Afeji
Hauts-de-France

TOUTES LES VIES
ONT LA MÊME VALEUR

Child Protection Charter

www.afeji.org

Table of Contents

Mapping of risks identified in institutions providing child protection services.

RISK SITUATIONS	DESCRIPTION	EXISTING PREVENTION MEASURES	ACTIONS TO BE TAKEN
Emergency reception	Placement carried out in difficult conditions, possibly involving law enforcement. Risk of trivialising emergency reception situations.	Where possible, a professional is assigned to the group to welcome the child and introduce them to their new living environment. Existing tool: welcome booklet	Provide a place for welcoming children outside of the (modular) groups.
Community life and pace of life	Each child has their own pace of development and specific needs related to their life experience.	Personalised project for the child	Dashboard to be formalised.
Community life and living space	The architecture of the houses does not allow children to have individual spaces. Problem / Physical and psychological privacy.	Attention paid by professionals (e.g. knocking on the door before entering the room, vigilance regarding alternating occupancy of the premises during hygiene care). Children are allowed to bring their personal belongings.	Maintain a discussion on the proper use of spaces with the teams.
Change of school	A change of geographical area due to placement is often accompanied by a change of school and a break with the child's social environment.	Regular meetings. Discussions between MECS psychologists and the school psychologist for the area.	Systematise referrals to the school with a professional.
Verbal and physical abuse	The exhaustion of professionals faced with psychological and behavioural issues is a significant risk factor for possible violence in response.	Educational meetings begin with a debriefing of past difficult situations that may or may not have required an incident report. Department heads and psychologists pay particular attention to the state of the professionals. Professionals are encouraged to express their difficulties. Discussions are frequent.	Training for professionals. Intensify traceability.
Possible representations by professionals regarding the child's situation.	Example: Child suffering from autism, who has committed sexual assaults...	Work on the representations of professionals.	Training planned on sexual assault.
Physical and psychological care to be identified.	Time required to access healthcare professionals and organisations.	Working in partnership with the nurse, paediatric nurse and psychologists on site, as well as with the various carers.	Development of care team partnerships
Use of vocabulary specific to social workers and the legal field. Use of	The unintentional use of professional vocabulary can lead to difficulties in	Professionals must be vigilant in ensuring that their speech is understandable and	Work on the PP in team meetings to consider communication with users and

acronyms.	understanding for children and their parents. This can impact the quality of the educational relationship.	that it is understood.	their families.
Consumption of Psychotropic drugs among minors in care. (medication, narcotics, alcohol, etc.)	Normalisation of substance use.	Health partnerships: CSAPA in Dunkirk Michel Association Collective prevention provides information about the risks. Individual support is more effective.	Develop partnerships on prevention.
Sexual exploitation of minors	Growing societal phenomenon Professionals must be vigilant and know how to detect these situations	Discussions about relevant situations with the 'Compass'.	Specific training over 3 days, offered in 3 sessions.
Instability of educational teams	Recruitment difficulties linked to a decline in interest in social work professions; this is particularly noticeable in boarding schools. This phenomenon is accentuated in the case of emergency replacements (sick leave). The risk is insecurity for the children and adolescents in care.	Support for new professionals.	Creation of a welcome booklet for new employees.
Decline in the number of qualified professionals.	Inexperienced or even untrained professionals may lack the interpersonal skills and expertise necessary to support those in care.	Support for professionals, training proposals (particularly intra-association training).	
Minors accompanied to appointments and visitation rights by drivers.	Insecurity linked to a lack of knowledge of the overall situation of the child and their family.	Preparing children for appointments and discussing their experiences afterwards.	Encourage the completion of DDVs on site and define the policy on Media Visits.

Prevention of unacceptable behaviour when working with children.

An associative procedure defines risk situations and the plan for promoting well-treatment in all establishments caring for children.

The guidance note on the prevention of abuse and violence is attached in Appendix 1. This note is supplemented by a procedure setting out the steps to be taken in the event of abuse, presented in Appendix 1.1.

These documents are revised in line with changes in French legislation, but also as part of the ongoing process of improving the quality of the services offered by AFEJI.

Description of secure recruitment procedures.

Decree No. 2024-643 of 28 June 2024 sets out the procedures for checking the criminal records of professionals and volunteers working with minors. The certificate of good conduct is a mandatory document for all professionals and volunteers working in the fields of child protection and early childhood care. It guarantees that the person has no convictions recorded on their criminal record or on the automated judicial file of sex and violent offenders (FIJAISV) that would prevent them from working with minors. When hiring or applying for accreditation, and at regular intervals during professional practice, this certificate must be presented to the employer, who will verify its validity and authenticity.

This obligation applies in particular to:

- childminders and family assistants (including persons over the age of 13 living in their home, with the exception of minors placed in care under child welfare services);
- professionals and volunteers working in early childhood care facilities or services (nurseries) and child protection services (MECS, children's villages, homes, etc.).

