **ensure better legal security** to research stakeholders by clarifying the legal framework applicable to research projects based on the processing of data accessible online and by providing these stakeholders with simple tools to understand the GDPR applied to their projects;
- **issue recommendations in line with the needs and constraints experienced by research organisations**, in order to enable them to successfully carry out their projects whilst ensuring their compliance with the applicable legal framework. These recommendations could be supported by consultation with stakeholders from the research community, particularly on the following topics: access to data deposited on platforms, implementation of data subjects’ rights, definition of data retention periods to be applied, provision of personal datasets to the research community or security measures to be implemented.



# How is children's data protected?



In 2018, 83% of 12 to 17-year-olds owned a smartphone. 91% of them connected to the Internet every day and spent on average 27 hours per week surfing the web. 37% of this age group made online purchases (source: *le baromètre 2018 du numérique* - the 2018 digital barometer - by Crédoc).

If underaged individuals have become digital stakeholders in their own right, it is precisely because of their massive use of **social media** (instant messaging, social networks, photo- and video-sharing networks) to share information on themselves or on other underaged individuals. And when children themselves aren't doing it, it is their parents who are posting photos and videos of their children on the Internet.

The number of **connected objects for children** - watches, bracelets, connected toys and even soft toys (cloudpets) - and for families - "smart" speakers, home automation, "smart homes", etc. - have

increased

Lastly, digital technologies have invaded the education sector, and particularly teaching methods, whether through tools to manage school life, digital workspaces, online educational services or the development of learning analytics.

These digital practices and uses are the result of a large amount of data processing and of trace analyses, which provide a wealth of information on children, their interests, their behaviour, their movements, their intellectual potential, their personality profile - and

which, as such, are extremely sought after. How can such data - which is particularly sensitive when it comes to children - be protected?

At the same time, our societies favour the development of autonomy and personal accountability, regardless of age. In the words of Michel Foucault, it is a question of making each individual an "Entrepreneur of the Self" and therefore preferring to assist children towards discovering their own personal identity and originality.

## The growing recognition of children's rights

The 1989 **International Convention on the Rights of the Child** set out this concept by acknowledging that each child has not only a right to protection – to compensate for his/her vulnerability – but also a right to a series of social benefits, to accompany his/her development, and to “freedom” rights which must prepare the child for his/her future adult life. The Convention sets out the principle of “the best interest of the child”, a dynamic concept whose scope can only be assessed in concreto, on an individual basis.

In France, the societal changes in progress have already been translated into law.

Many legal provisions authorise unemancipated minors to take initiatives. The principle of legal incapacity does not mean that they do not have any individual rights.

In the justice sector, the general rule is that a child is entitled to exercise his/her rights alone, without age restriction, since 2007 and the entry into force of the European Convention on the Exercise of Children's Rights of 25 January 1996 which aims “in the best interests of children, to promote their rights, to grant them procedural rights and to facilitate the exercise of these rights”. Thus, a child may make a complaint, bear witness, be heard by a judge in civil or criminal proceedings, request legal aid or refer to the Defender of Rights. Furthermore, no age conditions may restrict a minor's right to request political asylum, to request to give birth anonymously or to become a member of an association.

From the age of 13, a minor is entitled to request an organ donor card. He/she must consent to his/her full adoption and to the change of his/her name.

On occasion, the youth's independence requires prior intervention from his/her parents. Thus, from the age of 16, a youth may sign an employment contract or

open a bank account with a bank card alone, but only after having gained his/her parents' consent.

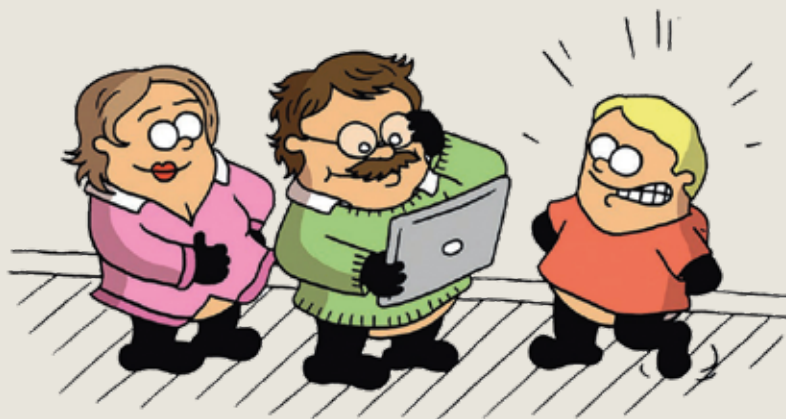
In other cases, the child's opinion must always prevail as a last resort. When a minor receives medical care without his/her parents' knowledge, said minor is entitled to object to his/her parents being informed. The doctor must play the role of conciliator in the event of a family conflict, with the final decision always being made by the minor.

