Deliberation 2021-028 of March 11, 2021Commission Nationale de l'Informatique et des LibertésLegal status: In force Date of publication on Légifrance: Wednesday March 31, 2021NOR: CNIL2108910XDeliberation no. of personal data implemented in the context of reception, accommodation and social and medico-social support for the elderly, people with disabilities and those in difficultyThe National Commission for Informatics and of freedoms, 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. I.2°.b); Considering the decree n° 2005-1309 of October 20, 2005 modified taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; After having heard Mr. Philippe GOSSELIN, Commissioner, in his report and Mr. Benjamin TOUZANNE, Government Commissioner, in his observations; Adopts a reference system relating to the processing of personal data implemented in the context of the reception, accommodation and social and medico-social support of the elderly, people with disabilities and those in difficulty and appended.ANNEX REFERENCE GUIDELINES RELATING TO THE PROCESSING OF PERSONAL DATA IMPLEMENTED IN THE FRAMEWORK OF RECEPTION, ACCOMMODATION AND SOCIAL AND MEDICO-SOCIAL SUPPORT FOR THE ELDERLY, PERSONS WITH DISABILITIES AND THOSE IN DIFFICULTY ADOPTED ON MARCH 11, 2021 You can consult the full text with its images from the authenticated electronic Official Journal extract.1. Who is this reference for? This reference system is intended for private or public organisations, whatever their legal form, hereinafter the organisations, which welcome, house or support socially and/or medico-socially the elderly, people with disabilities and those in difficulty. This reference system is likely to be of interest to the following organizations (non-exhaustive list): departmental councils; municipal social action centers (CCAS); accommodation establishments for dependent elderly people (EHPAD); departmental homes for the disabled (MDPH); home support services (SAAD); home nursing services (SSIAD); medico-social support services for disabled adults (SAMSAH); special education and home care services (SESSAD); medico-psycho-educational centers (CMPP); early medico-social action centers (CAMSP); aid establishments and services e through work (ESAT); specialized reception centers (MAS); medico-educational institutes (IME); therapeutic, educational and pedagogical institutes (ITEP); social life support services (SAVS) ;integration through economic activity services (SIAE);outsourced services and skills centers (PCPE);coordination and guidance platforms (PCO);family

carers welcoming elderly or in a situation of disability; organizations responsible for managing a legally compulsory basic social security scheme or the service of allowances, benefits and aid mentioned in the social security code or the code of social action and families; private law associations created under the law of 1901 whose mission is to welcome, accommodate, support and social and medico-social monitoring of the elderly, people with disabilities and those in difficulty é; the social and medico-social establishments listed by the provisions of article L. 312-1 of the social action and family code (CASF). In this context, these organizations are required to implement automated processing in whole or in part, as well as non-automated processing of personal data, as data controller, which subjects them to compliance with the rules relating to data protection. Organizations implementing processing in this context must ensure that they comply with: the provisions of the general data protection regulations (GDPR) as well as those of the amended law of 6 January 1978 (Data Protection Act or LIL); other rules that may apply, in accordance with the regulations in force, in particular the CASF and the Public Health Code (CSP). Are excluded from the scope of application of the standard because of their specificities, the processing implemented by: private and/or public law bodies in the context of the prevention and protection of children; legal representatives for the protection of adults.2. Scope of the reference This reference relates to the processing of personal data routinely implemented by organizations in the context of the social and/or medico-social support they provide to the elderly, disabled or in difficulty (the people who are threatened with exclusion for various reasons and who face problems that are themselves diverse, such as asylum seekers, people in very precarious housing situations, job seekers, people in difficulty financial, etc). Its purpose is to provide organizations implementing such processing with a tool to help them comply with regulations relating to the protection of personal data. Social and/or medico-social support must be entered in the register provided for in Article 30 of the GDPR (see model register). This reference 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.Organizations that deviate from the framework with regard to the particular conditions relating to their situation may do so. They may nevertheless 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 in terms of protection of personal data. The purpose of the guidelines is not 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 also apply (e.g.: CASF, CSP, etc.). This reference system also helps to carry out an impact analysis relating to data protection (AIPD), in the event that