AFEJI Hauts-de-France therefore makes the recruitment of professionals and volunteers in establishments caring for minors conditional upon the presentation of this certificate of good conduct.

Information on data protection procedures.

AFEJI Hauts-de-France has formalised a General Data Protection Regulation (GDPR) and officially appointed a Data Protection Officer (DPO).

The association's general data protection policy is attached in Appendix 2. In addition, Appendix 3 describes the association's procedure for managing personal data breaches.

These documents are reviewed in light of changes in French legislation, under the supervision of AFEJI's Data Protection Officer, whose role is to ensure that the association's general data protection policy remains compliant.

As part of the association's welcome programme at an AFEJI establishment, association procedures govern the protection of children's privacy:

- Charter of rights of the person being cared for: Appendix 7,
- The right to voice and image: Appendix 8,
- Image rights authorisation form for minors: Appendix 9.

Staff training in child protection and safeguarding policies.

AFEJI Hauts-de-France has a recruitment policy that aims to hire qualified professionals to work with children, who have the necessary qualifications: early years educators, specialised educators, nurses, psychologists, managers and executives.

The managing director of the AFEJI Hauts-de-France association, Mr Karim LOUZANI, is implementing a wide-ranging HR policy for professionals responsible for child protection. To this end, the managing director has approached the CREAI Hauts-de-France for a training programme dedicated to professionals in the "child protection sector". The association has developed a specific continuing education programme for child protection professionals. These training courses are developed in collaboration with an external organisation, the CREAI, and focus on specific topics related to supporting children in the context of child welfare:

- An annual refresher course
- A three-day programme on basic knowledge in child protection
- Specific training on professional writing in child protection
- A session on prostitution among minors.

All professionals working in child protection benefit from these training programmes, under annual agreements with CREAI. This child protection training mission updates the most current knowledge and reflects the challenges of the mandate.

public sector in the renovation of professional practices, provides professionals with theoretical and clinical frameworks.

The training courses have multiple objectives:

- Updating legal knowledge (child protection texts and reports),
- Understanding the fundamental needs and classification of children's needs,
- Use common knowledge frameworks,
- Sharing the same theoretical reference frameworks with partners,
- Develop a reflective and methodological approach to ensure collective professional practices are safe.

Procedures and reporting authority

AFEJI Hauts-de-France has established procedures for managing adverse events in childcare facilities. French law distinguishes between two types of adverse events
:

- undesirable events, which refer to a situation that deviates from procedures or expected results and that is or could potentially be a source of harm. An undesirable event can therefore jeopardise the safety of those receiving care, the safety of professionals or the organisation of the establishment.

- Serious adverse events, which affect the care of users, their support or the respect of their rights. Serious adverse events compromise the health, safety or physical or moral well-being of the people being cared for (Article L.331-8-1 of the Social Action and Families Code).
  Serious adverse events must be reported to the supervisory and pricing authorities within 48 hours of their occurrence (Département du Nord). The report is made by the director of the establishment.

The procedure for managing adverse events is presented in Appendix 4.

The adverse event reporting form is presented in Appendix 5. This form is intended for the Département du Nord, the supervisory and pricing authority for child protection establishments.

To ensure that all professionals are aware of the procedures in place, an information document on the management of adverse events is signed by all employees (Appendix 6).

Management of complaints and claims.

The issue of children's expression in child protection is central to the support offered by AFEJI. Tools and procedures are therefore in place to enable the collection, processing and management of complaints and claims in institutions: see Appendices 10 and 11.

These procedures ensure that every request and every complaint made by a child is heard, taken into account and responded to. Each child is therefore aware of these tools, which are adapted to their age so that they can be understood. Several institutions have introduced complaint or suggestion forms, accessible to children, which can be placed in suggestion boxes, promoting a simple and recognisable means of expression for children (Appendix 13).

Each establishment also displays the national helpline numbers for children (Appendix 12).

Lille, le 15 septembre 2025,
Karim LOUZANI,
General Director
AFEJI Hauts-de-France

Karim LOUZANI

Certified by yousign

Appendices

Appendix 1: Guidance note on the prevention of abuse and violence Appendix 1.1: What to do in the event of abuse

Appendix 2: General data protection regulations

Appendix 3: Procedure for managing personal data breaches Appendix 4: Management of adverse events

Appendix 5: Adverse event reporting form

Appendix 6: Information provided to employees concerning the management of adverse events Appendix 7: Charter of rights and freedoms of the person receiving care

Appendix 8: Image and voice rights

Appendix 9: Image rights form for minor beneficiaries Appendix 10: Complaints and claims management

Appendix 11: procedure for managing requests from data subjects Appendix 12: child protection helpline

Appendix 13: Idea and complaint form

Preventing abuse and promoting good treatment are major challenges for social, medical-social and health care institutions. Professionals work with people in complex situations on a daily basis. They must balance the quality of care with preserving the dignity of the person receiving care. Furthermore, the Law of 2 January 2002 requires that "the effective exercise of users' rights be guaranteed and, in particular, that any risk of abuse be prevented". The manual for assessing the quality of social and medical-social establishments and services reaffirms these principles.

