1.

WHO Is THIS REPOSITORY ?

This repository provides a framework implemented by bodies governed by private law or public treatment management of unpaid proved, that is to say, cases in which the person concerned is undoubtedly owed a sum of money.

It does not apply to the processing implemented to detect a non-payment risk or to identify violations other than monetary (such as, for example, antisocial behaviour of customers).

Given the particular nature of their activities, this repository does not apply to the treatments put in place by the organizations management and collection of receivables and the investigative agencies, civil.

2.

SCOPE OF THE REPOSITORY

The treatments implemented for the purposes of management of arrears, they are implemented on the basis of tools internal or outsourced to a service provider, lead to collect data about individuals (clients, prospects, suppliers, and any person likely to be in a relationship contract with the organization in the context of the management of its commercial activity). As such, they are subject to the provisions of the RGPD and the law of 6 January 1978, as amended.

The organizations involved, as controllers, must implement all the measures technical and organisational measures to ensure a high level of data protection as personal as the design of treatment and throughout the life of the latter. They must, furthermore, be able to demonstrate compliance at any time. The treatmer ered in the register provided for in article 30 of the RGPD (

see models register on the site cnil.fr
).

The application of this standard allows us to ensure treatment compliance management outstanding in the light of the principles relating to the protection of data. It is also a assistance with the completion of an impact assessment on the protection of data (AIPD) in the cases where it is necessary. The organizations will be able to define the measures to to ensure proportionality and the necessity of their treatment (points 3 to 7), to ensure the rights of persons (points 8 and 9) and control their risks (paragraph 10). To this end,

the organization may refer to the guidelines of the CNIL impact analyses relating to the protection of data (AIPD).

3.

OBJECTIVE(S) PURSUED(S) BY THE TREATMENT (PURPOSES)

Treatment of bad debt management can be implemented for the following purposes :

(a)

the census of unpaid proven ;

(b)

the identification of persons in a situation of a non-payment for the purpose of exclusion for any transaction to come.

The information collected for these purposes may not be re-used to pursue another goal, which would be incompatible with the original purpose. Out of any new use of the data must observe the principles of protection of personal data. The processes used must not give rise to interconnections or exchanges other than those necessary to the accomplishment of the purposes above set forth.

Because the more sensitive, this repository is not intended to frame the following treatments :

- prevention of unpaid, including an assessment (*scoring*) in order to determine whether a person is likely to be in a situation of a non-payment ;
- the enrichment of the processing on the basis of information collected by or from third parties ;
- share one-time and/or the sharing of the identity of persons in a situation of a non-payment with third party and/or with other accounts receivable.

3

4.

BASE(S) LEGAL(S) OF TREATMENT

Each purpose of the processing must match one of the legal foundations laid down by the regulation.

The purpose of the exclusion of the person for the entire transaction to come, can be based on **the execution of a contract to which the person concerned is a party.**

In the case where the exclusion decision would be taken in a fully automated way, it is imperative, in application of article 22, paragraph 2(a) of the RGPD, the processing is based on his character necessary for the conclusion of a contract between the person concerned and the body.

The legal basis should be brought to the attention of the persons whose data are being processed as they allow, in particular, to determine their rights.

5.

PERSONAL DATA CONCERNED

In an effort minimization of personal data processed, the organization should ensure that it does collect and use the data which is relevant and necessary in the light of its own needs in terms of management of arrears. It may include data relating to :

(a)

the identification of the person concerned ;

(b)

the means of payment used (see also point 7) ;

(c)

the payment incident (file number, date of occurrence of the unpaid amount of the outstanding reason of the non-payment, etc).

After being assured of the necessity and the relevance of the personal data that it uses, the agency must also ensure, throughout the lifetime of the treatment, the quality of the data it processes. This means in practice that, in accordance with the regulation, the data accurate and up-to-date.

6.

THE RECIPIENTS OF THE INFORMATION

The personal data must only be made accessible to the persons entitled to know in the light of their duties.

The access right must be documented by the organizations, and the access to the different treatments should be subject to measures of traceability (**see point 9 on the security**).

In case of using a sub-contractor, the contract with the agency must make mention of obligations obligations regarding data protection (article 28 of the RGPD). The

Guide sub-contractor

publ

ished by the

CNIL specifies the obligations and the clauses included in the contracts.

To ensure the continuity of the protection of personal data, the transfers of these outside the european Union are subject to special rules. Thus, any transmission of data outside of the EU must :

- be based on a decision of adequacy ; or
- to be framed by binding corporate rules, model clauses, data protection, a code of conduct or a certification mechanism approved by the CNIL ; or
- to be governed by contractual terms *ad hoc* pre-authorized by the CNIL ; or
- to respond to one of the derogations provided for in article 49 of the RGPD.

7.

RETENTION PERIODS

A shelf-life of certain should be fixed according to each purpose. **In any case, the data must not be stored for an indefinite period of time**.

In the case of regularisation of the non-payment, the information relating to the person concerned must be erased from the file identifying the persons in a situation of a non-payment at the latest within 48 hours from the time that the outstanding payment has been actually paid. If the circumstances so warrant, the agency may, on an exceptional basis, to keep the data relating to the unpaid-even if this has been rectified, provided that it can demonstrate that such preservation is necessary and proportionate, in order to prevent their renewal.

In the case of non-regularization, the information may be retained in the file, identifying the persons in the situation of unpaid and excluding the benefit of a service, within the limit of 3 years from the occurrence of the unpaid amount.

