Termination of the contract and the fate of personal data

Emmanuel Netter

Termination of the contract and the fate of personal data

This is the translation of an article originally published in French in
AJ Business Contracts - Competition - Distribution, October 2019, p. 416

Emmanuel Netter, Professor of private law
Avignon University, LBNC (EA3788)

contact@enetter.fr

The subject entrusted to us supports two different interpretations. In it natural sense of reading, from left to right, it reveals first of all "the termination of the contract", and only then "the fate of personal data". It would then be necessary to look at the question of knowing, since a convention has disappeared, what should be done with the processing of personal data for which it constituted the necessary basis. Reading the subject from right to left, on the other hand, reverses the chronology; it reverses the cause and the consequence: this time, the (bad) management of the data is the reason why the contract ended.

There is certainly some artifice in dealing, in a single contribution, with two issues that are intellectually quite distinct. But it would be lazy to dismiss one of them, when they are equally rich in theoretical and practical difficulties. We shall therefore consider the fate reserved for data as a cause of extinction of the contract (I), and then the fate to be reserved for data as a consequence of the extinction of the contract (II). It should be pointed out that the only contract to be considered here will be the one between the data controller and the person from whom the data originates, inasmuch as specific contributions during the symposium are dedicated to contracts between joint data controllers on the one hand, and to contracts between data controllers and processors on the other.

I - The fate of the data as a cause of termination of the contract

When a data controller behaves improperly with respect to the personal data it handles, the possibility of a breach of the GDPR is immediately considered. [1]But in some cases, the same conduct will also constitute a breach of a contract with the data subject, for example in the form of a privacy policy. In such cases, two analyses are possible. One can consider that what is first and foremost violated is a general and impersonal norm, a legal norm in the broadest sense - whether it is the GDPR, the french Data Protection Act or a decree - which would argue in favor of tort

1 In this sense, V. A. Danis-Fatome, "Quelles actions judiciaires en cas de violation du RGPD? "CCE, April 2018, file 18, note 23: "In the event that a contract between the data subject and the data controller constitutes the basis of the processing, the obligations incumbent on the latter could be of a contractual nature and their violation could lead to liability of this nature. However, it should be recalled that contractual obligations are not in principle intended to impose rules of conduct (V. G. Viney, P. Jourdain and S. Carval, supra note 10, no. 168-1). The obligations contained in the RGPD will therefore in this case retain a legal nature and will therefore lead to tortious liability".

liability. Or one can, considering that the parties' predictions have been thwarted, apply the remedies for non-performance of the contract. From this will arise well-known differences in legal regimes: should the controller be given formal notice, can one request the forced execution of the agreement, raise an exception of non-performance, obtain compensation for damage even if it was not foreseeable at the time of the conclusion of the contract, invoke the mechanisms for fighting unfair terms? We will try to analyze the nature, contractual or extra-contractual, of the breaches attributable to the data controller (A) before drawing consequences with regard to the applicable sanctions (B).

A - Defaults

Let's start with simple hypotheses: a person wants to run a social network account, have an e-merchant deliver to his home, entrust his employer with information as part of their work relationship. Here, a contract unites the person concerned with the data controller, and its proper execution makes it necessary to handle personal data. Do the duties of the data controller under the GDPR also have a contractual nature?

1- Identify contractual obligations

In some cases, the response seems clearly positive: when the data controller describes the purpose of the processing, the type of data collected, the storage periods, the recipients of the data, whether or not they circulate outside the European Union. By virtue of the transparency obligations (Art. 12 ff. GDPR), these points have necessarily been included in the Convention. They do not constitute a mere identical restatement of legal norms, but rather apply abstract requirements to the concrete case, giving them life: are the data kept for one month, six months, one year? The regulation does not provide the answer, but obliges the contract to provide one[2].

