STRATEGIC ROADMAP

2019-2021

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Introduction

In 2016, the CNIL adopted a three-year strategic and operational plan with two main goals. First to make the CNIL – which was faced with major quantitative and qualitative pressure due to far-reaching changes in a society entering the digital age – as an agile, comprehensive regulator committed to joint regulation and inter-regulation. Secondly to create a project to cover an unprecedented period in the Commission's history: the years in which the European General Data Protection Regulation (GDPR) was adopted and came into force.

Three years later, the vision put forward has proved pertinent: thanks to the ongoing commitment of all its teams, the CNIL is extensively repositioned and modernised. The strategic plan enabled a better preparation to tackle its missions and carry them out to good effect over the course of 2018, a remarkable year due to the switchover to a new legal framework, a new, largely Europeanised mode of personal data governance, and a consequent considerable increase in referrals to the CNIL from private individuals and professionals alike.

Major steps have also been taken in 2019. The new legal framework is now in place and European cooperation has become a reality. Nonetheless, there is still some way to go to complete the transformation and to live by a fully disseminated "information technology and civil liberties" culture all over the country.

It is in this context that, in March 2019, the CNIL committed to fresh orientations covering the period 2019-2021. It chose to do so via a progressive, collaborative procedure, involving the Commission's members, managers and staff, who previously got together in crosscutting workshops to gather collective thought and build final orientations.

This strategic roadmap for 2019-2021 sets the priorities for the years to come in order for the CNIL to carry out its public service mission with regards to its various audiences' expectations, and taking into account both the resources available and the European collective's requirements.

Following a phase marked by changes and transitions, this roadmap's **common thread** is **appropriation and achievement, for one and all** (private individuals, professionals and the European collective alike), **of all the GDPR's promises and potentialities**. The 2019-2021 period will be decisive in lending credibility to the new legal framework and in making the ambitious European challenge an operational success. Civil society and economic players have high expectations. The new model helps raise awareness and lays the groundwork for designing regulatory frameworks across the world. In order to remain an efficient and down-to-earth data regulator in this new context and play its role to the full at national and European level alike, the CNIL must test out theories in practice and continue to modernise. Consequently, it has identified **five strategic focuses** to guide its action up to 2021.

1. Giving priority to digital issues in everyday life

Protection of individual rights, further strengthened by the GDPR, has been a key CNIL goal since the Act of 6 January 1978. But the context has undergone far-reaching changes, marked by unprecedented scaling up, proliferation and diversification of personal data processing, along with changes in individual behaviours. Priority must therefore be given to whatever affects citizens' lives most directly, with a view to making the CNIL a trusted ally in their digital daily lives.

Four goals that will ensure our success in doing so:

1. **Facilitate processing of referrals from private individuals**: the quality of processing such referrals (grievances, complaints, indirect exercise of rights, etc.) must be maintained and, more than ever, constitute a priority for the CNIL. In a context where such referrals are proliferating, we must seek to be ever more effective in our actions. To do so, we must use all possible means likely to facilitate recourse to us, simplify internal processing of referrals and increase the usefulness of solutions obtained. In addition to focusing on individual cases, we will be able to achieve these goals by: improving IT tools, optimising the complaint examination management, continuing the development of standard responses to questions, etc.

2. **Diversify publications intended for private individuals**: The CNIL must step up its education role towards private individuals, who should be identified as the main target of its actions, young people in particular. Greater importance must be given to publications dedicated to the most common everyday-life issues. New communication formats (videos, tutorials, practical advice, etc.) will be developed to enable a better understanding of the issues involved. Furthermore, the number of contents dedicated on children's rights will be increased and given greater visibility.

3. **Provide greater clarity**: the CNIL must improve the clarity and intelligibility of its communications towards private individuals. This would include turning key responses, practical recommendations and digital tools on questions that affect them most directly so that they can be enabled to protect themselves effectively in their digital daily lives. When preparing a new work, we must anticipate the public communication which will be entailed. It will be intended for both private individuals faced with the issue at stake as well as the professionals who process their data, with a view to enlisting their help and raising their awareness more directly. Contents must be made as simply worded and accessible as possible without any loss of precision.

4. **Increase the focus on digital daily life in all the CNIL's actions**: in addition to its missions in direct contact with citizens (informing the public, processing referrals, etc.), the CNIL must carry out its missions with regards to private individuals' digital daily lives as it aims at increasing their control over their data in very practical terms. Questions and devices that affect people most directly in their private and professional lives must be at the heart of our work either when we provide advice to professionals, conduct oversight, make technological watch, promote technologies that protect private life or we advise the public authorities. .

