Deliberation 2021-057 of May 6, 2021Commission Nationale de l'Informatique et des LibertésLegal status: In force Date of publication on Légifrance: Friday May 28, 2021NOR: CNIL2115699XDeliberation no. of personal data implemented in the context of rental managementThe National Commission for Computing and Liberties,

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, and repealing Directive 95/46/EC (General Data Protection Regulation), 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-I.2°, b;

After having heard the report of Mr. Philippe GOSSELIN, Commissioner, and the observations of Mr. Benjamin TOUZANNE, Government Commissioner, Adopts a reference system relating to the processing of personal data implemented in the context of rental management and attached to this deliberation.The PresidentMarie-Laure DENISREFERENCES

RELATING TO THE PROCESSING OF PERSONAL DATA IMPLEMENTED IN THE FRAMEWORK OF RENTAL MANAGEMENT

Adopted on May 6, 2021[You can consult the full text with its images from the authenticated electronic Official Journal extract.]1. Who is this reference intended for?1/ This reference is intended for natural or legal persons who, on a professional basis, rent premises for residential use or for mixed professional and residential use, and which constitute the principal residence of the lessee within the meaning of law n° 89-462 of July 6, 1989 tending to improve rental relations and amending law n° 86-1290 of December 23, 1986.2/ It is intended in particular for organizations renting for their account of residential premises as well as to real estate professionals as representatives of the lessor or when they engage in, or lend their assistance to, transactions relating to the property of others. 3/ It is also intended for online platforms offering rental management services. organizations, are required to implement automated processing in whole or in part as well as non-automated processing of personal data (paper files) as data controller, which subjects them to compliance with the rules relating to the data protection.5/ Organizations implementing processing in the context of rental management must ensure that they comply with: the provisions of the General Data Protection Regulations (GDPR) as well as those of the law of January 6, 1978 amended (Data Protection Act, or LIL); to all other rules that may apply, in particular the housing construction code as well as law n ° 89-462 of July 6, 19 89 tending to improve rental relationships and amending law no. 86-1290 of December 23,

1986, which aims to regulate rental relationships.6/ Although this reference system is only intended for persons renting one or more properties professionally, individuals, who are subject to the regulations relating to the protection of personal data, can read them or refer to the compliance assistance tools specifically intended for them.7/ Due to their particularities, this standard is not intended to apply to the processing implemented by public or private law bodies in the context of the management of real estate assets of a social nature as well as to the processing implemented in within the framework of seasonal rentals.2. Scope of the reference system7/ This reference system aims to provide people implementing processing relating to rental management with a tool to help them comply with the regulations relating to the protection of personal data.8/ This referential has no binding value. In principle, it makes it possible to ensure the compliance of the data processing implemented by the organizations with the principles relating to data protection, in a context of changing practices in the digital age.9/ Similarly, it can be clarified that the organizations can deviate from a reference system with regard to the particular conditions relating to their situation and that they can then be asked to justify the existence of such a need and the measures implemented in order to guarantee the compliance of the processing with the regulations on the protection of personal data.10/ While any organization must comply with the principles relating to data protection, the measures must be adapted to the particularities of the processing. For example, the processing carried out by organizations leasing a property under direct management may be less likely to create a risk for the rights and freedoms of the persons concerned. Measures less strict than those presented in this reference document may therefore sometimes be sufficient.11/ The reference document is not intended to interpret the rules of law 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 that may apply elsewhere.12/ This reference system also provides assistance in carrying out an impact analysis relating to data protection (AIPD), in the event that it is necessary.13/ To carry out a AIPD and comply, the data controller may finally refer to the methodological tools offered by the CNIL on its website. The organizations will thus be able to define the measures to ensure the proportionality and necessity of their processing (points 3 to 7), to guarantee the rights of individuals (points 8 and 9) and to control their risks (point 10). The organization may also rely on the CNIL guidelines on DPIA. If the organization has appointed one, the data protection officer (DPD/DPO) must be consulted.3. Terminological clarifications14/ Different types of management having an influence on the quality of data controller must be distinguished: so-called delegated or total management: a natural or legal person mandates a professional to fully manage the rental of their property. In this situation, the professional agent determines the purposes and means of the processing implemented in the