The analysis is very different if we consider the order given by the GDPR to the controller to appoint a data protection officer, to keep a register of processing operations, to conduct an impact assessment. These duties will rarely be included in the contract. If they were, the agreement of the parties would merely recall their existence without specifying them or adding anything to them. Finally, it is difficult to consider that these duties are enacted in the individual interest of each of the persons concerned by the processing operation taken in isolation. For all these reasons, it seems difficult to see them as genuine contractual claims.

In between these two series of cases, which are easy to classify, there is a grey area. The obligation of the data controller to implement adequate means to ensure the security of the processing is undoubtedly part of it. Even if it is not expressly stipulated, the judge could easily "discover" it within the contract on the basis of article 1194 of the french Civil Code. Each of the persons concerned by the processing can easily justify that they have a clear and direct personal interest in the proper performance of this obligation. But is the contractual qualification in his interest? Perhaps, if it wishes to argue a defect in the organization of security to raise an exception of non-

2 The reasoning could be even more subtle. Suppose that the privacy policy has retained a data retention period of one year, whereas the CNIL considers that in such a situation, it should not exceed six months. Keeping the data for more than one year is a breach of contract. Retaining the data for eight months is a breach of the agreement but potentially a violation of the RGPD, and therefore a tort.

performance and thus stop payments. Probably not, if she acts in civil liability and wants to obtain compensation for even unforeseeable damage - think of the victims of the security flaw in the network of marital infidelity "Ashley Madison", some of whom have committed suicide[3].

2 - Identify the contracts

It was already difficult to reason from the simplest case: that of a processing of personal data based on its "necessity for the performance of a contract". Let us now assume that a basic contract still exists, but that the processing envisaged is not necessary for its execution: it is Google that proposes to the Internet user to display targeted advertising, or the e-merchant that suggests to him to save his credit card data for a future purchase. In this case, the basis of legality proposed by the GDPR is "consent for one or more specific purposes" (art. 6, a). This processing, which is optional and detachable from the main contract, will nevertheless be described in a privacy policy as part of the transparency obligations. The document will implicitly oblige the person in charge to respect the purposes, storage periods, etc. described therein. Isn't this a form of pollicitation? Isn't the special consent contemplated by the GDPR an acceptance then? The answer seems to us to be positive, and the fruit of the meeting of wills is then annexed to the basic contract - it can be expunged from it if the consent to the specific purpose is taken up again, which it should be possible to do without consequence, in principle, for the underlying contract (art. 7,4).

A similar reasoning may be proposed when the processing is based on special consent, in the absence of even a basic contract: a commune collects the email addresses of volunteer residents to keep them informed of the progress of work on the public roads; a school offers students who so wish to have their photo in a school magazine. The treatment proposal, once accepted, forms a contract - which is not attached, here, to a pre-existing agreement. This again makes it possible to address certain reproaches to the person in charge of treatment in the field of remedies for non-performance of the contract.

Finally, even outside these two bases of lawfulness (necessity for the performance of the basic contract and specific consent), it may happen that the processing takes place, so to speak, within the sphere of influence of a pre-existing contract. Let us imagine that a GAFA claims to process information about a user on the basis of his "legitimate interest" (6, f) because it improves the security of the service, but that it actually resells it to a third party for the purpose of targeted marketing. Or that an employer processes the withholding tax rates of its employees to meet a legal obligation (art. 6, c), but takes advantage of this to classify them according to the supposed wealth of their households and draw consequences with regard to the premiums to be paid to them. From these two misuses of purpose, it would seem logical that one can draw consequences in the framework, for the first, of the online service contract, and for the second, of the employment contract, as they constitute serious disloyalties.

Thus, in many hypotheses, the failures of a data controller are likely to be considered through a contractual prism.

3 M. Untersinger, "Suicides, resignation, blackmail: the tragic consequences of the hacking of the Ashley Madison dating site", article lemonde.fr of December 10, 2015.

B - Sanctions

If, by following the methods that have just been set out, it is possible to identify genuine contractual breaches on the part of the controller, all the usual remedies for breach of contract can theoretically be used. In particular, judicial termination of the contract, contractual civil liability or a combination of both may be sought.