2. Ensuring balanced data protection regulations in the era of the GDPR

The CNIL's "repressive" actions have gained added momentum with enactment of the GDPR, and the CNIL must commit itself fully in this respect. At the same time, the CNIL must ensure that data protection becomes part and parcel of professionals' behaviour and everyday culture, a condition essential to the GDPR's success and the legal security of its actions. The CNIL will therefore continue to "walk on both feet" in a balanced and coordinated way, by providing support and taking repressive action.

Four goals that will ensure such balance in the new legal context:

1. **Better target and promote our support offer**: in order to optimise the effectiveness of its support offer in the context of the resources it is allocated with the CNIL must base it mission on a clearly defined strategy, fully disclosed to the public, ensuring tiered prioritised support to collectives, professionals and civil society, as well as to the types of data processing which, due to their nature or scale, have the greatest impact on citizens and tomorrow's world. The positions taken by the CNIL in such context must then be disseminated more widely (to the public, to "network heads", to delegates, etc.). The CNIL's and its actions' visibility must be improved in order to increase their effects, by seeking partnerships with key players closely connected with companies of all sizes, on a daily basis.

2. **Adapt to professionals' maturity and varying needs**: in order to give legal security to all professional actors as well as to facilitate their interpretation of the GDPR without actually advising them individually, the CNIL must better adapt what it says according to professionals' needs and levels of expertise. It must ensure that what it produces is easily understandable by small and medium-sized concerns in particular; and that new, more practical compliance tools are made available to them. Consideration of the specificities of various types of bodies – SMEs/VSEs, local authorities and their groupings, various associations, etc. – now constitutes a focus in its own right. The CNIL website's clickstream will also be redesigned to take account of the variety of needs. Eventually, organisations should be able to self-assess their levels of preparation and draw their conclusions on compliance actions they possibly need to implement.

3. **Make repressive action more visible**: Now that the CNIL's repressive powers have been increased, it is essential that organisations have better knowledge of control and sanction procedures. The many actions carried out by the CNIL in the context of complaint processing and oversight missions should be more highlighted (on the website and with professional federations) with a view to relaying the best and worst practices observed, and therefore to maximise the usefulness of solutions found in individual cases.

4. **Better coordinate sanctions and support**: The strengthening of the CNIL's repressive powers also involves an increased risk of litigation. To a wider extent than at present, this new context requires delicately handled, flexible coordination between its services on numerous cases and work programmes, in order to safeguard actions taken by the CNIL. Such coordination must also incorporate professionals' expectations, whose understanding of the CNIL's position and approach must be made clear in their various exchanges.

3. Promoting data diplomacy

The GDPR requires the CNIL to be fully committed to the European cooperation. Active participation in the European collective's work is both a legal and a political necessity: the new European data governance model is the key to true European sovereignty in this area and also reinforces the impact of actions taken at national level. The CNIL must therefore contribute to the European collective's success by promoting its own vision, based on its long experience as regulator. Reaching beyond the European circle itself, and within the limits of its resources, the CNIL must play an active part in international data geopolitics in concert with French diplomacy.

These imperatives will be ensured by achieving three goals:

1. **Incorporate European cooperation into the CNIL's work on a daily basis**: Europeanisation of the CNIL's activities, which is already well underway, must be definitively completed. Internal operating procedures and methods must henceforth be fully adapted to the European era. A reinforced strategy of cooperation with other national supervisory authorities must also guide this new cooperative approach, in order to facilitate joint work, emergence of a common culture, and greater effectiveness visible to all eyes.

2. **Play a leading role within the European collective**: the CNIL's expertise is unanimously acknowledged in Europe. In order to maintain and further enhance its added value and contribution to European work, the CNIL must both optimise its targeting strategy at European level and manage for efficiently its activities relating to the European Data Protection Board (EDPB). The CNIL must also ensure that the European collective's work is better known in France by the public authorities, institutions and the public at large.

3. **Make the CNIL's voice heard internationally**: reaching beyond the European collective itself, the CNIL will keep carrying weight at international level as the coming years will see major data privacy geopolitical balances come into play. To the extent of its resources, the CNIL must therefore develop new relays and levers of influence at this level with other public authorities, French diplomacy in particular, and other networks ("Francophonie" or French-speaking network, for example), on legal and technical matters of major strategic importance.

