Deliberation 2021-130 of September 23, 2021Commission Nationale de l'Informatique et des LibertésLegal status: In force Date of publication on Légifrance: Tuesday April 12, 2022NOR: CNIL2210112XDeliberation no. of personal data used for the purposes of managing unpaid bills in a commercial transactionThe National Commission for Computing and Liberties,

Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in particular its article 58 ;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 8;

Having regard to Decree No. 2019-536 of May 29, 2019 taken for the application of Law No. 78-17 of January 6, 1978 as amended relating to modified computing, files and freedoms; Article After hearing Mr. François PELLEGRINI , Commissioner, in his report, and Mr. Benjamin TOUZANNE, Government Commissioner, in his observations;

Adopts a standard relating to the processing of personal data implemented for the purposes of managing unpaid bills in a commercial transaction.APPENDIXREFERENTIAL

RELATING TO THE PROCESSING OF PERSONAL DATA IMPLEMENTED FOR THE PURPOSES OF MANAGING UNPAID IN A COMMERCIAL TRANSACTIONYou can consult the full text with its images from the extract from the authenticated electronic Official Journal accessible at the bottom of the page1. Who is this reference aimed at? This reference offers compliance solutions for the implementation by private or public law bodies of a processing of data for the management of proven unpaid bills, i.e. the cases in which the person whose data is processed is indisputably liable for a sum of money. It relates more specifically to unpaid debts following a commercial transaction relating to goods or services.

It does not apply to the processing implemented to detect a risk of non-payment or identify non-monetary breaches (such as, for example, customer incivility).

Given the specific nature of their activities, this standard does not apply to the processing implemented by: - debt management and collection organizations;

- civil investigation bodies;

- banking or similar establishments;

- insurance companies.2. Scope of the repositoryThe processing implemented for the purposes of managing unpaid bills, whether implemented using internal tools or outsourced to a service provider, leads to the collection of data relating to natural persons who are customers of the 'organization. As such, they are subject to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on free movement. of these data (hereinafter "GDPR") and the law of January 6, 1978 as amended.

The bodies concerned, as data controllers, must put in place all the appropriate technical and organizational measures to guarantee a high level of protection of personal data from the design of the processing operations and throughout the life of the processing operations. this. They must also be able to demonstrate this compliance at any time. This processing must be recorded in the processing register, in accordance with the provisions of Article 30 of the GDPR (see the register models on the cnil.fr website).

The reference document does not address legal rules other than those relating to the protection of personal data. It is up to the players concerned to ensure that they comply with the other regulations which may also apply.

The application of this reference system, which is not binding, makes it possible to ensure the compliance of the management processing of unpaid bills with regard to the principles relating to data protection. Organizations may choose to deviate from the reference system with regard to the specific conditions relating to their situation, making sure to take all the appropriate measures to guarantee compliance of the processing with the regulations on the protection of personal data. .

Organizations must, in accordance with the GDPR, assess whether their processing is likely to result in a high risk as interpreted by the European Data Protection Board in its “Guidelines on Data Protection Impact Assessment”. data (DPIA) and how to determine whether the processing is likely to create a high risk", in order to determine whether they should carry out an impact analysis or not.

This repository will be regularly updated by the CNIL in order to guarantee its compatibility with the latest legislative and technological developments.3. Objective(s) pursued by the processing (purposes) The reference system provides a framework for the processing operations, the purposes of which are as follows: a) Listing proven unpaid bills;

b) The identification of persons in default of payment for the purpose of exclusion from any future transaction.

The information collected for one of these purposes cannot be reused to pursue another objective that would be incompatible with the purpose defined when it was collected. Furthermore, the processing implemented within the framework of this reference system must not give rise to interconnections or exchanges other than those necessary for the fulfillment of the purposes set out above. This reference system is not intended to provide a framework for the processing responding to the following purposes:- prevention of unpaid bills including an evaluation (“scoring”) aimed at determining whether a person is likely to be in a situation of unpaid bills;

- the enrichment of the processing from information collected by or from third parties;
- the occasional sharing and/or pooling of data relating to the identity of persons in default of payment with third parties and/or with other creditors, excluding subcontractors.4. Legal basis(s) of the processingEach purpose of the processing covered by the reference system must be based on one of the legal bases set by the GDPR.