context of the rental of the property and is considered to be responsible for this processing. direct management: a natural or legal person directly rents premises from a dwelling without intermediary. It is then considered to be responsible for the processing implemented in this context. So-called semi-delegated management: a natural or legal person entrusts part of the administration of their property to a professional and retains control of the other tasks. In the event of semi-delegated management, the following is considered to be responsible for processing:

the real estate professional for all the processing implemented within the framework of the missions that the owner has delegated to him; the natural or legal person, for the processing implemented within the framework of the tasks that he wished to keep .15/ Various actors are also likely to take part in the processing referred to in this standard: the lessor: a natural or legal person who rents out a property; the candidate for rental: a person sending the supporting documents relating to his solvency after inspection of the property; the agent: a natural or legal person mandated to rent a property on behalf of the lessor; the subcontractor: a natural or legal person who processes personal data on behalf of and under the instruction and authority of another person, responsible for processing (for example, in the event of outsourcing of the financial aspect of rental management: call for rents, receipt or in the event of outsourcing the drafting of the lease, etc.).4. Objective(s) pursued by the processing (purposes)16/ The processing implemented must meet a specific objective and be justified with regard to the missions and activities of the organisation.17/ Processing relating to the management allow in particular: to offer properties for rent (in particular for the analysis of the criteria of the properties sought by potential tenants and the sending of similar rental offers); to manage the pre-contractualization and the conclusion of the contract of lease (organization of visits to the accommodation; assessment of the solvency of candidates for rental, etc.); to manage the life of the contract (in particular the follow-up of the payment of rents, charges and security deposits or even the management of the occupation housing); to terminate the lease contract (in particular the end of solidarity in the event of violence against a spouse or a child who usually resides with him and in the event of a reduction in notice). 18/ The information collected for one of these purposes s cannot be reused to pursue another objective that would be incompatible with the initial purpose. Any new use of data must in fact comply with the principles of protection of personal data, in particular the principle of the purpose of processing.5. Legal basis(s) of the processing 19/Each purpose of the processing must be based on one of the legal bases set by the regulations (article 6 of the GDPR) (for an explanation of the rule, consult the data sheet on the website of the CNIL entitled Lawfulness of processing: the essentials of the legal bases provided for by the GDPR).20/ It is up to the data controller to determine these

legal bases before any processing operation, after having carried out a reflection, that he may document, with regard to its specific situation and the context. Having an impact on the exercise of certain rights, these legal bases are part of the information that must be brought to the attention of the persons concerned.21/ In order to help organizations in this analysis, this reference document proposes in the table below , as an indication, a choice of legal basis for each purpose. Processing activities

Purposes Possible legal bases (subject to different choices justified by a specific context) Proposal of properties for rent Analysis of the criteria of the properties sought by potential tenants for the sending of rental proposals Pre-contractual measures Sending of rental proposals similar to the property for which the data subject has shown an interest Legitimate interest (provided that the data subject can object at any time) Management of the pre-contractualization and the conclusion of the lease contract Organization of the visits Pre-contractual measures Assessment of solvency Measures Conclusion of the lease and its annexes Pre-contractual measures Management of the progress of the contract Monitoring of the payment of rents, charges and security deposits Execution of the contract Management of the occupation of the accommodation Execution of the contract Verification of the subscription of the insurance Execution of the contract Management Exécu unpaid rent insurance end of contract Aggregation of data for the transmission of statistics to local rent observatories Legal obligation Management of the end of the contract Termination of the lease Execution of the contract Management of the end of solidarity Execution of the contract6. Personal data concerned 6.1 Principles of relevance and minimization of data22/ Under the principle of minimization of data, the data controller must ensure that only the data necessary for the pursuit of the purposes of the processing are actually collected and processed. The following data are in principle considered relevant, for the purposes mentioned above: 6.1.1 When looking for accommodation 23/ When looking for accommodation, people may be required to provide various data to organizations, and more particularly to real estate professionals. The data processed in this context relate to: their identification (surname, first name); their contact details (according to the preference of the persons concerned: e-mail address and/or telephone number); their search criteria (location, rent, surface , etc.).24/ At this stage, again with a view to minimizing data, it does not seem relevant to collect data relating to the personal situation of the persons concerned (professional or financial situation of the person concerned, for example). 6.1.2 At the stage of assessing the solvency of candidates for rental 25/ In terms of assessing the solvency of candidates for rental, the data that can be collected are specified in Decree No. 2015-1437 of 5 November 2015 setting the list of supporting documents that may be requested from