4. Providing up-to-the-minute public expertise on digital technology and cybersecurity

The CNIL must take an active part in the implementation of new forms of IT regulation, in which data protection is of key importance. It possesses acknowledged expertise in such regulation, and the CNIL will further develop it. In order to bring more complete responses to the challenges it encounters, as well as to provide the State as a whole with an overall capacity for effective response, it must promote and participate in the networking of expertise and tools with other components of the digital State. Overall, regulation cannot be based on legal and technological expertise alone: the CNIL will carry on with its commitment to involve other approaches such as economic and ethical approaches in particular.

Four goals express this strategic focus:

1. **Deepen the CNIL's technical expertise**: in order to remain capable of legal and technical mastery of an increasingly complex ecosystem, the CNIL must further increase its level of expertise, which must always keep pace with the levels of major private actors. Every lever for improving such competence must be activated, in terms of training, investigative tools and cooperation with similar authorities, or other public authorities competent with regard to digital technology, as well as the research world.

2. **Promote the CNIL's vision of digital technology and innovation**: the CNIL has no monopoly on such regulation and has no such vocation. However, due to its long experience as a regulator, it is unique in its ability to assert the diversified, horizontal character of its field of intervention and the items that it regulates: personal data, the digital world's guiding thread. The CNIL must therefore contribute to the debates that shape the vision of digital technology and its regulation. It will promote its vision of innovation and experimentation in the GDPR era, along with the consequent concrete actions that it carries out in support of private and public entrepreneurs.

3. **Make inter-regulation more of a reality**: although there has been a modicum of progress here, there is still some way to go before inter-regulation of digital technology, with other public authorities, comes into its own. Yet this is the only way to meet the challenges posed by the rise of digital technology, which affects every individual and entity in all their activities and cannot be covered in a single public policy or regulatory framework. This being so, the CNIL is convinced that inter-regulation must be made more of a reality, by exchanges on specific projects and further joint work between regulators.

4. **Disseminate the ethical approach**: just as IT regulation can only be effective if public authorities are networked and pool their resources, legal and technical approaches – the CNIL's core activity – are not enough on their own to assimilate the changes underway and protect individuals to the full. The CNIL must therefore extend the multidisciplinary of its approach. In line with the path it has taken for some years now, it will continue its commitment to the field of ethics, in collaboration with other public operators involved in the debate, further promoting the ethical considerations already presented in its products.

5. Embodying an innovative public service that holds fast to its values

The CNIL must be exemplary in the performance of its missions as well as in its dealings with its employees. Entrusted with the protection of fundamental rights, its actions must reflect the humanist values of its DNA, especially at a time when digital technology is transforming social and professional relationships and is creating new opportunities and seeing new risks emerge. The CNIL must also build on the advantages provided by the digital technology in developing internal tools and in strengthening its relationship with the public. These imperatives form the cornerstone of the CNIL's actions, essential to perform its public service mission.

Four goals result from these requirements:

1. **Listen more closely to its audiences**: regulation of personal data in the digital world cannot be carried out "in chambers"; on the contrary, it requires a continuous confrontation with reality and a checking of the validity of the CNIL's actions and decisions over time. Assessing the impact of the CNIL's actions and measuring the satisfaction of the CNIL's public are essential. Its course of action must finally be more innovative, more focused on its public's usages by increasing the exploitation of the alerts and numerous weak signals it receives.

2. **Know itself better and integrate better**: in addition to tools and procedures, consolidation of the CNIL's collective identity will also be achieved by increasing work on integration around a core of shared values, a greater capacity on the institution's part to integrate new staff, and maintenance of friendly, benign professional and human relations in a context of rapid evolution of its framework for action.

3. **Improve collective work within the CNIL**: the CNIL's internal cohesion is a necessity now more than ever as to ensure the legal security of its actions, to facilitate its employees' work as well as to maintain - or reassert - the ties that bind them, in the context of an increased and renewed workforce. Practical tools ensuring transversality (knowledge management, intranet, circulation of information, etc.) must therefore be modernised, as part of an ambitious digital transformation plan.

4. **Create a CNIL "employer brand"**: a collective identity and ways of working must constitute the CNIL's specificity as a public-sector employer. This will also happen through an efficient management of its members of staff's careers (internal and outside) and skills, which needs to be further formalised. These are the bases to ensure the quality of the CNIL's collective work, to contribute to recruitment attractiveness, and on which the CNIL must implement a real "employer brand".