Thus, each establishment and service of the AFEJI Hauts-de-France must implement a plan to prevent the risk of abuse and violence and define an adequate organisation to ensure that it is dealt with. This guidance note sets out the expected formal requirements.

This note applies to all AFEJI Hauts-de-France establishments and services.

Reference documents:

- Law No. 2002-2 of 2 January 2002 reforming social and medico-social action,
- Law No. 2022-140 of 7 February 2022 on child protection,
- Articles L.331-8-1 and P.331-8 of the Social Action and Families Code,
- Article P.226-2-2 of the Social Action and Families Code,
- Article P.4127-44 of the Public Health Code,
- Decree of 28 December 2010 on the obligation to report social
  social and medico-social facilities,
- High Authority for Health Manual for assessing the quality of social and medical-social establishments social and medico-social services, March *2022.*
- High Authority for Health: Manual for the certification of healthcare establishments for quality of care, September *2021*

Related documents:

- Charter of rights and freedoms of residents,
- Standard template for a charter of good treatment,
- Standard template for the procedure "Conduct to follow in the event of suspected abuse"
- Standard table format for "Situations at risk of abuse"
- Example of a list of situations at risk of abuse
- Awareness-raising material: " prevention of abuse"
- Allo Enfance en Danger poster (I 19),
- Poster on taking action against abuse of elderly people and adults with disabilities (3977),

ACT: Control and Pricing Authority

Abuse: Article L119-1 of the CASF specifies that "abuse refers to any person in a vulnerable situation when a gesture, word, action or failure to act compromises or harms their development, rights, basic needs or health, and when this harm occurs in a relationship of trust, dependence, care or support. Situations of abuse may be isolated or ongoing, intentional or unintentional. They may originate from an individual, a group or an institution. Violence and neglect can take many forms and be combined within these situations."

Violence (WHO): "The intentional use of physical force or threats against others or oneself, against a group or community, which results in or has a high risk of resulting in trauma, psychological harm, developmental problems or death, moral harm, maldevelopment or deprivation."

The French National Authority for Health (, HAS): "A comprehensive approach to patient or user care and support for their families and friends, aimed at promoting respect for their rights and freedoms, listening to them and taking their needs into account, while preventing abuse.

It promotes

The involvement of users in their care, a central aspect of quality and safety of care:

- Quality of life at work, by focusing on the meaning of work
- Developing active user participation in conjunction with all healthcare stakeholders.

In order to guarantee the safety of care, establishments draw up a plan to prevent situations of abuse and violence. This plan is drawn up on the basis of reports from professionals or situations identified in the course of implementing the personalised project for the people in care (an annual review meeting may be devoted to drawing up/updating this plan).

Depending on the situations identified as posing a risk of abuse, the institution mobilises the necessary resources to limit their occurrence. Examples: training/awareness programme, sharing of best professional practices, establishment of partnerships, creation of practice analysis teams, etc.
To identify situations at risk of abuse, a table entitled "Situations at risk of abuse" is available for your use.

This plan for the prevention of abuse and violence is included in the School Project. For schools r e q u i r e d to set up a Social Life Council, CVS members are systematically consulted on the areas of focus identified.

The establishment or service is free to appoint a "Well-treatment" representative ( ) from among of its teams.

The establishment or service displays its commitment to combating abuse and violence. The following are displayed in the designated areas

- the Charter of Rights and Freedoms of the Person Receiving Care,
- Government helplines for reporting abuse
  - For establishments or services caring for children, call 119 "AIIo Enhance en danger" (Children in danger).
  - For establishments or services caring for elderly people and adults with disabilities: 3977 "Report abuse of elderly people and adults with disabilities"
- The Charter of Good Treatment (if the establishment or service has has one). *A standard template for the Charter of Good Treatment is available.*

These various elements are also mentioned in the welcome booklet.

The institution formalises a procedure or guidelines to be followed in relation to the management of situations of abuse. *A standard template for this document is available and includes the main points to be considered (listed below).*

Any professional who witnesses or suspects abuse must report it without delay to the director of the establishment or service using the adverse event reporting form.

In accordance with regulatory provisions, the director of the establishment or service is responsible for reporting the facts to the ACT within 48 hours. For establishments caring for minors, the drafting of a report of concern should be considered.

The user's file ensures that the measures put in place for each person receiving support can be traced (both in terms of prevention and immediate action when abuse is confirmed). Examples: consent, refusal of support, gathering expectations and needs, access to common rights, etc.

The personalised support plan (PPA) takes into account the occurrence of abuse. The objectives must be adopted to respond to changes in the situation of the person receiving support.