this is necessary. Organizations can also refer to the methodological tools offered by the CNIL on its website in order to facilitate the compliance of the processing carried out. They will thus be able to define the measures to ensure the necessity and proportionality 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. Objective(s) pursued by the processing(s) (Purposes) The processing operations implemented must meet a specific objective and be justified with regard to the missions and activities of the organisations. The processing operations relating to the reception, accommodation and social and medico-social support for people can be implemented in particular in order to: a. to provide the services defined within the framework of a contract concluded between the organization and the person concerned or his legal representative and, if necessary, to ensure the management of the administrative file of the person concerned (management of medical appointments and/or social services, management of family visits, if applicable, etc.); Examples for people with disabilities or the elderly (non-exhaustive list): the residence contract or the individual care document (DIPEC) provided for by article L. 311-4 of the CASF between the organization (EHPAD, accommodation homes for disabled adults, etc.) and the person concerned or his legal representative; the home care contract between the family carer and the person being cared for or their legal representative; the contract for support and assistance through work between the establishment or the assistance through work service and each worker with a disability. Examples for people with difficulty (non-e list xhaustive): the reciprocal commitment contract (CER) or the personalized plan for access to employment (PPAE) concluded between the beneficiary of the active solidarity income (RSA) and the president of the departmental council to improve professional integration ;the accommodation contract concluded between the beneficiary and the organization providing accommodation for people in an emergency situation.b. to instruct, manage and, where applicable, grant rights and/or pay legal and optional social benefits; Examples of legal aid for people with disabilities or the elderly (non-exhaustive list) social assistance for accommodation (ASH); personalized autonomy allowance (APA); allowance for disabled adults (AAH); education allowance for disabled children (AEEH); disability compensation benefit (PCH); the mobility inclusion card (CMI). Examples of legal aid for people in difficulty (non-exhaustive list): active solidarity income (RSA); social housing allowance (ALS). Examples of optional assistance (non-exhaustive list): household help; transport assistance; payment of funeral expenses; payment of gas and/or electricity bills; assistance fund for youth.c. to offer social and medico-social support adapted to the difficulties encountered, with the particular aim of developing a personalized

support plan with regard to the lifestyle, special requests, special needs, physical and psychological autonomy of the the person and to ensure the follow-up in accordance with the provisions of articles L. 311-3 of the CASF, to ensure the follow-up of the people in the access to the rights in particular the assistance in the relations and the steps to be carried out and, the if necessary, to direct people to the competent structures likely to take care of them; Examples for people with disabilities or the elderly (non-exhaustive list): ensuring medical follow-up adapted to the condition of the person ;support people in the essential acts of their daily life (e.g. help with preparing meals, help with cleaning and home maintenance, help with travel, help with the toilet, etc.) tc.); manage individual care files within the framework of the medical follow-up of people, including the management of reimbursements of medical expenses; manage requests for places in establishments or services, medicalized or not; ensure the organization and monitoring of paths to integration and/or educational, social and professional integration; drawing up a municipal register for alerting and informing populations; ensuring access to rights relating to the end of life (information on the possibility of living one's last days accompanied and peaceful, accompaniment in the drafting of advance directives, etc.); providing assistance in the context of the digital administrative procedures to be carried out with the most fragile and in particular people who are not able to move around (a good practice guide for professionals is available on the CNIL website). Examples for people in difficulty (non-exhaustive list): ensuring the organization and monitoring of integration/reintegration and/or educational, social and professional integration paths; ensuring educational and budgetary support and monitoring people and prevent over-indebtedness; manage requests for accommodation and access to housing; manage unpaid bills and prevent rental evictions; monitor people and families received as part of family mediation, social or criminal justice, excluding measures relating to social assistance for children; monitoring the execution of criminal court decisions restricting or depriving freedoms by the authorized bodies; assisting people in the context of formalities to obtain domiciliation for people without a stable home; to assist people with the administrative procedures necessary for asylum application procedures (p. ex. translation, information and support with regard to recourse in the event of refusal of the request, etc.); assisting people in the context of procedures with private and/or public creditors (e.g.: assistance in the context of over-indebtedness procedures with the Banque de France, etc.).d. to exchange and share strictly necessary information, in compliance with the provisions of article L. 1110-4 of the CSP and the provisions of the CASF, making it possible to guarantee the coordination and continuity of the support and monitoring of people between social, medical and paramedical workers; e. to ensure the administrative management (number of places available, reception capacity of the establishment, etc.), financial and accounting of the

establishment, department or organization; Note: With regard to administrative management of personnel, the organizations can usefully refer to the reference system relating to the processing of personal data implemented for the purposes of personnel management available on the Commission's website.f. to ensure the feedback of previously anonymized information to the competent authorities concerning serious malfunctions or events having the effect of threatening or compromising the health, safety or well-being of the persons taken care of in accordance with the provisions of Articles R. 331- 8 and following of the CASF, establish statistics, internal studies and satisfaction surveys for the purposes of evaluating the quality of the activities and services and the needs to be covered. Please note: As soon as these statistics, studies and evaluations enter into the field of research, studies and evaluations in the field of health, the processing operations must comply with the provisions of articles 72 and following of the Data Protection Act. The information collected for one of these purposes cannot in principle be reused to pursue an objective that would be incompatible with the initial purpose. Any new use of data must in fact respect the principles of protection of personal data, in particular the principle of the purpose of the processing (for example, the processing implemented for the purposes set out above must not give rise to interconnections or exchanges other than those necessary for the accomplishment of these).4. Legal basis(s) of the processingEach purpose of the processing must be based on one of the legal bases set by the regulations (article 6 of the GDPR). (see for an explanation of this rule: the legality of the processing: the essentials on the legal bases provided for by the GDPR). It is up to the data controller to determine these legal bases before any processing operation, after having carried out a reflection, which he can document, with regard to his 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. be used in the most common cases. These elements must be adapted to the specific situation of each organization concerned. Thus, for example, depending on whether the organization in question is in the private or public sector, certain processing operations that nevertheless serve the same purpose (for example, those related to the administrative management of persons monitored, received or accommodated) may be based on different legal bases (eg legitimate interest in the private sector, performance of a task in the public interest in the public sector). Please note: in the context of social and/or medico-social support for the elderly, disabled or in difficulty, the commission draws the attention of organizations to the need to exercise the greatest caution in the use of consent as the legal basis for their processing of personal data. The persons concerned may in fact suffer from impaired judgment which may render the consent invalid. In addition, it is recalled that the person concerned who provides his consent may withdraw it at any