the rental candidate and his deposit. These are the data of the candidates for rental and their possible guarantors, relating to: their identification; their postal address; their professional situation and their resources. 26/ In application of this decree and in accordance with the principle of relevance, no additional information such as bank documents (copy of bank or postal account statement, proof of financial situation), a social security card, an extract from the criminal record , a medical file, a document attesting to the payment or non-payment of alimony, a marriage contract or even a certificate of cohabitation is in principle not considered to be relevant.27/ Additional documents may however be requested, in particular when the rental is part of a system aimed at reserving accommodation for low-income households (for example: the tax or non-taxation notice drawn up for the penultimate year preceding that of the signing of the rental within the framework of the Pinel device) provided that the data allow the lessor to ensure that the tenant fulfills the conditions of the device and that these conditions are specified in a legislative or regulatory text of a level at least equal to a decree (for example, for the Pinel and Duflot devices, article 199 novovicies of the general tax code provides that the annual ceilings of the tenant's resources set by decree must be assessed on the date of conclusion of the lease). return of superfluous documents to the candidate, in order to comply with the regulations.29/ The table reproduced below lists the supporting documents which may be considered relevant. valid identity, including the photograph and signature of the holder One of the following documents: National identity card French or foreign identity;French or foreign passport;French or foreign driving licence;Document justifying the right of residence of the foreign rental candidate.Proof of addressFor the candidate (one of the following documents):Three last rent receipts or, failing that, certificate from the previous lessor, or his representative, indicating that the tenant is up to date with his rents and charges; Certificate of election of domicile establishing the link with an organization approved under Article L. 264 -2 of the code of social action and families; Certificate on the host's honor indicating that the candidate for rental resides at his home; Last property tax notice or, failing that, title deed of the residence principal.For the guarantor (one of the following documents): Last rent receipt; Water, gas or electricity bill less than three months old; Housing insurance certificate less than three months old; Last notice property tax or, failing that, title deed of the main residence. A certificate of professional activities Work or internship contract or, failing that, certificate from the employer specifying the job and the proposed remuneration, the date of entry envisaged in office and, where applicable, the duration of the trial period; Extract K or K bis from the trade and companies register of less than three months for a commercial company; Original D1 extract from the register of trades of less than three months for a craftsman; Copy of the INSEE identification certificate, including identification numbers, for a

self-employed worker; Copy of the professional card for a liberal profession; Any recent document attesting to the activity for others professionals; Student card or school certificate for the current year. A certificate of resources Last or penultimate notice of taxation or non-taxation; Three last payslips; Juice proof of payment of internship allowances; Two last balance sheets or, failing that, certificate of resources for the current financial year issued by an accountant for self-employed professions; Proof of payment of allowances, pensions, pensions, social and family benefits and allowances received during the last three months or proof of eligibility, established by the paying body; Simulation certificate drawn up by the paying body or simulation drawn up by the tenant relating to housing aid; Grant award notice for scholarship students; Title deed of real estate or last notice of property tax; Proof of land income, life annuities or income from securities and movable capital. chosen tenant, additional data is in principle considered relevant: his bank details; his email address subject to having obtained his consent; his beneficiary number at the Family Allowance Fund (CAF) or the Mutualité sociale agricole (MSA) in the event of receipt of the housing allowance by third-party payment; the insurance certificate; identity of the husband, wife or person in a civil partnership with the tenant in title in the event of a request for co-ownership, in accordance with article 1751 of the civil code. 6.1.4 At the request for an end of solidarity 31 / When the tenant's spouse, his partner bound by a civil pact of solidarity or his notorious cohabitant leaves the accommodation because of violence exerted within the couple or on a child who usually resides with him, the victim of the violence can request the end of solidarity, in accordance with article 8-2 of the law n° 89-462 of July 6, 1989. The following data are therefore considered relevant: the copy of the protection order issued by the judge for family affairs which he benefits and previously notified to the another member of the couple; a copy of a decision of criminal conviction for acts of violence committed against him or on a child who usually resides with him and rendered for less than six months. 6.1.5 Upon termination and expiry of the lease32/ When the tenant terminates the contract, the organization processes the information relating to the notice and the inventory of fixtures when leaving the accommodation. 33/ If the tenant wishes to benefit from a reduced period of notice, the organization may consult, in accordance with article 15 of law n° 89-462 of July 6, 1989 tending to improve rental relations, data justifying: a possible professional change; the allocation of accommodation defined in Article L. 831-1 of the Construction and Housing Code; the state of health requiring a change of residence; receipt of the active solidarity income or the disabled adult allowance. For accommodation located in a tight zone, no additional data can be processed as part of the reduction in notice. 6.2 The processing of sensitive data and data relating to convictions criminal offenses and offences34/ Two categories of data call for heightened vigilance because of their particularly sensitive nature.