- ☐ Identification of situations at risk of abuse in the form of a summary table,
- ☐ A plan to prevent the risk of abuse is included in the support plan and developed jointly with members of the CVS (for the establishments concerned),
- ☐ A procedure on how to behave in the event of abuse, presenting the reporting process and the procedures for analysis by the team.
- ☐ A notice displayed in reception areas
  - ☐ From the Charter of Rights and Freedoms of the Person Received,
  - ☐ For establishments supporting children: from 119
  - ☐ For establishments supporting adults: from the Charter of Human Rights and Freedoms ( ) 3977
- ☐ A welcome booklet,
  - ☐ Including the Charter of Rights and Freedoms of the Person Received,
  - ☐ Including government emergency numbers (119 or 3977)

1. Purpose

The purpose of this procedure is to guide professionals on how to proceed in the event of suspected abuse within the institution.

2. Intended recipients

This procedure applies to all professionals within the establishment.

3. Scope of application

This document applies as soon as suspected abuse is reported.

4. Reference documents/related documents

Sources:

- Law No. 2002-2 of 2 January 2002 reforming social and medico-social action,
- Law No. 2022-140 of 7 February 2022 on child protection,
- Articles L.331-8-1 and P.331-8 of the Social Action and Families Code,
- Article P.22ó-2-2 of the Social Action and Families Code,
- Article P.4l 27-44 of the Public Health Code,
- Decree of 28 December 2016 on the reporting obligation of social and medical-social facilities,

Related documents.

- Procedure for reporting an adverse event,
- Adverse event reporting form (incident report),
- [Procedure to follow when reporting information of concern]
- [Form for reporting information of concern]

5. Definitions/abbreviations

ACT: Control and Pricing Authority APS: Regional Health Agency

Abuse: Any situation (gesture, word, action or failure to act) that could compromise or harm the person being cared for (physical, psychological or moral violence, any deprivation of rights, sexual assault or theft).

ó. Description

@UI ?	@UOI? (STEPS)	HOW?
All professionals	In the event of a situation where there is a risk of abuse, the professional • Secures the situation, • Alerts [their line manager] without delay, • Completes the adverse event reporting form, • Record the facts in the user's file.	Procedure and form for reporting an adverse event
[Line manager]	Investigate the facts reported by the professional	Interviews, team meetings, user file, incident report form
Director establishment	Based on the findings of the investigation, the headteacher reports the incident to the relevant AcT and takes the necessary measures. [For institutions caring for minors, the director shall forward any information giving cause for concern to the ACTs].	Procedure for reporting an adverse event

General policy on personal data protection

Date of application	September 2022
Author	DPO Consulting
Issuing department	AFEJI Hauts-de-France – General Management
Validator	DPO Consulting

Distribution		
☐ Confidential	☐Internal	☐Public

Update tracking				
Date	Reference	Author	Subject	Status
12/04/2022	V1	DPO Consulting	Policy	In progress

Table of contents

1. Objectives and scope of application

The terms, beginning with a capital letter, used in this general personal data protection policy (hereinafter the "Policy") are defined in the Appendix "Definitions".

1.1 Objectives of the Policy

AFEJI Hauts-de-France undertakes to **guarantee the protection of Personal Data** obtained in the course of its activities and to comply with applicable laws and regulations regarding the processing of Personal Data and Sensitive Personal Data.

The objectives of this Policy are to:

- **define** AFEJI Hauts-de-France's **commitments** regarding the principles imposed by applicable legislation, in particular European Regulation No. 2016/679 on the protection of personal data, dated 27 April 2016, applicable since 25 May 2018;
- **define the roles and responsibilities** of key contributors; and
- **ensure that adequate methods and procedures are in place**, as well as **appropriate governance and control structures** to guarantee compliance with commitments and applicable legislation.

AFEJI Hauts-de-France's commitments are summarised in the inserts to Rule R010. AFEJI Hauts-de-France's compliance with these rules will be audited under the conditions defined in the "Compliance Control" section.

This Policy is supplemented by the following policies and procedures:

- Privacy by design procedure
- Individual rights management procedure
- Personal data breach management procedure
- Impact assessment guide
- Data retention policy

1.2 Scope

The policy is intended to apply to all employees, partners and subcontractors of
AFEJI Hauts-de-France.
In the event of any conflict between this policy and applicable legislation, the following rules shall apply
shall apply:

- If the policy provides greater protection, it shall take precedence over the applicable legislation.
- If the applicable legislation provides greater protection, it shall apply to the points concerned in place and in place of the Policy.

If any doubt remains, AFEJI Hauts-de-France employees shall seek advice from the DPO.

1.3 Revision

This policy is updated by the AFEJI Hauts-de-France DPO in the event of:

- Significant changes in the business context or in AFEJI Hauts-de-France's personal data protection strategy;
- Significant changes in risk exposure (e.g. new threats, new trends, etc.);
- Significant changes in applicable legislation.

These changes are subject to approval by the AFEJI Hauts-de-France GDPR Steering Committee. Appropriate communication will be provided to AFEJI Hauts-de-France employees in the event of changes.