time, in principle putting an end to the possibility of processing the data concerning it for the future. In general, the data controller must ensure compliance with the conditions for obtaining consent and more particularly the free, specific, informed and unequivocal consent.Purposes

Possible legal bases

(subject to different choices justified by a specific context which it is recommended to document)

Provision of the services defined under the contract concluded between the organization and the person concerned or his legal representative and, where applicable, administrative management of the persons concerned

Public bodies or legal persons governed by private law managing a public service

Performance of the contract or mission of public interest when the processing implemented exceeds what is necessary for the contract

Private organizations

Performance of the contract or legitimate interests when the processing implemented exceeds what is necessary for the contract

Social and medico-social support adapted to the difficulties encountered, the purpose of which is in particular to develop a personalized support plan, to ensure the follow-up of people in access to rights and, if necessary, to direct people to competent structures likely to support them

Public bodies or legal persons governed by private law managing a public service

Mission of public interest

Private organizations

Legitimate interests

Special case concerning the follow-up of persons and families received within the framework of family, social or penal mediation, excluding measures relating to social assistance for children and the follow-up of the execution of decisions restrictive or deprivation of freedoms by the authorized bodies

Legal obligation, subject to compliance with the provisions of Article 46 of the Data Protection Act relating to criminal convictions, offenses and security measures

Special case concerning rights relating to the end of life

Consent

Examination, management and, where applicable, opening of rights and/or payment of requests for legal or optional social benefits

Legal aid

Mission of public interest

Optional aids

Public bodies or legal persons governed by private law managing a public service

Mission of public interest

Private organizations

Legitimate interests

Exchange and sharing of strictly necessary information to guarantee the coordination and continuity of support and follow-up of people between social, medical and paramedical workers

Public bodies or legal persons governed by private law managing a public service

Mission of public interest

Private organizations

Legitimate interests

Administrative, financial and accounting management of the establishment, service or organization

Public bodies or legal persons governed by private law managing a public service

Legal obligation (e.g.: decree no. 2012-1246 of November 7, 2012 relating to public budget and accounting management, etc.)

Private organizations

Legal obligation (e.g.: regulation n° 2018-06 of December 5, 2018 relating to the annual accounts of non-profit private law legal entities, etc.)

Feedback of previously anonymized information to the competent authorities concerning serious malfunctions, establishment of statistics, internal studies and satisfaction surveys for the purpose of evaluating activities, the quality of services and the needs to be covered

Public bodies or legal persons governed by private law managing a public service

Legal obligation (e.g.: the provisions of article L. 232-17 of the CASF provide for the transmission to the minister in charge of the elderly of statistical data relating to the development of the APA system; the provisions of the article L. 345-2-4 of the CASF regulate the production of statistical data on activity, monitoring and management of reception, accommodation and support towards integration and housing for integrated reception services and orientation, etc.) or mission of public interest

Private organizations

Legal obligation (e.g.: the reporting of previously anonymized information to the competent authorities concerning serious malfunctions or events having the effect of threatening or compromising the health, safety or well-being of the people taken care of in accordance with the provisions of the articles R. 331-8 and following of the CASF) or legitimate interests5. Personal data concerned5.1. Principles of relevance and minimization of data 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 categories of data relating to the identification of the beneficiaries of social and medico-social support and, where applicable, their legal representatives, are in principle considered relevant for the purposes mentioned above; personal life; the professional career and training in the context of assistance with the professional integration of people; material living conditions; social security coverage; bank details insofar as this information is necessary for the payment of a service; the social and medico-social assessment of the person concerned; the type of support and the actions implemented; the identification of the people contributing to the social and medico-social care and to the entourage likely to be contacted; the identification of people in the context of digital support. In general, the data controller must only collect the data for which he has really need and should only do so from the moment when this need materializes. when the benefit of the assistance or the service requested is subject to a condition of regularity of stay. As part of the support relating to the asylum application and/or the application for a residence permit, may be collected information relating to the asylum application procedure in the form of filing an asylum application yes/no and/or information relating to the procedure for applying for a residence permit in the form of filing a request for a residence permit yes/no, the nationality of the person concerned as well as the information necessary to draw up the life story.5.2. The processing of the social security number (NIR), sensitive data and data relating to criminal convictions and offencesCertain categories of data call for increased vigilance due to their particularly sensitive nature. Benefiting from specific protection, they can only be collected and processed under conditions strictly defined by the texts. This is: NIR, which is the subject of specific regulations and can only be recorded in the processing in the context of exchanges with

