## 1.

## WHO Is THIS REPOSITORY ?

**This repository oversees the implementation by organizations of private or public law, of their files "customers" and " prospects ".**

Given the particular nature of their activities, this repository does not apply to treatments work by :

- the health facilities or education ;
- the banking establishments, or similar ;
- insurance companies ;
- the operators subject to the approval of the regulatory Authority of online games.

## 2.

## SCOPE OF THE REPOSITORY

The treatments implemented for the purposes of managing business activities, whether they are implemented from internal tools or outsourced to a service provider, lead to collect data relating to individuals (customers, 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), law of 6 January 1978, as [illegible] specific provisions relating to

the protection of privacy in the electronic communications sector.
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 treatments implemented must be entered 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
trade in the light of the principles relating to the protection of data.
It is also an aid to the completion of an analysis of impact relative to the protection
data (AIPD) in cases where it is necessary. The organizations will be able to define
their measures to ensure the proportionality and the necessity of their treatment
(points 3 to 7), to guarantee the rights of persons (points 8 and 9) and control their risks
(item 10). To this end, the agency can refer the guidelines of the CNIL on the
impact analysis relating to the protection of data.**

## 3.
## OBJECTIVE(S) PURSUED(S) BY THE TREATMENT (PURPOSES)

Treatment management of business operations can be implemented for the following purposes :
**(a)**
**contract management** (e.g. : management of orders, the delivery, the execution of the service
or the supply of goods, invoices, and payments) ;
**(b)**
**management of loyalty programmes ;**
**(c)**
**bookkeeping general and auxiliary accounting methods that can be
attached ;**
**(d)**
**establishment of financial statistics ;**
**(e)**
**conducting satisfaction surveys and customer studies** , including surveys, test
products, the statistics of sales made by the body concerned ;
**f)**
**claims management, after-sales service and guarantees** ;
**(g)**
**conducting marketing activities and marketing** (sending of messages,
advertising, contests, sponsorship, promotion, survey) ;
**(h)**
**selection of suppliers.**
3
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 :**
- the detection and prevention of fraud ;
- the exclusion of temporary or permanent people the benefit of the provision of services or the
provision of a property (for example, because of unpaid, to incivility from customers or conduct that is
abusive). These objectives are framed by the repository XXXX ;
- the profiling of people. For what concerns the tracking of their navigation, the organization that wants to put
implementation of such treatment shall comply with the deliberation n° 2013-378 of 5 December 2013
on the adoption of a recommendation on the *cookies* and other tracers covered by the article 32-II
of the law of 6 January 1978 and may refer to the dedicated section on the website of the CNIL ;
- the monitoring of attendance and of course customers in physical stores ;
- the enrichment of databases from information collected by third parties.

## 4.

## BASE(S) LEGAL(S) OF TREATMENT

Each purpose of the processing must be based on a legal basis laid down by the regulation. The different foundations, allowing an organisation to process personal data are listed below.

**(a)**

**the consent is free, specific, informed and unambiguous of the person concerned ;**

The consent to be valid, requires positive action and specific to the person concerned (e.g. : a check box dedicated, non-pre-checked). Acceptance of terms and conditions of use, may not be enough : the agreement must be free and not influenced or forced (he may not condition the purchase of a service or the purchase of a property, the creation of an online account for access to a service, *etc*.).

**(b)**

**the execution, or of a contract to which the person concerned is a party**or of measures pre-contractual taken at his request. The data collected must be necessary for the execution of contractual and/or pre-contractual ;

**(c)**

**to respect a legal obligation to the organization ;and**

**(d)**

**the purposes of the legitimate interests pursued by the organization or by the recipient of the data, provided that it does not recognise the interest or rights and freedoms the fundamental of the person concerned.**

A table, below, illustrates through practical examples, the cases in which the legal bases can be selected on the basis of the objective pursued by the processing.

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 the activities of business. This may include data relating to :

4

(a)

**the identification of the person concerned** ;

The internal code used to identify it in the database may not be his credit card number, social security or identity.