2. Organisation and governance of personal data protection

Everyone at AFEJI Hauts-de-France is responsible for the protection of personal data. This protection must be a constant concern, reflected in policies, procedures and operational practices.

The key contributors identified in this section shall assume their respective roles and responsibilities to ensure that this Policy is implemented in a consistent and coordinated manner within AFEJI Hauts-de-France.

2.1 Key contributors

2.1.1 Senior Management

Senior Management guarantees AFEJI Hauts-de-France's strong commitment to the protection of Personal Data as a strategic asset of the association. As such, Senior Management must:

- Ensure that appropriate personal data protection governance is in place, defining roles and responsibilities within AFEJI Hauts-de-France and enabling the DPO to be involved, in an appropriate and timely manner, in all matters relating to data protection;
- Communicate to all employees about the appointment of a DPO, his or her tasks and how to contact them;
- Ensure that the DPO:
  - Has the necessary resources and means to carry out their duties;
  - Receives no instructions regarding the performance of their duties;
  - Receives appropriate training;
  - Is able to report directly to senior management.

2.1.2 Business departments

Each head of a business division responsible for the implementation of one or more Processing must:

- Ensure compliance with the principles and rules set out in this Policy and the supplementary procedures and policies;
- Involve the DPO from the design phase onwards in all new projects involving the processing of personal data;
- Carry out a Privacy Impact Assessment, if necessary, with the assistance of the DPO and any other technical experts;
- Document and justify in writing the reasons why the DPO's opinion was not followed, where applicable ;
- Respond to any request for information from the DPO on any matter that impacts the private lives of individuals. of individuals;
- Provide all documentation relating to Processing within their scope of intervention;
- Register any new processing operations in the AFEJI Hauts-de-France processing register.

2.1.3 The Data Protection Officer ("DPO")

AFEJI Hauts-de-France has appointed a Data Protection Officer (DPO) to ensure AFEJI Hauts-de-France's compliance with applicable legislation and the commitments made under this Policy.

DÉLÉGUÉ À LA PROTECTION DES DONNÉES DÉSIGNÉ

N° SIREN	817754138
Organisme désigné	DPO CONSULTING
Nom du représentant légal	Madame Marine BROGLI
Nom de la personne en charge de la désignation	Madame Externalisation dpo DPO CONSULTING
Date de prise de fonction	16/06/2021
Adresse postale	1 RUE DE CAUMARTIN 75009 PARIS
Pays	FRANCE

The DPO has several responsibilities within AFEJI Hauts-de-France:

- Informing and raising awareness among employees of the rules to be followed with regard to the protection of personal data;
- Ensuring compliance with applicable legislation and the commitments made under this Policy;
- Advising business departments on the practical application of principles to projects Processing;
- Inform and empower, or even alert if necessary, the senior management of AFEJI Hauts-de-France of the risks that operational initiatives or failure to comply with its recommendations could pose to AFEJI Hauts-de-France;
- Determine whether a Data Protection Impact Assessment (DPIA) needs to be carried out and advise the business department on how to carry out the DPIA;
- Assist in the event of a personal data breach to assess the risk of the breach and act as a point of contact in the event of notification to the competent supervisory authority and/or the data subjects;
- Analyse, investigate, audit and monitor AFEJI Hauts-de-France's level of compliance and assist the business departments in defining and implementing a remediation plan where necessary;
- Establish and maintain documentation for accountability purposes;
- Ensure the proper management of the rights of data subjects as defined in the relevant procedure;
- Submit an annual report to senior management;
- Interact with the supervisory authority.

The DPO may appoint one or more deputies from among AFEJI Hauts-de-France employees.
Hauts-de-France. The DPO shall communicate this appointment in an appropriate manner.

2.1.4 Information systems management

For each project, the CISO provides support and expertise on the following topics:

- Assessment of the context and criticality of the project;
- Risk analysis, particularly in the context of the preliminary assessment prior to the impact assessment on ;
- Advice on security measures to reduce, avoid or transfer risks:
- Assessment of the security level of third parties involved and negotiation with them to incorporate AFEJI Hauts-de-France's requirements in this area into the contract;
- Coordination of the monitoring, detection and management of security incidents, with advice from the DPO in the event of a data breach.

2.2 Annual report by the DPO

The DPO prepares and publishes an annual report on privacy-related activities within AFEJI Hauts-de-France. To this end, the DPO defines, collects and publishes indicators that highlight the level of compliance with internal policies and procedures in this area and with applicable legislation.

3. Principles to be observed in relation to the processing of personal data

In accordance with applicable legislation, AFEJI Hauts-de-France undertakes to comply with the following principles when collecting and processing personal data.