health professionals or social security, provident organizations and MDPH. In this respect, the decree in Council of State n ° 2019-341 of April 19, 2019 taken after opinion of the CNIL, determines the categories of data controllers and the purposes of this processing in view of which the latter can be implemented. when they relate to data including the NIR (see also All about the NIR framework decree in the field of social protection); the national health identifier or INS (articles L. 1111-8-1 and R. 1111-8-1 and following of the Public Health Code) which can only be used to list and find health data and administrative data related to a person benefiting or called to benefit from health or medical care. -social. The INS can only be used by professionals, establishments, services or organizations involved in prevention or care whose conditions of practice or activities are governed by the CSP (self-employed health professionals, health establishments, etc.) .), by professionals in the social and medico-social sector, by social or medico-social establishments or services (e.g.: retirement homes, MDPH, etc.) or by professionals forming a care team within the meaning of Article L. 1110-12 of the CSP and involved in the health or medico-social care of the user; 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 (art. 46 of the LIL); For example if: they are strictly necessary within the framework of the actions implemented in favor of persons detained or placed under m for the sake of justice, on the one hand, and in the context of the aid and support of victims of offenses or the families of detainees; they make it possible to establish the existence of a situation of past or current mistreatment in order to adapt the accompaniment of the person concerned (p. ex. : support for female victims of domestic violence by a victim support association approved by the Ministry of Justice in accordance with the provisions of Article 46 para. 1 of the Data Protection Act and Article 76 of Decree No. 2019-536 of May 29, 2019). so-called sensitive data, i.e. data revealing ethnic or allegedly racial origin, a person's 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 as provided for by the texts. By way of example, data relating to health may be collected, provided that these data are collected for the purposes of: administering care, processing , medical diagnostics, preventive medicine or health services management. The processing operations in which these data are integrated must be implemented by a member of a health profession or by another person on whom, by reason of his duties, the obligation of professional secrecy is imposed, the breach of which is repressed by article 226-13 of the penal code; or the delivery of a social benefit intended for people with a loss of autonomy or disability provided for by a legislative or regulatory text, provided that this information is strictly necessary

for the delivery of the said service. When the collection of health data is necessary for the social support provided but does not fall within one of the two situations mentioned above, this can be carried out after obtaining the consent of the data subject or their legal representative (e.g.: a home helper may receive communication of a person's state of health when this information is necessary for social support al and medico-social carried out at home). In this respect, the data controller must ensure compliance with the conditions for obtaining consent and more particularly the free, specific, informed and unambiguous nature of the consent. Data relating to religious and/or philosophical beliefs may also be collected subject to (cumulative conditions): to be collected from the person concerned or his legal representative, after obtaining express consent. In the same way, the data controller must ensure compliance with the conditions for obtaining consent and more particularly the free, specific, informed and unambiguous nature of the consent; and to be strictly necessary for social and/or medical support. social (e.g.: organization of meals, funerals, support for people who are victims or likely to be victims of extremist movements, etc.). A distinction should be made between consent as an exception provided for by the GDPR authorizing the collection of sensitive data, consent as a legal basis or legal basis which legally authorizes the implementation of the processing. Example: In the context of social and medico-social support adapted to the difficulties encountered by people, sensitive data, in particular religious beliefs, are likely to be collected by the data controller. Consequently, if the legal basis for the processing is based on the legitimate interest, the performance of the contract or the mission of public interest, specific consent must be obtained in order to be able to process information relating to religious beliefs. The table reproduced below below provides illustrations of the data that the CNIL considers to be in principle adapted according to the purposes of the processing.