This is also the case when medical research on a minor is considered. The authorisation to participate in such research must be collected from the individuals with parental authority. However, the participating minor must also be consulted, when his/her condition allows it, and provided with information adapted to his/her ability to understand. His/her personal acceptance of the research must be sought. If the minor does not wish or no longer wishes to participate, his/her decision must be respected under all circumstances.

## Ensuring children an effective right to data protection

In France, children's right to personal data protection witnessed its first major legal step forward in the field of medical research. The act for a digital republic of October 2016 provided that a 15-year-old minor can object to his/her parents having access to data collected for this purpose concerning him/her. Said minor can also object to his/her parents being informed of any preventive, screening or diagnostic acts. The minor is the only individual to receive such information and able to exercise his/her rights.

The CNIL – considering that French law already took into consideration a minor's age in order to allow them to perform certain acts – has questioned, as from the early 2000s, whether minors beyond a certain age of maturity should be allowed to perform certain “daily acts” on the Internet, for example the mere act of creating an electronic messaging account or registering on a child's website.



The advice that it provides on its website, on the Educnum website or through the awareness-raising initiatives that it carries out targeting youths attest to its desire to improve children's rights over their personal data, whilst ensuring them further protection. These discussions must take into account the new legal framework set out by the **GDPR**. For the first time, the latter has introduced provisions especially relating to minors into personal data protection law, considering that they are **particularly vulnerable** individuals who must benefit from specific protection due to their lesser awareness of the risks run in the event of the processing of their personal data, on social networks for example. This is true in terms of both advertising and profiling. Thus, the GDPR provides that, for online services targeting minors under the age of 16 and requiring consent, parental consent is necessary. However, Member States may provide for a lower minimum age in their national law, no lower than 13 years old; in France, this age is set at 15 years old.

For this reason, the GDPR encourages the adoption of codes of conduct specific to the protection of children's data and urges data protection authorities to pay special attention to activities specifically targeting children.

However, the GDPR does not merely content itself with setting out a protective framework for the processing of data relating to children. It also recognises that they have **specific individual rights**:

- As from a certain age, set out by each State (15 years old in France), their consent may be considered as a legal ground for the processing of data related to direct service offers via the Internet, notwithstanding exceptions for being underaged.
- Compliance with the principle of transparency implies that the information targeting children is drafted in a way that is easily understandable for them.
- The rights to rectification and to be forgotten are considered especially important when consent to the processing of information has been given by a minor.



## “The GDPR recognises that minors have individual rights”.

**Several questions are raised as regards the interpretation and application of the GDPR. However, beyond the general regulation, we must also consider under which conditions children should be able to exercise their rights, as is the case in the works carried out by other European data protection authorities:**

- Which operational mechanisms should be promoted to verify children's age?
- Under what circumstances must the prior consent of those with parental authority be requested?
- How should such consent be collected?
- How can we ensure that a child has indeed been authorised by his/her parents to consent?
- How can information targeting minors be adapted to ensure that it is easily understandable?
- How can we facilitate the exercise of the right to rectification and the right to be forgotten especially granted to minors?
- More generally, under what conditions can minors be granted the ability to directly exercise their rights (right to access, to erasure, etc.) and what safeguards can be put in place, particularly as regards the use of their data for commercial purposes?

In this context, in light of the GDPR, it is important **to start a comprehensive discussion on the rights of minors over their personal data**, and on the conditions under which they should be encouraged to exercise them.

For all these reasons, the CNIL has decided to launch discussions on these topics this year, in collaboration with all stakeholders involved, including parents, youths, the educational community and professionals from the digital sphere.

At the same time, the International Working Group on Digital Education - created by the International Conference of Data Protection and Privacy Commissioners and steered by the CNIL - has also started working on best practices to inform children of their rights.