3.1 Lawfulness, fairness and transparency

Personal data must be collected and processed in a **lawful, fair and transparent** manner**.**
As such, AFEJI Hauts-de-France guarantees that all processing is based on a **legal basis recognised** by applicable legislation, such as:

- The data subject has given their consent to the processing of their personal data for one or more specific purposes (subject to compliance with the additional requirements detailed in the "Consent" section);
- The processing is necessary for the performance of a contract to which the data subject is party or in order to take appropriate measures at the request of the data subject prior to entering into a contract;
- The processing is necessary for compliance with legal obligations to which AFEJI Hauts-de-France is subject;
- Processing is necessary for the purposes of the legitimate interests pursued by AFEJI Hauts-de-France;
- Processing is necessary to protect the vital interests of the data subject;
- Processing is necessary for the performance of a task carried out in the public interest.

When processing is based on legitimate interest, AFEJI Hauts-de-France conducts an analysis to determine whether this legitimate interest takes precedence over the interests or fundamental rights and freedoms of the data subjects. This assessment and its results must be documented and recorded for evidentiary purposes (accountability).

In exceptional cases, AFEJI Hauts-de-France may process sensitive personal data, in which case AFEJI Hauts-de-France shall ensure that it complies with the requirements of the "Processing of sensitive personal data" section of this Policy.

R01 All Processing is based on a clearly identified legal basis and documented in the register.

Furthermore, AFEJI Hauts-de-France ensures that personal data processing activities are carried out in an **open and transparent** manner. To this end, AFEJI Hauts-de-France provides accessible and intelligible information to Data Subjects on how their Personal Data is used, in accordance with the terms and requirements of the data subject rights management procedure (see the "Relations with Data Subjects" section of this Policy).

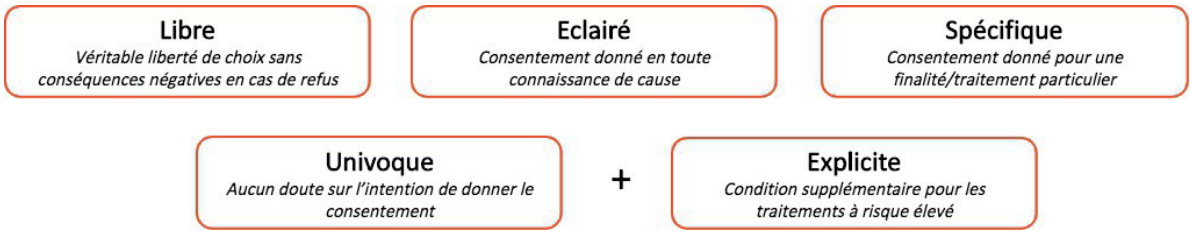
3.2 Consent

When Processing is based on the Consent of the Data Subject, AFEJI Hauts-de-France ensures that this Consent has been obtained legally (see Section on "Conditions of

Consent Validity") and is properly managed throughout the duration of the Processing (see Section "Consent Management").

3.2.1 *Conditions for the validity of Consent (characteristics and methods of collection)*

AFEJI Hauts-de-France ensures that the consent obtained from the data subject (or their legal representative/guardian) meets the following criteria:



In addition, AFEJI Hauts-de-France must, where applicable, ensure compliance with local laws on the conditions for the validity of Consent.

This Consent must be obtained prior to the collection of Data and, at a minimum, concurrently with the collection of Data. The request for Consent must be distinguished from any other request/subject, in an intelligible and easily accessible form, in clear and simple language.

R02 When the legal basis is Consent, the Consent obtained meets the conditions of validity in terms of substance (characteristics) and form (collection).

3.2.2 *Management of consent (duration, proof)*

AFEJI Hauts-de-France ensures that **consent remains valid**: when the processing methods change or evolve, the original consent is no longer valid. New consent must then be obtained.

AFEJI Hauts-de-France keeps **track**, as far as possible, **of the declarations of consent received**, i.e. who gave their consent, how and when consent was obtained, as well as a copy of the information provided to the data subject at the time.

R03 Consents are renewed in the event of a significant change in the terms of Processing.

R04 A system for monitoring declarations of consent is put in place.

3.2.3 *Withdrawal of consent*

The Data Subject must be able to **withdraw their Consent at any time**. AFEJI Hauts-de-France must provide the Data Subject with the means to withdraw their Consent as easily as it was given, as far as possible by a method equivalent to that used to obtain Consent.

Once consent has been revoked, AFEJI Hauts-de-France must ensure that the **withdrawal is recorded in its systems** and databases as soon as possible, so that personal data is no longer processed for the purpose in question (for example, a customer who revokes their consent to receive advertising should no longer receive it). In addition, this change of

status must be **communicated to all third parties involved**, in particular Subcontractors, so that none of them process the Personal Data concerned for the purpose in question. Once Consent has been revoked, AFEJI Hauts-de-France can no longer rely on Consent as the legal basis for Processing. However, the withdrawal of Consent:

- does not affect the lawfulness of Processing based on Consent prior to its withdrawal, and
- does not necessarily require the deletion of the Personal Data concerned, as it may still be useful for other Processing and/or be of administrative interest.