Categories of data Examples of data For the identification of beneficiaries of social and medico-social support and, where applicable, of their legal representatives Last name, first name, sex, address, email, telephone number, date and place of birth , photography. The photograph should only be collected when it is strictly necessary with regard to the objective pursued (eg: to find a resident of an EHPAD who has escaped the vigilance of the staff). Identification number attached to an organization: membership or beneficiary number. Social security number under the conditions set by Decree No. 2019-341 of April 19, 2019. Nationality of the beneficiary in the form French / EU / non-EU, documents proving the regularity of the stay in France of the person concerned as soon as the benefit of social assistance or benefits is subject to a condition of legal residence. Information relating to the asylum application procedure in the form of submitting an asylum application: yes/no and/or to the procedure for applying for a residence permit in the form of submitting an application for a residence permit yes /no , the

nationality of the person concerned as well as the information necessary to draw up the life story of the person concerned. In exceptional cases, the photocopy of the identity document of the person concerned, particularly in the context of support relating to budget management with public and/or private bodies (e.g.: filing of a file of over-indebtedness with the Banque de France, etc.). Personal life Family situation and composition of the household, if applicable, identification of children taken into care within the framework of child protection, lifestyle habits necessary for the organization of daily life (p. eg: eating habits, physical activity, daily grooming, number of hours of sleep, etc.), interests, language spoken insofar as this information is essential to mention the need for interpreters. Professional career and training within the framework of assistance with the professional integration of people Education, situation with regard to employment, training and qualification. Material living conditions Financial situation: resources, charges, credits, debts. Information may also be collected relating to the list of existing bank accounts, the dates of opening of said accounts, the means of payment, the amount of the authorized overdraft as well as registration, where applicable, in the national incident file. reimbursement of credits to individuals (FICP) and to the central check file (FCC) provided that this information is strictly necessary for the budgetary support provided. Benefits and benefits received: nature, amount, family quotient, beneficiary number. Housing and accommodation situation: type and characteristics of housing or accommodation arrangements (personal home, family home, homeless, makeshift accommodation, mobile accommodation, emergency accommodation, integration accommodation). Means of mobility. To social security Connected organizations and affiliation schemes, open rights. To the bank details insofar as this information is necessary for the payment of a service Bank identity statement (RIB). A social and medico-social assessment of the person concerned Difficulties encountered and assessments of these, assessment of the situation of the people in order to identify the aggravation of difficulties or even a loss of autonomy with regard to the people elderly or disabled. The type of support and actions implemented Areas of intervention, history of support measures, objectives, pathways, planned integration actions, interview and follow-up. For the identification of people contributing to the social and medico-social care and to the entourage likely to be contacted Surname, first name, quality, organization to which they belong, telephone number of the organization, address, email, telephone number of professional or family carers (if applicable, the family relationship: husband / wife, brother / sister, son / daughter, etc.), of the attending physician, of medical experts, of the person of trust. For the identification of people in the context of digital support In exceptional cases, it is possible to save the identifiers and passwords of the personal space of the person concerned when the latter is not in ability to log on alone (e.g. the person concerned is unable to move

around and does not have access to the Internet). The recording of the user's passwords must only be carried out within the framework of a mandate signed between the user and the professional (see example of mandate available on the CNIL website). With regard to the choice of password, the CNIL strongly advises compliance with deliberation no. 2017-012 of January 19, 2017 adopting a recommendation relating to modified passwords. Information relating to certain legal social assistance (non-exhaustive list) Social assistance for accommodation (ASH) and personalized autonomy allowance (APA): data likely to be collected by the departmental councils as part of the investigation, the management and payment of APA and ASH are listed in article R. 232-41 of the CASF. Mobility inclusion card: the data likely to be collected by the MDPHs and the departmental councils within the framework of the instruction, the management and the delivery of the mobility inclusion cards are listed by article D. 241-18-1 of the CASF . Active solidarity income (RSA): data likely to be collected by the family allowance funds (CAF) and the agricultural social mutual funds (MSA) as part of the investigation, liquidation and payment of the RSA are listed in article R. 262-103 of the CASF. Information relating to RSA beneficiaries is the subject of exchanges between the departmental councils and Pôle emploi in order to coordinate their professional integration actions in accordance with the provisions of article R. 262-116-2 of the CASF. be assured of the relevance and proportionality of the personal data it processes, the organization must also ensure, throughout the life of the processing, the quality of this data which must be exact , updated and always necessary for the objective pursued.6. Recipients of data and access to information Personal data can only be made accessible to persons authorized to know it with regard to their attributions. In general, access authorizations must be documented by the organizations, and access to the various treatments must be subject to traceability measures. See point 10 relating to security. Except in special cases, the sharing of information collected should in particular respect the following principles: the information exchanged must only be used to assess the situation of the person or family concerned in order to determine the actions to be taken. implement; these exchanges of information must also be strictly limited to the accomplishment of the missions of the organization or service implementing the processing; they cannot relate to all the information of which the participants are depositaries but must be limited to those necessary for the support and follow-up of people, while respecting their privacy; exchanges must be carried out under the conditions set by the legislative and regulatory texts.6.1. Persons accessing data on behalf of the data controller 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 attributions and the accomplishment of these missions and functions. These may be, for example, professionals and any staff member of