The various grounds that may be used to process personal data for the purposes of managing unpaid bills in the context of this standard are listed below: a) The performance, either of a contract to which the data subject is party, or pre-contractual measures taken at his request. In accordance with the GDPR, the data collected must be necessary for the execution of contractual and/or pre-contractual measures. In this respect, the EDPS indicates that the fact that the contract concluded between the data subject and the controller mentions the collection of specific data is not in principle sufficient to demonstrate that these data are necessary for the performance of the contract. Thus, to be based on this legal basis, the collection of data must be essential to provide the service or the good expected by the data subject; b) The fulfillment of the legitimate interest pursued by the organization or by the third party, subject to not to disregard the interest or the fundamental rights and freedoms of the data subject. of the contract, however, seems more appropriate.

Furthermore, in the event that the exclusion is decided in a fully automated manner, the processing must, pursuant to Article 22, paragraph 2.a, of the GDPR, be based on the performance of the contract in order to comply with the reference system. .

As provided for by the GDPR, the legal bases must be brought to the attention of the persons whose data are processed since they make it possible, in particular, to determine their rights.5. Personal data concerned In order to minimize the personal data processed, the organization must ensure that it only collects and uses the data that is relevant and necessary with regard to its own needs for managing unpaid bills. This may be data relating to: a) The identification of the person concerned (who may be the debtor as well as the natural person or persons having the quality of guarantor because they have undertaken to fulfill the debtor's obligation in case of default of the latter);

The internal code used to identify the person concerned in the database cannot be their bank card number, nor their social security number, nor even that of their identity document.

If the organization must ensure the identity of a person, the simple consultation of proof (identity document) may be sufficient. When the law provides for it or if the organization justifies needing it to pre-constitute proof in the event of litigation, and this according to the risks of litigation, a copy of this proof may be kept for a period of 6 years. . In this case, reinforced security measures such as, for example, the limitation of the quality of the digitized image or the integration of a watermark bearing the date of collection and the identity of the organization, must be put in place. implemented to combat the risks of misuse of this information, in particular the use of photographs for facial recognition purposes. Similarly, this information must not be kept in an active database but must be stored in an intermediate archiving database. b) To the means of payment used (see point 7); c) To the payment incident: file number , date of occurrence of the unpaid, amount of the unpaid, object of the unpaid (description of the product or service not having been the subject of payment by the person concerned). necessity and relevance of the personal data it uses, the organization must also, throughout the lifetime of the processing, take all reasonable measures to guarantee the quality of the data it processes, in order to to ensure their accuracy, throughout the duration of the processing.

Under this obligation of accuracy of the data it processes, the organization must take specific measures to guarantee that the people excluded from future transactions are indeed those who are in a proven unpaid situation. These measures may include additional checks in case of doubt about the identity of the person concerned or measures to prevent identity fraud.6. Recipients of the information In order to comply with the obligation of data security, personal data must be made accessible only to persons authorized to know it with regard to their attributions within the company's internal departments, departments responsible for controls or with subcontractors.

In the event of recourse to a subcontractor, the contract which binds it to the organization must mention the obligations which are incumbent respectively on each of the parties in terms of data protection (article 28 of the GDPR). The data controller must document the instructions that he sends to the subcontractor and which concern the methods of data processing (Article 22, paragraph 3.a, of the GDPR). The Subcontractor's Guide published by the CNIL specifies the nature of these obligations and the clauses that it is recommended to include in the contracts. In addition, access authorizations must be documented and access to the various processing operations must be subject to traceability measures. See point 10 on safety.

To ensure the continuity of the protection of personal data, transfers of this data outside the European Union are subject to special rules. Thus, any transmission of data outside the EU must, in accordance with the GDPR:

- be based on an adequacy decision; Where

- be governed by internal company rules, standard data protection clauses, a code of conduct or a certification mechanism approved by the CNIL; Where

- be governed by ad hoc contractual clauses previously authorized by the CNIL; Where

- meet one of the derogations provided for in Article 49 of the GDPR.7. Storage periods A precise storage period must be set according to each purpose. Under no circumstances should the data be kept for an indefinite period. In general, retention periods should not, in principle, exceed the durations of legal prescriptions.