R05 The Data Subject has the option to withdraw their Consent at any time as easily as it was given.

R06 Withdrawal of consent is effectively taken into account in the processing tools.

3.3 Purpose limitation

Before collecting any personal data, AFEJI Hauts-de-France clearly defines the purpose(s) of the collection, which must be **specific, explicit and legitimate**. AFEJI Hauts-de-France also ensures that the purpose(s) thus defined are compatible with its activities.
Personal Data must not be processed for a subsequent purpose that is incompatible with the initial purpose for which the Data was collected. To this end, AFEJI Hauts-de-France carries out a **compatibility test** to verify whether the subsequent purpose is compatible with the initial purpose. This test takes into account:

- The existence of a link between the two purposes;
- The context in which the Personal Data was collected, in particular with regard to the relationship between the Data Subjects and AFEJI Hauts-de-France;
- The nature of the Personal Data, in particular if sensitive Personal Data is processed;
- The possible consequences of the envisaged further processing for the Data Subjects;
- The existence of appropriate safeguards.

When the subsequent purpose is incompatible with the initial purpose, AFEJI Hauts-de-France ensures that it obtains the consent of the data subject, in accordance with the requirements of the applicable legislation (Article 6(4) of the GDPR).

R07 Personal Data is collected only for specific, explicit and legitimate purposes, and must not be further processed in a manner incompatible with those purposes.

3.4 Minimisation and accuracy

Personal Data collected must be **adequate, relevant and not excessive** in relation to the purpose of the Processing. In other words, AFEJI Hauts-de-France ensures that only Data that **is strictly necessary** to achieve the purpose is collected.

In addition, AFEJI Hauts-de-France ensures that Personal Data is **accurate and, where necessary, updated**. To this end, and taking into account the purpose for which it is processed and the resulting need for accurate Data, AFEJI Hauts-de-France takes **reasonable measures** to delete or rectify any inaccurate Personal Data without delay.

R08 Personal Data is adequate, relevant and not excessive in relation to the purpose of the Processing. It is accurate, complete and updated where necessary.

3.5 Limited retention

AFEJI Hauts-de-France ensures that Personal Data processed is **not retained for longer than is necessary** for the purposes for which it was collected.

Personal Data may be retained:

1) In a form that allows the identification of data subjects for a **period not exceeding that necessary for the purposes** for which it is processed by AFEJI Hauts-de-France. Once the purpose has been achieved, the Data must therefore **be deleted**.

2) Beyond the period necessary for the purpose of the Processing, when it is still **of administrative interest**. The retention period for the Data may then be extended beyond the period deemed relevant for the initial purpose of collection. This extension must be duly **justified and documented**.

Data may still be retained in order to comply **with legal limitation periods**, **specific retention periods** (retention of accounting documents and supporting documents, archiving of electronic contracts, etc.), mainly for **evidentiary purposes**, or in order to be able to **respond to requests for disclosure** that may be made by certain legally authorised third parties (tax authorities, social security organisations, etc.)..

3) For **longer periods**, insofar as Personal Data will be processed exclusively by AFEJI Hauts-de-France **for archiving purposes** in the public interest, for **scientific** or **historical research purposes,** provided that appropriate technical and organisational measures are implemented to guarantee the rights and freedoms of the data subject, such as **anonymisation** or **pseudonymisation**.

In order to ensure compliance with this principle, AFEJI Hauts-de-France defines the retention periods applicable to each Processing operation. The following elements must be taken into account when determining the retention period for each category of Data collected:

- legal obligations;
- CNIL recommendations;
- best practices in each relevant field;
- the operational needs of AFEJI Hauts-de-France.

These periods are **reviewed and updated as necessary** to reflect changes in applicable legislation and/or practices within AFEJI Hauts-de-France.

At the end of this period, the Data is **deleted without undue delay**. This deletion may be carried out by destroying the Data and/or anonymising it. In the event of deletion by destruction, AFEJI Hauts-de-France ensures that the Data is effectively destroyed from the systems (including when the systems concerned are those of a third party).

The requirements and procedures for implementing the principle of limited retention of Personal Data are detailed in AFEJI Hauts-de-France's "Personal Data Retention/Deletion Policy".

R09 Retention periods are defined and implemented.

3.6 Security of Personal Data

AFEJI Hauts-de-France takes **technical and organisational measures** to ensure **the security, confidentiality and integrity** of Personal Data throughout the entire Processing period. The following factors are taken into account when determining these measures:

- the severity and likelihood of potential harm resulting from the loss, alteration and/or unauthorised access to the Data;
- the characteristics of the Processing concerned;
- where applicable, the results of the privacy impact assessment conducted;
- the state of the art;
- the implementation costs.

AFEJI Hauts-de-France has established an information system security policy (PSSI) detailing all the technical and organisational security measures implemented. This PSSI is regularly reviewed and updated.

AFEJI Hauts-de-France undertakes to regularly review security measures in order to **test, evaluate and measure their effectiveness and to make any necessary improvements**.