the establishment, the service contributing to one or more of the above-mentioned purposes, within the limits of their respective attributions and the rules governing the sharing and the exchange of information (e.g.: the multidisciplinary team of MDPH referred to in the provisions of article L. 146-8 of the CASF, the professionals and any staff member who is a member of the same care team practicing within the same establishment, etc.).6.2. Recipients of dataThe GDPR defines recipients as any organization that receives the communication of data. Before any communication of information, the data controller must, on the one hand, question the purpose of the transmission to ensure its relevance and legitimacy and, on the other hand, verify that the data communicated is adequate. , relevant and not excessive with regard to the purpose pursued. Within the framework of this reference system, the recipients of the data may in particular be (non-exhaustive list): in the case of data processed by a person subject to medical/professional secrecy, professionals and any member of staff who is a member of the same care team or not and who does not practice within the same establishment, subject in the latter case to obtaining the consent of the person concerned in accordance with the provisions of Article L. 1110- 4 of the CSP, who participate in one or more of the aforementioned purposes; the persons called upon to intervene in the financial and succession management of the assets of the person who has been the subject of a accompaniment and follow-up; bodies instructing and paying social benefits; bodies funding and managing, exclusively concerning previously anonymized data, with the exception of those authorized by a legal or regulatory provision to obtain the communication of data of the personal nature of the persons supported; the competent administrative authorities mentioned in the provisions of Articles R. 331-8 et seq. of the CASF, with regard exclusively to previously anonymized data, in the context of reports of serious malfunction or event having the effect of threaten or compromise the health, safety or well-being of supported persons.6.3. ProcessorsThe GDPR defines processors as the natural or legal person, public authority, service or other body which processes personal data on behalf of the controller. This may be, for example, IT service providers (hosting, maintenance, etc.) or any organization offering a service or provision involving the processing of personal data on behalf of another organization (e.g.: payroll management for employees or agents, etc.). 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). To find out more, a guide for subcontractors, published by the CNIL, recalls these obligations and gives examples of clauses to be included in contracts.6.4. Authorized third partiesThe legally authorized authorities are likely, within the framework of a particular mission or the exercise

of a right of communication, to ask the data controller for the communication of personal data (e.g.: Pôle emploi or social security organizations in the context of the fight against fraud, the administration of justice, the police, the gendarmerie, etc.). In this case, the controller must ensure the binding nature of the provision put forward and transmit only the data provided for by the text, or, if the latter does not list them, the only data essential with regard to the purpose of the right of communication in question. To find out more, the organization can consult the practical guide authorized third parties on the CNIL website. 6.5. Transfers of personal data outside the European Union 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 clauses protection, a code of conduct or a certification mechanism approved by the CNIL; or be framed by ad hoc contractual clauses previously authorized by the CNIL; or meet one of the derogations provided for in Article 49 of the GDPR. To find out more, the organization can consult the section Transferring data outside the EU on the CNIL website.7. Storage periods A precise storage period for the data must be set according to each purpose: this data cannot in fact be kept for an indefinite period. The data storage period or, when it is impossible to set it, the criteria used to determine this duration, are part of the information that must be communicated to the data subjects. Under these conditions, it is the responsibility of the controller to determine this duration before carrying out the processing. recommended that the data collected and processed, for the needs of reception, accommodation and social and medico-social support for people, not be kept in the active database for more than two years from the last contact from of the person who has been the subject of this support (e.g.: last email or letter sent by the person concerned, etc.), except for legal provisions laws or regulations to the contrary or particular case. This storage period is that recommended by the Commission with regard to all the purposes covered by the reference system. The data may also be kept longer than the periods mentioned above, in intermediate archiving, in certain specific cases, for example if the data controller has a legal obligation to do so (for example, to meet accounting, social or tax obligations) or if he needs to constitute proof in the event of litigation and within the limit of the applicable statute of limitations/preclusion (e.g. discrimination). The duration of the intermediate archiving must however respond to a real need, duly justified by the data controller after a preliminary analysis of various factors, in particular the context, the nature of the data processed and the level of risk of a possible dispute. At the end of these periods, the data is destroyed in a secure manner or archived under conditions defined in accordance with the provisions of the Heritage Code

relating to the obligations of archiving public sector information for the organizations subject to these provisions, d on the one hand, or in accordance with the provisions of the deliberation of the CNIL on the adoption of a recommendation concerning the methods of electronic archiving of personal data for organizations in the private sector, on the other hand. The following table contains examples for which the retention period is in principle adequate with regard to the texts (non-exhaustive list):Processing activities

Processing details

active base

Intermediate archiving

Reference texts

Instruction on the management and payment of legal social benefits

APA/ASH

Six years after the cessation of his right to the benefit or after the intervention of a final decision in the event of litigation

For the purposes of departmental management concerning knowledge of the population of applicants and beneficiaries of APA and ASH as well as for the constitution of statistically representative samples provided for in Article L. 232-21-2 of the CASF, aimed at making it possible to study people's situations and backgrounds, including when they change departments, the data may be kept beyond the six-year period, linked to an anonymity number

Art. CASF R. 232-46

As part of the exchange of data between Pôle emploi and the departmental council for the orientation and support of RSA beneficiaries

A maximum of two months from the transmission of the information

Three years from the transmission of the information to Pôle emploi

Art. CASF R. 262-116-4

Instructions for managing and issuing the mobility inclusion card

Inclusion mobility card

Five years from the expiry date of the last decision made or during which no intervention was recorded in the person's file

Beyond this period, the information output from the processing system is archived on a separate medium and can be kept for

ten years under security conditions equivalent to those of the other data recorded in the processing.