The retention periods listed below are proposed. If the organization chooses to keep the data for a longer period than that proposed by the reference system, it must ensure that this period does not exceed that necessary with regard to the purposes for which they are processed. - In the event of regularization of the unpaid, the information relating to the person concerned should be erased from the file listing the people in a situation of unpaid within 48 hours following the observation of the regularization by the organization or from the moment when the unpaid has been actually settled;

- In the event of non-regularization, the information can be kept in the file listing the people in a situation of unpaid and thereby excluding them from the benefit of a service, within the limit of 5 years from the occurrence of the 'unpaid. In any event, they can be archived if the organization has a legal obligation to do so (for example, to meet accounting or tax obligations) or if the organization wishes to constitute evidence in the event of litigation. and within the applicable limitation period.

To find out more, you can refer to the CNIL guides: Security: Archiving securely "; Limiting the retention of data ". Data used for statistical purposes is no longer qualified as personal data when they have been duly anonymized (see G29 guidelines on anonymization) .8. Information of personsThe processing of personal data must be implemented in complete transparency vis-à-vis the persons concerned.

From the stage of the collection of personal data, individuals must be informed of the procedures for processing their data under the conditions provided for by the provisions of Articles 13 and 14 of the GDPR. See the information notice models on the website www.cnil.fr.

In accordance with the GDPR, the organizations must implement the following information methods:- firstly, general information on the existence of personal data processing relating to people in a situation of unpaid must be given to the the moment of conclusion of the contract or data collection or before carrying out the processing, in accordance with Article 13 (3) of the GDPR. The person concerned must be clearly informed of the possibility of being registered there if he does not fulfill his payment obligations;

- secondly, in the event of an outstanding payment, the person concerned must be informed of the means at his disposal to regularize his payment, of the possibility he has of presenting his observations and, if necessary, of requesting a re-examination of his situation;
- thirdly, if the person has not regularized the payment, he must be informed of his registration in the file listing the persons in default of payment, thereby excluding them from the benefit of a service. Data subjects must also be informed of how to exercise their rights.9. Rights of personsThe persons concerned have the following rights, which they exercise under the conditions provided for by the GDPR:- right of access, rectification and erasure of data concerning them;
- right to limit processing: when the person contests the accuracy of the data concerning him, he can ask the organization to temporarily freeze the processing of this data, while it carries out the necessary checks;
- right to portability: the organization must allow any person to receive, in a structured and commonly used format, all the data processed by automated means. The data subject may request that his data be transmitted directly by the initial body to another body. Only the data provided by the person, such as the data relating to the regularization of the unpaid, on the basis of his consent or a contract, are concerned. It is therefore recommended to specify to the data subjects the processing concerned by the right to portability. In accordance with article 21 of the GDPR, if the legal basis of the processing is the legitimate interest, the persons concerned have a right of opposition. , unless the organization demonstrates that there are legitimate and compelling grounds for the processing which prevail over the interests and rights and freedoms of the data subject, or for the establishment, exercise or defense of legal claims .

In accordance with Article 22 of the GDPR, and when the processing is based on the performance of a contract to which the person is a party, the person concerned may be the subject of a decision based exclusively on automated processing producing legal effects concerning him, such as the refusal of any subsequent transaction in the event of non-regularized unpaid debt, subject to guaranteeing him the right to obtain human intervention to analyze his situation, to express his point of view and to contest decision.

To facilitate the exercise of rights, the CNIL recommends that the organization make available to the persons concerned, at a minimum, a dedicated email address and/or the contact details of the data protection officer (DPD/DPO) of the organization.10. SecurityThe organization must take all necessary precautions with regard to the risks presented by its processing to preserve the security of personal data, and in particular at the time of their collection, during their transmission and their storage, to prevent them from being distorted, damaged or that unauthorized third parties have access to it.

In particular, in the specific context of this standard, the organization is invited to adopt the following measures, to justify their equivalence or the fact of not needing or not being able to use them:

Categories

Measures

Educate users

Inform and educate people accessing the data.

Draft an IT charter and give it binding force.

Authenticate users

Define an identifier (login) specific to each user.

Adopt a user password policy in accordance with the recommendations of the CNIL.

Force user to change password after reset.

Do not store passwords in plain text.