A more incongruous question is whether a breach of the GDPR can simultaneously constitute a cause of invalidity justifying the retroactive annihilation of the agreement. Let us note here that the reading grids of data law and civil law do not overlap. Thus, the CNIL's deliberation of January 21, 2019 in the Android case states that Google's privacy policy was not understandable by ordinary users, and moreover that consent to processing was not given by a clear positive act[4]. Taken at face value by the civilist, this reasoning should mean that there was no real meeting of the minds and therefore the appearance of a contract can be defeated by way of an action for nullity. However, the CNIL conducts an abstract reasoning, at the level of the users as a whole, where the civil judge brought to rule on a defect of consent should carry out a concrete control individual by individual. Moreover, the civil law does not seem to us to have instruments allowing such a demanding and pragmatic examination, on the one hand of the clarity of the offer, and on the other hand of the clarity of the acceptance, as that carried out by the independent administrative authority on the basis of the GDPR.

II - The fate to be reserved for the data as a consequence of the termination of the contract

We will postulate here that a contract has ended. This may be due to the behaviour of a party, by the simple arrival of the term, by the play of a condition; the termination may be retroactive or not. In any case, the contract will take in its fall a certain number of data processing operations for which it was the necessary support. The natural slope of the GDPR is then to order or allow the deletion of the information concerned (A). However, this is only a principle, which must be subject to useful exceptions: there are data that deserve to survive the contract that gave birth to them (B).

A - The principle: data deletion

This is one of the main principles of the GDPR: data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed" (art. 5, e). When the disappearance of a contract leads to the disappearance of the purposes of processing, the data controller should therefore spontaneously draw the consequences and, in principle, delete the information. The alternative would be to anonymize them, which implies definitively preventing any re-identification of the data subjects, but this often proves very difficult, and sometimes impossible. Assuming that this spontaneous deletion by the data controller has not been carried out, it could take place on the initiative of the data subject, on the basis of the right to erasure (art. 17). If the contract has been erased without retroactivity, the a) will be mobilized: "the personal data are no longer necessary in relation to the purposes (...)". If it has been

4 Deliberation SAN-001 of January 21, 2019.

retroactively cancelled, the processing that was based on this contract must be considered unlawful from the outset, which refers to d).

These principles having been recalled, it should be noted that their implementation is not without its sometimes considerable difficulties. It should first be noted that, if the data controller is required to prove that it has erased the data, it will have to prove a negative fact - that there are no copies left anywhere - which is almost impossible.

The extent of the deletion can be a first difficulty. Let's imagine a social network user who closes his account: the contract that founded the treatment ends. Should the platform erase the conversations in which he was only one of the interlocutors, at the risk of damaging the data of others? Or should the lines corresponding to his interventions be censored?

A second, considerable difficulty is the precise moment at which the deletion must take place. When a lawyer, in an advisory relationship, has episodic contact with a client, when is it considered to be the end of the service[5]? The solution consists, after 12 months without any new event, in taking the file out of the "active base" accessible to the firm's lawyers, and placing it in an archive, from where it can only be retrieved by the archivist, upon presentation of a sufficient reason. Archiving thus drastically restricts the people likely to access the information, and reduces the risks to the privacy of those concerned. The interest is twofold: to be able to retrieve the file if the customer relationship comes back to life, but also, of course, to keep proof of the advice given in case of litigation. However, archiving itself poses formidable problems. A lawyer and DPO says that, according to the CNIL, only data potentially useful in the context of litigation should be kept, a highly speculative sorting exercise, if at all possible[6] . The same reminds that in civil law, some limitation periods have sliding starting points with a deadline 20 years after the birth of the law (art. 2232 of the Civil Code), which could delay the deletion of archived data long after the end of the contract.

We can already see this now with the question of intermediate archives: the application of the GDPR is not incompatible with certain hypotheses of data conservation well beyond the termination of the contract. Let us develop this question in conclusion.

B - Temperaments: data retention

Certain rights to keep the data beyond the disappearance of the contract are recognized, both for the benefit of the data controller and for the benefit of the data subject.