Art. CASF 241-19-3

Medical and social support for the person concerned

Medical file

Two years from the last contact with the data subject

Twenty years from the date of the last stay of its holder within the establishment of its care

If the person holding the file dies less than ten years after his last visit to the establishment, the file is kept for a period of ten years from the date of death.

Art. R. 1112-7 of the CSP7.2 Retention of anonymized data 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, by anyone, be related to the identified natural person to whom they initially related. Anonymization must be distinguished from pseudonymization where it is technically possible to find the identity of the data subject through third-party data. Indeed, the pseudonymization operation is reversible, unlike anonymization. Thus, the data controller can keep the anonymized data for an indefinite period. In this case, the organization concerned must guarantee the anonymized nature of the data in a permanent way. To find out more, the organization can consult the following CNIL guides: Security: Archiving in a secure manner; Limiting the retention of data;Practical guide: retention periods.Anonymisation is a process that consists of using a set of techniques in such a way as to make it impossible, in practice, to identify the person by any means whatsoever and this in an irreversible manner. Also, once anonymised, the data can no longer be linked to a person (For more information, you can refer to the EDPS guidelines on anonymisation).8. Information to individuals Processing of personal data must be carried out in complete transparency vis-à-vis the individuals concerned. , 13 and 14 of the GDPR. From the stage of the collection of personal data, the persons concerned must in particular be informed of the existence of the processing, of its essential characteristics (including the identity of the controller and the purpose pursued) and the rights they have. Examples of information notices are available on the CNIL website and can be consulted in the GDPR section: examples of information notices .8.2 Information procedures In order to respect fully the principles of fairness and transparency and in accordance with the provisions of Articles 13 and 14 of the GDPR, persons must in principle be directly informed at the time the data is collected. If the GDPR does not impose any specific form, written information must be preferred so as to be able to justify its content, as well as the

time when it was issued. social and medico-social support for individuals, the data controller informs the individuals concerned and, where applicable, their legal representatives by any appropriate means (eg. ex. : mentions of information inserted in the welcome booklet, the residence contract, the DIPEC, the accommodation contract, the application forms for social benefits, etc.), in an understandable language and according to appropriate and adapted to their situation (e.g.: pictogram, orally, fun images, especially when the public concerned is a minor, use of the Easy to read and understand method known as FALC, etc.) in accordance with the provisions of the article 12 GDPR. In general, the Commission recommends oral information in addition to written information in order to ensure that the data subject understands the information communicated.9. Rights of persons The persons concerned have the following rights, which they exercise under the conditions provided for by the GDPR (to go further, see the section entitled Understanding my rights on the CNIL website): the right of access, allows the data subject to know whether data concerning him is processed by the data controller and, in this case, to obtain details of the conditions of this processing and, at his request, to obtain a copy of the data concerning him held by this person in charge; the right of rectification, allows the data subject to request the rectification of inaccurate or incomplete information concerning him; the right to erasure, allows the data subject to ask an organization to erase data from personal nature concerning it (e.g.: the data is erased by the data controller to comply with the retention periods set by legislative or regulatory texts, the person has withdrawn the consent on which the processing is based, etc.); the right to limit processing (for example, when the person disputes the accuracy of their data, they can ask the body to temporarily freeze the processing of his data, the time that he carries out the necessary checks); the right to portability, under the conditions provided for in accordance with the provisions of the GDPR, offers the person concerned the possibility of recovering part of the data concerning him in an open and machine-readable format in order to reuse them for personal purposes. This right only applies if the following three conditions are met: limitation to personal data provided by the person concerned; application only if the data is processed in an automated manner (exclusion of paper files) and on the basis of the prior consent of the data subject or the performance of a contract concluded with the data subject; respect for the rights and freedoms of third parties; the right to object to the processing of their data, subject to the conditions for exercising this right pursuant to the provisions of Article 21 of the GDPR. social and/or medico-social support, the person concerned may object to the processing of their data, provided that they invoke reasons relating to their particular situation, and only when the processing is implemented on the legal basis of the legitimate interest of the data controller, or for the performance of a task in the public interest or a task falling within the