Benefiting from special protection, they can only be collected and processed under conditions strictly defined by the texts. These are: sensitive data, i.e. data revealing a person's ethnic or alleged racial origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation. These data cannot be collected, except for exceptions provided for by the texts; data relating to offences, criminal convictions and related security measures which can only be processed in certain cases, in compliance with the legal provisions relating to offense data. 35/ As part of the processing relating to the reduction of notice, data relating to health (medical certificates) may be processed. Despite a general principle of prohibition, the processing of this data can be considered as compliant in accordance with: Article 9-2-a) of the GDPR when the tenant requests a reduction in notice for the collection of the allowance for disabled adults (AAH) in accordance with Article 15 of Law No. 89-462 of July 6, 1989; Article 9-2-g) of the GDPR when the tenant's state of health requires a change of residence, the processing being necessary for reasons of important public interest on the basis of national law (i.e. Article 15 of Law No. 89-462 of July 6, 1989 to improve rental relationships and amending Law No. 86-1290 of December 23, 1986). 36/ Similarly, the data processed within the framework of the end of solidarity due to violence may also include data relating to offences, convictions and security measures concerning natural persons (copy of the protection order issued by the judge to family affairs or a copy of a criminal conviction for acts of violence handed down less than six months ago). Such data can only be collected and processed in cases strictly provided for by the texts, and in particular when a law expressly authorizes it. In the context of a request for the end of solidarity due to violence exerted within the couple or on a child, the processing of data relating to convictions is effectively authorized by the provisions of article 8-2 of law no. 89-462 of July 6, 1989 aimed at improving rental relationships and amending law no. 86-1290 of December 23, 1986.7. Recipients and access to information37/ Personal data must only be made accessible to persons authorized to know it with regard to their duties.38/ Access authorizations must be documented by the organizations, and access to the various processing operations must be subject to traceability measures. See point 9 relating to safety. 39/ The data controller who wishes to use a subcontractor must ensure that he only uses organizations that offer sufficient guarantees. A contract defining the characteristics of the processing as well as the different obligations of the parties in terms of data protection must be established between them (article 28 of the GDPR). A subcontractor's guide, published by the CNIL, specifies these obligations and the clauses to be included in the contracts.7.1. Persons accessing data on behalf of the data controller40/ Only persons authorized by virtue of their missions or functions may access the personal

data processed, and this within the strict limits of their respective powers and the performance of these missions and functions. 41/ For example, if the persons in charge of rental management within the organization may be authorized to access the data, this is not the case for the persons in charge of commercial prospecting. 7.2. Recipients of data42/ The GDPR defines recipients as any organization that receives the communication of data. 43/ As part of this processing, real estate professionals, when they engage in or assist in transactions involving the property of others, may be required to communicate certain data to the owners. 44/ Indeed, in accordance with the code of ethics of real estate professionals and the provisions of Law No. 70-9 of January 2, 1970 and Decree No. 72-678 of July 20, 1972, the data controller, when he engages in or lends his assistance to transactions involving the property of others, regularly reports to the owner of the accommodation on the performance of his duties. 45/ Within the framework of a delegated or total management, the communication to the owner of the only information necessary for the verification of the good management of the property (effective payment of the rents, maintenance of the accommodation, etc.) is in principle considered as compliant. 46/ If the mandate provides for semi-delegated management, the communication is in principle considered to be compliant: of the information necessary to carry out the missions incumbent on the owner, in accordance with the distribution of roles provided for in the management mandate; of the only information allowing the professional to report on the proper execution of his missions to the owner. 47/ For example, if the semi-delegated management mandate provides that the choice of tenant is up to the real estate professional, the owner should not in principle obtain the communication of all the files of the candidates for rental. If he wishes, he can however obtain the communication of the files of the candidates who have been pre-selected by his representative in order to make the final choice. 48/ Data may also be transmitted: to insurers for the guarantee of unpaid rents; to the tax authorities, in particular to document compliance with tenant resource ceilings in the context of intermediate rental investments; to the new manager if the owner decides to change it; to the TRACFIN unit, in accordance with the provisions of Article L. 561-2 of the Monetary and Financial Code (real estate professionals are subject to the system for combating money laundering and the financing of terrorism); to representatives of tenant associations if a legal provision so provides or if the persons concerned have consented to such transmission. Other persons or organizations may be likely to receive communication of the data, provided that this communication complies with the principle of specific, explicit and legitimate purpose and that the person concerned is able to oppose it (trustee, company having to carry out work, etc.).7.3. Transfers of data outside the EU49/ To ensure the continuity of the protection of personal data, their transfer outside the