In any event, they can be archived, if the person responsible for the processing is the legal obligation (for example, to meet obligations, accounting or tax) or if he wants to be used as an evidence in case of litigation and in the limit of the applicable limitation period.

For more information, you can refer to the guides of the CNIL :

- "
Safety : Archive in a secure manner
"
;
- " Limit the retention of data ".

The data is used for statistical purposes only are more qualified of personal data when they have been duly anonymized (
See the guidelines of the article 29 working party on the anonymisation
).

8.

PEOPLE INFORMATION

A processing of personal data should be implemented in full transparency vis-à-vis the persons concerned.

From the stage of collection of personal data, data subjects should be informed of the terms and conditions of the processing of their personal data under the conditions provided for in articles 13 and 14 of the RGPD.
See
the
templates mention information
.

In the first place, a general notice on the existence of a processing of personal data relating to persons in a situation of unpaid must be given at the time of the conclusion of the contract or for the collection of data. The person must be clearly informed of the possibility that it be recorded if it does not meet its payment obligations.

In the second place, in the event of the occurrence of an unpaid, the person concerned must be informed of the means that it has to regulate its payment, and the possibility that she has to submit its comments and, where appropriate, to request a review of his situation.

In the third place, if the person has not made the adjustment of the payment, it must be informed of his entry in the file, identifying the people in the situation of unpaid and excluding them from the benefit of the provision.

In the fourth place, the people whose data would be kept so that the adjustment has taken place must be specifically informed, in accordance with the principles of fairness and transparency. This information should present the particular circumstances justifying such preservation, and explain in clear terms his character to be necessary and proportionate. In addition, the person must be clearly informed of the period for which the data will be stored, the duration of which may not exceed 1 year from the regularization.

The persons concerned must be informed of how to exercise their
rights
.

9.

RIGHTS OF PERSONS

The persons concerned have the rights following, that they would exercise under the conditions laid down by the RGPD :

- right of**access, rectification and erasure** of the data ;
- right to **limitation** of processing (for example, when the person contests the accuracy of its data, it can apply to the temporary freezing of the processing of their data, the time that it shall make the necessary checks) ;
- right to **portability** : the organization shall permit any person to receive, in a format structured and commonly used, all data processed by automated means. The person concerned may request that their data be transmitted directly by the organization's initial to another organization. Are concerned that the data provided by the person on the basis of consent or contract. Therefore, it is recommended to clarify to the people of the treatments affected by this right to portability.

10.

SECURITY

The organization must take all necessary precautions in regard to the risks presented by its treatment to preserve the security of personal data and, in particular, at the time of collection, during transmission and storage, prevent their being distorted or damaged, or that unauthorized third parties will have access to it.

In particular, in the specific context of this repository, **or the agency shall adopt the measures following it proves their equivalence or the fact you do not need or be able to use** :

Educate users

Raise awareness and inform the persons accessing the data

Draw up a charter it and give it a binding force

Authenticate users

Set a username (*login*) is unique to each user

to Adopt a policy of password that the user complies with the recommendations of the CNIL

Force user to change password after reset

Limit the number of attempts to access an account

Manage permissions

Define profiles of clearance

to Remove access permissions obsolete

Carry out an annual review of the authorisation

Plot the access to and manage incidents

Provide a system log

to Inform the user of the implementation of the logging system

to Protect the equipment logging and the information logged

lay down the procedures for the notification of data breaches to personal

Secure the posts to work

Provide a procedure for the automatic locking of session

to Use anti-virus software is regularly updated
to Install a "firewall" (*firewall*) software
to Collect user consent before any intervention on his post

Secure
mobile computing
Provide a means of encryption of mobile devices,
Make backups or synchronize data
Require a secret to unlocking ordiphones
Limit the stream network to the strict minimum necessary

Protect the network
's in-house it
Secure access to remote computing devices nomadic by
VPN
implement the protocol, WPA2, or WPA2-PSK for the network Wi-Fi
Secure servers
Limit access to the tools and management interfaces, the only
persons authorised
to Install, without delay, the critical updates that
Ensure availability of data
Secure web sites
Use TLS and verify its implementation
to Verify that no password or username is not incrporé the URL
, Check that user input is
expected
to Put a strip of consent for *cookies* that are not necessary to the
service
Save and provide for
the continuity of activity
Perform regular backups
Store backup media in a safe place and
Provide a means of security for the transfer of backups
Provide and regularly test the continuity of activity
Archive them
secure
Implement specific modalities for access to data
archived
Destroy the archives obsolete in a secure manner
Oversee the
maintenance and
destruction of
data
Save the maintenance interventions in a handrail
Frame by a responsible officer of the body interventions by
third parties
to Delete the data of any of the material prior to its disposal
Manage the sub-
contracting
Provide specific clauses in the contracts of subcontractors to
Provide the terms and conditions of return and destruction of the data
ensure the effectiveness of the safeguards provided (security audits, visits,

	etc.)
Secure exchanges with other organizations	

Encrypt the data before sending them to
ensure that it is in the proper recipient
to Transmit the secret by sending separate and via a different channel
Protect the premises
Restrict access to the premises through locked doors,
Install alarms and anti-intrusion, and check them periodically
Frame the
developments in
computer
Offer default settings respectful of privacy for
end-users
to Avoid areas of open-ended comments or strictly
Tested on phantom data or anonymised
Use functions
cryptographic
Use of algorithms, software, and libraries recognized
to Keep the secrets and cryptographic keys in a secure manner

To do this, the organization may usefully refer to the
Guide to data security
personal
.