1 - For the benefit of data controllers

For the benefit of data controllers, the GDPR provides for certain derogations from the right to erasure. The hypothesis of processing remaining necessary "for the establishment, exercise or defence of legal claims" is expressly provided for (art. 17, 3, e). Processing for "statistical purposes" may also continue (d). The question that arises here is that of the long-term memory of organizations. For their actuarial services, insurers must keep a permanent record of the outcome of the guarantees issued, associated with the risk profile. These are indeed "statistics", and it is

5 A close problem is posed by user accounts for online services that remain inactive for a long time without being closed. The privacy policy should provide that after a certain period of inactivity, the data is deleted.

6 Interview with Me Lorette Dubois dated March 20, 2019.

sometimes even possible to anonymize the data sets, which makes them fall outside the scope of the regulation. On the other hand, let us imagine a criminal law firm wishing to preserve the memory of the defenses insured at the trial: some files are almost impossible to separate irreversibly from the identity of the defendant client, and this is not strictly speaking a matter of "statistics". The solution may lie elsewhere. The GDPR sometimes admits that a new processing operation may be carried out on data already in possession, provided that the new purpose is "compatible" with the original purpose (art. 6,4). In such cases, the text is deliberately abstract, in order to gain flexibility, and uses vague criteria: "the possible existence of a link between the initial purposes" and the new purposes, the "context in which the personal data were collected", the "possible consequences" of further processing for the data subjects, or the existence of "appropriate safeguards". The inevitable counterpart of this flexibility is the weakness of the legal certainty provided, and the risk of diverging interpretations between supervisory authorities and data controllers.

2 - For the benefit of the person concerned

Finally, the outright destruction of data is sometimes avoided, this time to the benefit of the data subject, who wishes to dispose of it as he or she sees fit.

He can dispose of it for himself. In particular, it will be able to exercise its right to portability (art. 20 GDPR), if it does not only wish to know the content of the information that was in the hands of the data controller - for this purpose, the right of access is sufficient - but rather to re-inject this data somewhere - the right to portability guaranteeing here to receive it in a machine-readable and exploitable format. This may involve handing them over to a new data controller competing with the previous one - another email provider, another online photo manager - but also using the data yourself. Indeed, theoretically, the right to portability could be exercised against a supermarket by a customer who would like to carry out statistical analyses on his monthly consumption of fatty products, as revealed by his "loyalty card" data.

The data subject can finally have the data at his disposal for those who will survive him. The solution does not derive from the GDPR, but from the choices specific to French legislation[7]. It is provided that the person can leave general or special instructions as to the fate to be reserved for his data. Such a solution is immune from criticism. On the other hand, in the absence of directives, "the heirs of the person concerned" can access the data to the extent necessary "for the organization and settlement of the estate of the deceased". The death of the data subject may have put an end to the contract that constituted the basis of the processing: the purpose having disappeared, we have seen that the data controller should theoretically delete the information that it used in this context. And yet, he has to prepare himself for heirs to come forward, months later, and ask for access to the information for the proper settlement of the estate. This raises many questions. It would seem excessive to give them access to everything and let them sort it out themselves. Do they have to describe in advance, even approximately, what they are looking for[8]? If so, should their access to

7 Art. 85 of the law n° 78-17 ”informatique et libertés”.

8 The text does not seem to be in this sense, which goes on like this: "As such, the heirs can access the processing of personal data concerning them in order to identify and obtain communication of information useful for the liquidation and distribution of the estate". But it is so badly drafted that it will bear the interpretations that the Court of Cassation will want to make of it. It should be noted in passing that access "to the extent necessary" for the

the data be restricted to a period of time or to keywords related to this query? Who, in the course of these operations, should temper the heirs' appetite for information: the notary in charge of the estate, the data controller himself? It will be up to the practice and to the bereaved families, with the help of the judge, to bring out the concrete solutions that the legislator has clearly lost interest in.

---

settlement of the succession gives way, in the following sentence, to information that is simply "useful" for the liquidation and partition, which is quite different.