exercise of official authority (e.g.: the data controller may refuse to the person concerned the exercise of his right of opposition when the processing of information concerning him is based on a legal obligation). The controller may refuse to respond to this request for opposition if he demonstrates that he has interests legitimate and compelling reasons which prevail over the rights and freedoms of the applicant. Note: The controller must respond to requests received as soon as possible and within a maximum of one month. If additional time is necessary to process the request (for example, due to its complexity), the data subject must be informed within this same period of one month. In all cases, a response must be provided within a period that may not exceed three months. The exercise of rights by individuals must be facilitated by the data controller and be free of charge. The persons concerned must be informed of their possibility of lodging a complaint with the National Commission for Computing and Liberties if they are not satisfied with the processing of their personal data. 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 reference system, the organization is invited to implement the following measures, or to be able to justify the implementation of equivalent measures or their lack of necessity or possibility (individuals processing a small volume of data take, for example, basic security measures to ensure the security and confidentiality of the data they process):

Categories

Measures

Educate users

Inform and raise awareness of the people handling the data

Write an IT charter and give it binding force

Authenticate users

Define a unique identifier (login) for each user

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

Force user to change password after reset

Limit the number of attempts to access an account

Manage authorizations

Define authorization profiles

Remove 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 mobile computing devices by VPN

Implement WPA2 or WPA2-PSK, or higher, 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 identifier is encapsulated in the URLs

Check that user input matches what is expected

Put a consent banner 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 safe place

Provide security means for the transport of backups

Plan 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

Relations with service providers who process data in the name and on behalf of the data controller (the employing body) must be the subject of a written agreement.

This agreement must contain one or more specific clauses relating to the respective obligations of the parties resulting from the processing of personal data.

The agreement must in particular provide for the conditions for the restitution and destruction of the data. It is the responsibility of the data controller to ensure the effectiveness of the guarantees provided (security audits, visits, etc.).

For more details, you can refer to the subcontracting guide and the examples of subcontracting clauses.

Secure exchanges with other organizations

Do not transmit files containing the personal data of users in clear via general public messaging

Favor means of communication other than general public messaging to communicate information relating to the people accompanied to other social workers or organizations (e.g.: secure exchange platforms, internal messaging, etc.)

Encrypt the sensitive documents to be transmitted, if this transmission uses e-mail

Make sure it's the right recipient

Ensure the confidentiality of secrets (encryption key, password, etc.) by transmitting them through a separate channel (for example, sending the encrypted file by email and transmitting the secret by telephone or SMS

Protect physical premises and offices

Restrict access to premises with locked doors

Install intruder alarms and check them periodically

Store all paper documents relating to users in locked cabinets

Lock the access door to the office in case of prolonged absence

Supervise IT developments

Offer privacy-friendly settings to end users

Strictly regulate free comment areas

Test on fictitious or anonymized data

Use cryptographic functions

Use recognized algorithms, software and libraries

Store secrets and cryptographic keys securely

Securing user passwords

Use a password manager or a notebook stored in a safe to record the passwords of users supported in the context of digital support. To do this, the data controller can usefully refer to the Guide to the security of personal data.Warning:

In the event of the hosting of personal health data carried out on behalf of organizations providing social or medico-social monitoring by an IT service provider, the latter must be approved or certified for the hosting, storage, conservation of health data, in accordance with the provisions of Article L. 1111-8 of the Public Health Code.11. Data protection impact assessment (DPIA) Processing for the purpose of social and medico-social support for persons appearing on the list of types of processing operations for which a DPIA is required must systematically give rise to prior completion of a DPIA.

Types of processing operations

Examples

Processing of health data implemented by health establishments or medico-social establishments for the care of people

- Processing of the files of residents cared for by a municipal social action center (CCAS) or by an accommodation establishment for dependent elderly people (EPHAD).

Processing for the purpose of social and/or medico-social support for people

- Processing implemented by an establishment or association as part of the care of people in social and professional integration or reintegration;

- processing implemented by the MDPH in the context of the reception, accommodation, support and monitoring of these people;

- treatment implemented by a municipal social action center as part of the follow-up of people with chronic disabling pathologies in a situation of social fragility. In this respect, it is based on two pillars: the fundamental principles and rights set out in particular by the GDPR and the Data Protection Act and which must be respected regardless of the nature, gravity and likelihood of the risks incurred; the management risks to privacy, which makes it possible to determine the appropriate technical and organizational measures to protect the data. To carry out an impact study, the data controller may also rely on: - the principles contained in this reference system; - as well as on the methodological tools offered by the CNIL on its website. If the organization has appointed any, the DPD/DPO must be consulted. In accordance with article 36 of the GDPR, the data controller must consult the CNIL beforehand to the implementation of the processing if the impact assessment indicates that it fails to identify sufficient measures to reduce the risks to an acceptable level.

M. L. Denis