European Union is subject to specific rules. Thus, in accordance with the provisions of Articles 44 and following of the GDPR, any transmission of data outside the EU must: be based on an adequacy decision; or be governed by internal corporate rules (BCR), standard data protection clauses, a code of conduct or a certification mechanism approved by the CNIL; or be governed by ad hoc contractual clauses previously authorized by the CNIL; or comply with one of the derogations provided for in Article 49 of the GDPR. To find out more, consult the section Transferring data outside the EU on the website of the CNIL.8. Storage periods50/ A precise storage period for the data must be set according to each purpose: this data cannot be kept for an indefinite period.51/ The data storage period or, when it is variable, the criteria used to determine this duration, are part of the information that must be communicated to the data subjects.52/ Under these conditions, it is the responsibility of the controller to determine this duration or these criteria prior to carrying out the processing.8.1 Storage periods53/ With regard to the purposes justifying the implementation of processing relating to rental management, and unless otherwise provided by law or regulation, the following examples of retention periods may be retained by the organizations concerned: for data collected prior to an application for the rental processed for prospecting purposes (identification data, contact details, search criteria), and A storage period of three (3) years from the last contact of the persons concerned with the organization is considered adequate; for data collected at the stage of assessing the solvency of applicants for rental, the storage period three (3) months on an active basis is in principle adequate; for data relating to the successful rental candidate: the contractual duration and until the closure of the tenant's accounts in the active database is in principle adequate is in principle adequate, then in intermediate archiving for a period that cannot in principle exceed: three (3) years in the event of direct management (limitation period in leases); five (5) years in the event of delegated or semi-delegated management (limitation period in civil matters). for the tenant's data collected from the conclusion of the lease until its termination: the contractual duration until the closing of the tenant's accounts is in principle an adequate retention period on an active basis. At the end of this period, the data can be archived, in intermediate archiving. Intermediate archiving periods considered adequate are in principle as follows: the limitation period for the lease contract, i.e. three (3) years in the context of direct or semi-delegated management (depending on the distribution tasks between the agent and the principal); the time of civil prescription, namely five (5) years under delegated or semi-delegated management (depending on the distribution of tasks between the agent and the principal). the data collected within the framework of the termination of the contract justifying the end of solidarity or the reduction of the notice cannot in principle be the subject of conservation by the owner, except to justify a particular need. On the other hand,