If the organization shall verify the identity of a person before entering into business relations with it, the simple presentation of a proof may be sufficient. A copy of this proof can be kept for a period of 6 years when the law so provides or if the organization can justify the need to pre-establish an evidence in case of litigation. In this case, of the enhanced security measures, such as, for example, the limitation of the quality of the scanned image, or the integration of a watermark with the date of collection and the identity of the body, must be implemented in order to combat the risk of misuse of such information, in particular the use of the photographs for facial recognition.

(b)
**the professional life** (for example, to the management of supplier contracts) ;
(c)
**the means of payment used** (see also point 7) ;
(d)
**the transaction and the goods or services you have purchased** (data related to the settlement of bills, in the monitoring of the business relationship, notices, left, claims management, etc) ;
(e)
**the family situation, economic and financial information** of the person or persons involved in the transaction when such data are linked to the business relationship.
Exceptionally, for example if the information is necessary for the purpose of the treatment and if you have an appropriate legal basis, certain information known as " sensitive " (which may, in particular, revealing political opinions, religious or philosophical orientation, sexual or information on the health of the person concerned) may be collected.

A table, below, lists the data that can be collected and processed according to the purposes of the processing. 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.
The transmission of personal data to commercial partners requires, upstream :
- to inform the persons concerned on the support of data collection (online form, or paper form) the purpose of this transmission, and categories of recipients concerned. The specific list of recipients must be regularly updated and made available to persons from the same media (for example, by including a hyperlink) ;
- collect the consent (see section 4.(a) persons when these business partners

have a calling to do their own marketing by electronic means (for text messages,
e-mails, faxes, or automatic calling machines). The consent of the individuals collected for this purpose must be maintained for purposes of proof ;
- allow people to oppose it when the exploration is carried out by post or by the
through a phone call.
5
Data designated as " sensitive ", as referred to in point 5 may be passed on to third parties.
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
- respond to one of the derogations provided for in article 49 of the RGPD.

## 7.

## TIMES OF CONSERVATION

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**.
E.g. : the security code of the credit card should be removed as soon as the payment for the service or
the purchase was made. In contrast, the number of a payment card may be kept to allow for
future purchases under the conditions laid down by the
recommendation on the processing of the card
payment terms of the sale of goods or supply of services at a distance
.
The data necessary for the performance of a contract are kept for the duration of the contractual relationship.
They can also be kept :
-
for a period of 3 years from the last contact that the persons to which they relate
have been with the organization (e.g., for customers, a purchase or the date of expiration of a guarantee, warranty, or for the prospects, with a click on a hyperlink in an email) ;
-
after the execution of the contract, in filing intermediary, if the controller has the obligation
by law (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 the commercial activities that involve the creation, by the customers themselves, an online account (for example, online dating sites or social networking), the data are intended to be retained until the
deletion of the account by the user. However, it is common that users no longer use these accounts
are not clear, which leads to sustained indefinitely. In this case, a reasonable period of time (e.g. :
2 years) should be determined, after which the accounts are to be classified as inactive. It should then
notify the affected users, and to delete accounts of those who have not responded within the time limit
set by the organization.
**When a person exercises his right of objection to receive from prospecting**, to ensure
its effectiveness, the information allowing to take into account this law shall be kept for at least
3 years. These data may in no case be used for purposes other than the management of the right of opposition, and
only the data necessary to take into account the right of objection must be preserved (e.g. :
e-mail address).
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
).
6

## 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, individuals 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 models of reference information.

According to the aim pursued and the data collected, the consent of the person (e.g. : in case of transfer of electronic data for purposes of commercial prospecting), or a way to object to certain processing operations (e.g. : prospecting for similar products or services, exploration between professionals or postal mail) must also be provided on the data collection form.

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 to **withdraw consent** or to**object** to the processing of their personal data ;
- right of**access, rectification and erasure** of the data ;
- right to **limitation** of processing (e.g. : when the person contests the accuracy of its data, it may apply to the agency, 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.

Any organization wanting to implement the commercial prospection by telephone will have to be removed from its list of the individuals on the list of opposition as provided by articles L. 223-1 and following of the code of consumption (so-called list " BLOCTEL ").