Limit the number of attempts to access an account.

Manage authorizations

Define authorization profiles.

Delete obsolete access permissions.

Carry out an annual review of authorizations.

Trace access and manage incidents

Provide a logging system.

Inform users of the implementation of the logging system.

Protect logging equipment and logged information.

Provide procedures for personal data breach notifications.

Securing workstations

Provide an automatic session locking procedure.

Use regularly updated anti-virus software.

Install a software firewall.

Obtain the user's agreement before any intervention on his workstation.

Securing Mobile Computing

Provide encryption means for mobile equipment.

Make regular data backups or synchronizations.

Require a secret to unlock smartphones.

Protect the internal computer network

Limit network flows to what is strictly necessary.

Securing the remote access of nomadic computing devices by VPN.

Implement WPA2 or WPA2-PSK protocols for Wi-Fi networks.

Securing servers

Limit access to administration tools and interfaces to authorized persons only.

Install critical updates without delay.

Ensure data availability.

Securing websites

Use the TLS protocol and verify its implementation.

Check that no password or username is embedded in the URLs.

Check that user input matches what is expected.

Collect consent for cookies and other tracers not necessary for the service.

Back up and plan for business continuity

Perform regular backups.

Store backup media in a secure location away from the main site.

Provide security means for the transport of backups.

Plan for and regularly test business continuity.

Archive securely

Implement specific access procedures for archived data.

Securely destroy obsolete archives.

Supervise the maintenance and destruction of data

Record maintenance interventions in a logbook.

Supervise by a person in charge of the organization the interventions by third parties.

Erase data from any hardware before disposal.

Manage subcontracting

Include specific clauses in subcontractor contracts.

Provide the conditions for restoring and destroying data.

Ensure the effectiveness of the guarantees provided (security audits, visits, etc.).

Secure exchanges with other organizations

Encrypt data before sending it.

Make sure this is the correct recipient.

Transmit the secret through a separate send and through a different channel.

Protect the premises

Restrict access to premises with locked doors.

Install intruder alarms and check them periodically.

Supervise IT developments

Offer privacy-friendly default settings to end users.

Avoid free comment areas or strictly frame them.

Test on fictitious or anonymized data.

Use cryptographic functions

Use recognized algorithms, software and libraries.

Store secrets and cryptographic keys securely. An organization that is not required by its own analysis to carry out a data protection impact analysis must nevertheless ensure that the processing complies with the appropriate level of security required by Article 32 of the GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks posed by the processing, the likelihood and severity of which vary for the rights and freedoms of natural persons.

To do this, the organization may usefully refer to the Personal Data Security Guide.11. Data protection impact analysisUnder Article 35 of the GDPR, the data controller may have to carry out a data protection impact analysis (DPIA) when the processing it implements implemented is likely to pose a high risk to the rights and freedoms of data subjects.

First of all, it will be necessary to refer to the lists published by the CNIL relating to the processing likely or not to be systematically the subject of a DPIA: the list of processing for which a DPIA is not required; then, the list of processing for which a DPIA is required: With regard to the latter, there is in particular the following type of processing operations:

Types of operations

treatment

Examples

Processing involving the profiling of persons which may result in their exclusion from the benefit of a contract or in the suspension or even termination thereof

processing to combat fraud in means of payment. For this purpose, the criteria established by the European Data Protection Board (EDPB) in the DPIA Guidelines should be consulted. These provide that the completion of a DPIA is mandatory when at least two of the nine criteria below are met: - assessment or rating of a person;

- automated decision-making;
- systematic monitoring;
- processing of sensitive or highly personal data;
- large-scale processing;
- crossing or combination of data sets;
- data concerning vulnerable persons;
- innovative use or application of new technological or organizational solutions;
- processing that prevents people from exercising a right or benefiting from a service or a contract.

In order to carry out a DPIA, the data controller may use:

- the principles contained in this reference system;

- the methodological tools offered by the CNIL on its website.

In the event that the organization has appointed a data protection officer (DPD/DPO), the latter must be consulted. As a reminder, in accordance with article 36 of the GDPR, the data controller must consult the CNIL before any implementation of its treatment if the impact assessment indicates that it fails to identify sufficient measures to reduce the risks to an acceptable level.

M. L. Denis