they can be kept until the validation by the owner of the reduction of the notice or the end of solidarity in the event of indirect management, subject to implementing strong measures to ensure their security and confidentiality. .54/ The data may be kept for longer than the durations mentioned above, in intermediate archiving, if the controller has a legal obligation (for example, to meet accounting, social or tax obligations) or s he needs to constitute proof in the event of litigation and within the limit of the applicable limitation/foreclosure period, in matters of discrimination for example. The duration of the intermediate archiving must however meet a real need, duly justified by the data controller after a prior analysis of various factors, in particular the context, the nature of the data processed and the level of risk of a possible dispute. 55/ In the event of termination of the management mandate, the real estate professional, former agent, hands over all the information relating to rental management to the new lessor or agent. He may keep a copy of any document necessary to enable him to protect himself against litigation in intermediate archiving for a period of five (5) years. It is however recommended to anonymize them when possible or to pseudonymize them in order to reduce as much as possible the directly identifying character. To find out more, consult the section Data retention periods on the CNIL website. retention of anonymized data56/ The regulations relating to the protection of personal data do not apply, in particular with regard to retention periods, to anonymized data. These are data which can no longer be linked by anyone to the identified natural person to whom they relate. In this case, the organization concerned must guarantee the anonymized nature of the data in a sustainable manner. It is reminded that in general, the simple deletion of the surnames and first names of persons only constitutes pseudonymization, ineffective in guaranteeing the data against the risk of re-identification.58/ To find out more, you can refer to the guides of the CNIL:Security: Archiving securely;Limiting the retention of data..Data used for statistical purposes are no longer qualified as personal data once they have been duly anonymized (for more information, you can refer to the EDPS guidelines on anonymisation).9. Information of persons59/ Processing of personal data must be implemented in complete transparency vis-à-vis the persons concerned.9.1 Content of the information to be provided60/ The information communicated to the persons concerned must be done under the conditions provided for in Articles 12, 13 and 14 of the GDPR. 61/ From the stage of the collection of personal data, data subjects must be informed of the existence of the processing and of its essential characteristics (including the identity of the data controller and the objective pursued) as well as of the rights which they have. 62/ The contract concluded between the agent and the principal may specify the practical procedures for informing the persons concerned, in particular if the owner wishes to delegate this mission to the agent. Examples of information notices are available on the CNIL website and can be consulted in

the GDPR section: examples of information notices .9.2 Information procedures9.2.1 Information for rental applicants and tenants63/ In order to fully comply with the principles of fairness and transparency and in accordance with Article 13 of the GDPR, individuals must be informed directly at the time the data is collected. 64/ So that the information that must be brought to the attention of candidates is easily accessible, it is recommended that a confidentiality policy containing all the information required by Article 13 of the GDPR be attached to the list of supporting documents to be submitted. provide. 65/ A link to the privacy policy may also be inserted in the rental announcement, in emails to candidates as well as on the contact form on the real estate agency's website for people interested in an announcement.9.2.2 Information to guarantors66/ In accordance with Article 14 of the GDPR, the data controller must inform by any means the persons acting as guarantors within a reasonable time, not exceeding one month, following upon receipt of the rental file. 67/ The data controller may, for example, when he is able to demonstrate it, directly inform the guarantors by post, or provide an informative document to the candidate, on the condition that the latter undertakes to communicate it. to its guarantors. 10. Rights of persons68/ The persons concerned have the following rights, which they exercise under the conditions provided for by the GDPR (to go further, see the section dedicated to the rights to respect the rights of persons on the CNIL website): right of access to their file, as well as to all data concerning them in general; right of rectification of data concerning them, if they are inaccurate; right of erasure of data concerning them subject to the conditions of exercise of this right pursuant to the provisions of Article 17 of the GDPR; right to restriction of processing. For example, when the person disputes the accuracy of their data, they can ask the organization to temporarily freeze the processing of their data, while the latter carries out the necessary checks concerning their request; right to portability in the conditions provided for in Article 20 of the GDPR; right to oppose the processing of their data, subject to the conditions for exercising this right pursuant to the provisions of Article 21 of the GDPR. Thus, the right of opposition only applies when the processing is based on the legitimate interest pursued by the data controller or a third party (for example when the data controller sends rental proposals similar to the property for which the data subject has presented an interest). However, it will not apply when the processing is based on a legal obligation or on the performance of the contract.69/ It should be noted that the choice of a legal basis for the processing conditions the existence of certain rights (https://www.cnil.fr/fr/la-liceite-du-traitement-lessentiel-sur-les-bases-legales-prevues-par-le-rgpd). Thus, the transmission of statistics to local rent observatories meets a legal obligation. The tenant cannot therefore object in principle to the processing of his personal data, in accordance with the provisions of Article 21 of the GDPR. 11. Security70/ The organization must take