## 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 clearance

Remove the 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 violation de données à caractère
personnel
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
Provide a means of encryption of mobile devices,
Make backups or synchronize data
Require a secret to unlocking ordiphones
Protect the network
's in-house it
Limit the stream network to the strict minimum necessary
to Secure the access to remote computing devices nomadic by VPN
implement the protocol, WPA2, or WPA2-PSK for Wi-Fi networks
Secure servers
Limit access to the tools and administration interfaces to only those
authorized
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 embedded in the URL,
Check that the user input corresponds to what 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 archived data
to 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 subcontracting
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 agencies
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 to the users
end
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 the security of personal data
.
8

# PRACTICAL ILLUSTRATION OF BASES LEGALES IN THE LIGHT OF THE OBJECTIVES

Orders, deliveries, service
after-sale
Performance of the contract
Duration of the contractual relationship
Accounting requirements, tax,
etc
To Respect a legal obligation to
retention of data (e.g. : obligation
to ensure the identity of the person
requesting the provision of a proof
identity)
In the form of archive intermediary :
legal retention (e.g. :
obligation of accounting to 10 years)
For instance, the management of pre-
litigation and litigation
Legitimate interest of the organization to
the establishment of proof of a right or
of a contract (e.g. : in case of legal proceedings)
Duration of the prescription-related (civil,
commercial, etc)

By electronic means (for
sending e-mail, SMS, robotic
voice, etc)
Consent
Until the withdrawal of consent or
3 years from the last contact
By post or response
human
Legitimate interest of the agency subject to
allow people to oppose it
prior to and at any time
Destination of professionals
For goods and services
analogues

Electronic data (for
sending email, SMS, automatic
call, etc)
Consent
Until the withdrawal of the consent
Transfer of your data only
to contact people by
phone or postal mail

Legitimate interest of the agency subject to
affixing or to comply with a law
objection (*opt-out*).
Until the exercise of the right of opposition

Specific consent
Until the withdrawal of consent or
date of expiry of the bank card.
9
Conservation of the card number
bank to facilitate purchases
subsequent (non crypto)
Legitimate interest
For customers who opt for a
subscription "premium" / " to
will " to receive,
free or not, service
appendices to facilitate their purchases
(fast delivery, private sales, access
additional content, etc).

## DATA THAT CAN BE COLLECTED AND PROCESSED IN ACCORDANCE WITH THE OBJECTIVES OF THE TREATMENT

Title, name or corporate name, first name, address (including head office, place billing) n° of
phone, fax no., email address, date of birth, code internal to treatment, allowing
the identification of the client, identification code book, SIREN number.

Married life, number of persons in the household, number and age of child(ren) in the home,
profession, field of activity, socio-professional category, the presence of domestic animals.

Profession, in the category of economic activity.

Payment, terms and payment terms (e.g. : discounts, down payments, dividends), RIP/RIB, n° of
cheque, credit card number, date of end of validity of the credit card security code,
credit terms, duration.
Discounts granted, receipts, balances and loans (amount and duration, name of the lender)
in case of financing of the order by credit.

Number of the transaction, the details of the purchase, subscription to, the property or service is subscribed to.

Requests for documentation, testing applications, articles, purchased products, services or subscriptions
subscribed to, services which are the subject of the order and the invoice, quantity, amount, frequency, date
and amount of the order and the invoice due date of the invoice, conditions and delivery address,
purchase history and benefits of service, return of product, the origin of the sale (vendor,
representative, partner, affiliate).
The orders, invoices, correspondence with the client and after-sales service, exchange, and
comments of customers and prospects, person(s) in charge of the customer relationship.

Data necessary for the realization of the actions of loyalty, exploration, study, survey,

test, product and promotion, the organisation and treatment of the contests, sweepstakes and any promotional event such as the date of participation, the answers to the games, contests and the nature of the lots offered.

The data relating to the contributions of individuals filing of the notice on the products, services or content, including their nickname.

*Cookies* and other tracers in the respect of the recommendation n° 2013 378 of December 5, 2013.