all useful 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, prevent them from being are distorted, damaged or accessed by unauthorized third parties. 71/ In particular, in the specific context of this standard, the organization is invited to adopt the following measures or otherwise be able to justify the implementation of equivalent measures or their absence of necessity or possibility due to their particular situation :CategoriesMeasuresRaising user awarenessInforming and raising awareness of people handling dataDrafting an IT charter and giving it binding forceAuthenticating usersDefining a unique identifier (login) for each userAdopting a user password policy in line with CNILOrequiring the user to change their password after resetLimit the number of attempts to access an accountEnsure data confidentialitySend group emails to recipients in hidden copyDo not display identifiers and passwords in clear text on charge call emailsDestroy documents dad in a secure manner, in particular by shredding them before throwing them away or by using secure binsManaging authorizationsDefining authorization profilesDeleting obsolete access permissionsCarrying out an annual review of authorizationsTracing access and managing incidentsPlanning a logging systemInforming users of the implementation of the logging systemProtect logging equipment and logged informationProvide procedures for personal data breach notificationsSecure workstationsProvide an automatic session locking procedureUse regularly updated antivirus softwareInstall a firewall fire (firewall) softwareGet the user's agreement before any intervention on his workstationSecure mobile computingProvide means of encryption for mobile equipmentMake regular backups or synchronization of dataRequire a secret for unlocking ordiphones (smartphones)Protect the internal computer networkLimit network flows to what is strictly necessarySecure remote access for mobile computer equipment by VPNImplement the WPA2 or WPA2-PSK protocol for Wi-Fi networksSecure serversLimit access to administration tools and interfaces for authorized persons only Installing critical updates without delay Ensuring data availability Securing websites Using the TLS protocol and checking its implementation Checking that no password or identifier is transmitted in the URLs Checking that the user entries correspond to what is expected Collect user consent for the deposit of cookies that are not strictly necessary for the provision of the service Back up and plan for business continuity Perform regular backups Store backup media in a safe place Provide means of security for the transport of backupsPlan and regularly test business continuityArchive in a secure mannerImplement specific access procedures for archived dataDestroy obsolete archives in a secure mannerSupervise the maintenance and destruction of dataRecord maintenance interventions in a daybookSupervise by a manager of the organization interventions by third

partiesErase the data of any equipment before its disposalManage subcontractingProvide a specific clause in the contracts of subcontractorsPrescribe the conditions for the restitution and destruction of dataEnsure effectiveness provided guarantees (security audits, visits, etc.) Secure exchanges Encrypt data before sending Ensure that it is the right recipient Transmit the secret during a separate sending and via a different channel Provide a secure channel for the filing of rental candidate files (for example: deposit form via HTTPS on the organization's website)Protect the premisesRestrict access to the premises by means of locked doorsInstall anti-intrusion alarms and check them periodicallySupervise IT developmentsPropose settings that respect the privacy of users purposesTest on fictitious or anonymized dataUse cryptographic functionsUse recognized algorithms, software and librariesKeep secrets and cryptographic keys securelyTo do this, the data controller may usefully refer to the Personal Data Security Guide.12. Data protection impact analysis (DPIA)72/ Pursuant to the provisions of Article 35 of the GDPR, the data controller may have to carry out an impact analysis when the processing it implements work is likely to pose a high risk to the rights and freedoms of data subjects. First of all, you should refer to: the list of processing operations for which an impact analysis is not required; then to the list of types of processing operations for which a data protection impact assessment is required.73/ Insofar as the processing implemented is not present on one of these lists, it is necessary to question the need to carry out a DPIA.74/ To do this, it is necessary to rely on the criteria established by the European Data Data Protection Impact Assessment (DPIA). In accordance with this text, carrying out a DPIA is mandatory when at least two of the nine criteria are met: evaluation or rating of a person; automated decision-making; systematic monitoring; processing of sensitive or highly personal data; processing on a large scale; matching or combining data sets; data concerning vulnerable persons; innovative use or application of new technological or organizational solutions; processing operations which prevent persons from exercise a right or to benefit from a service or a contract.75/ In the context of rental management, the data controller seems in principle to have to carry out an impact analysis insofar as he meets the criteria relating to :to sensitive or highly personal data (particularly financial data);on a large scale due to a large volume of data and the potentially large number of data subjects;to the assessment of rental candidates;to any data relating to offences, convictions and security measures. To carry out an impact study, the person in charge of tr It may: refer to the principles contained in this reference system; refer to the methodological tools offered by the CNIL on its website. If the organization has appointed one, the DPD/DPO must be consulted.76/ In accordance with Article 36 of the GDPR, the data controller must consult the CNIL prior to the implementation of the processing if the impact analysis indicates that it is unable to identify sufficient measures to reduce the risks to an

acceptable level.