AFEJI Hauts-de-France also ensures that any Data Breaches are handled correctly in accordance with the "Data Breach Management" section of this Policy.

R10 Appropriate technical and organisational measures are implemented to ensure the security, integrity and confidentiality of Personal Data.

3.7 Transfer of Personal Data outside the European Union

Transfers of personal data require additional attention and safeguards. AFEJI Hauts-de-France ensures that all transfers of personal data are **adequately secured** and **legally regulated** in accordance with the requirements of applicable legislation.

To this end, AFEJI Hauts-de-France ensures that it:

- **Identify all transfers** of personal data, including, where possible, subsequent transfers by subcontractors (of the first rank);
- **Regulate** Data Transfers **in the contract** with the service provider and, where applicable, the location where the Data is hosted (which must, in principle, be within the European Union). The service provider must therefore guarantee the implementation of measures to ensure a level of protection of Personal Data equivalent to that provided by the GDPR;
- **Secure all transfers** using appropriate technical and organisational measures;
- When the Transfer is not to a country recognised as adequate (under an adequacy decision by the European Commission), provide a legal framework for the Transfer through an **appropriate mechanism**.

Where possible, Personal Data should not be transferred automatically to a country outside the European Union without the authorisation of the DPO of AFEJI Hauts-de-France.

R11 All transfers of personal data are adequately secured and legally regulated in accordance with the requirements of applicable legislation.

3.8 Processing of sensitive personal data

In addition to the generic legal basis (see section "Lawfulness, fairness and transparency"), sensitive personal data may ONLY be collected if one of **the** following **special conditions** applies:

- The Data Subject has given their explicit Consent;
- Processing is necessary for the purposes of fulfilling the obligations and exercising the rights specific to AFEJI Hauts-de-France or to the data subject in relation to labour law, social security and social protection;
- Processing is necessary to safeguard the vital interests of the data subject;
- The processing relates to personal data which are manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise or defence of legal claims ;
- Processing is necessary for reasons of substantial public interest, on the basis of European Union or Member State law which must be proportionate to the objective pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the Data Subject;
- The processing is necessary for the purposes of preventive medicine, occupational medicine, the assessment of the worker's ability to work, medical diagnoses, health or social care, or the management of health care systems and services;
- A specific condition provided for by local law applies.

AFEJI Hauts-de-France must provide **specific security measures** for this Data in view of the risk they may pose to the Data Subject.

Data relating to criminal convictions, offences or related security measures should not, in principle, be collected, except in very exceptional cases and with the approval of the DPO (e.g. collection of criminal records to verify information about a job applicant due to the specific nature of the job offer). In any event, this type of sensitive personal data may not be processed (thus, a copy of a criminal record, if it can be collected, may not be retained).

R12 The processing of sensitive data is prohibited in principle. Any exceptions must be made in accordance with the conditions required by applicable legislation and validated by the DPO.

4. Documentation and risk management

All evidence of regulatory compliance must be retained in order to demonstrate AFEJI Hauts-de-France's compliance to the supervisory authority.

4.1 Data protection by design and by default ("*Privacy by Design/by default*")

For any new project involving the processing of personal data, AFEJI Hauts-de-France implements measures to protect personal data from the moment the processing is designed, but also throughout the project and the life cycle of the personal data (from collection to destruction).

To this end, any AFEJI Hauts-de-France employee managing a project must follow the following steps:

Step 1. Verify that the principles defined in Section 3 of this Policy are being followed. Step 2. List the existing and planned technical and organisational measures to ensure the security, integrity and confidentiality of Personal Data.
Step 3. Carry out the preliminary assessment for the Privacy Impact Assessment. Step 4. If necessary, carry out the Privacy Impact Assessment.
Step 5. Implement security measures appropriate to the level of risk.

The process to be followed is detailed in the AFEJI Hauts-de-France's "Privacy by design/by default procedure".

When the project involves entrusting all or part of the processing to a subcontractor, AFEJI Hauts-de-France ensures that the requirements of the "Management of third parties involved" section are met.

R13 All projects take into account the protection of personal data from the design stage and by default.

4.2 Privacy Impact Assessment (PIA)

When Processing is likely to result in a **high risk** to the rights and freedoms of Data Subjects, AFEJI Hauts-de-France carries out a **Privacy Impact Assessment** (PIA) on the Processing **prior to its implementation**.

AFEJI Hauts-de-France also ensures that a **prior assessment** is carried out for any new processing operation in order to determine the level of risk involved and, consequently, whether a PIA should be conducted. This prior assessment takes into account:

- The mandatory cases defined in the GDPR and by the supervisory authority;
- The criteria established by the European Data Protection Board;
- The exemptions provided for by the GDPR and the Supervisory Authority.

The DPIA must be **documented** and must, at a minimum:

- describe the nature, scope, context and purposes of the Processing;
- assess the necessity, proportionality and compliance measures;
- determine and assess the risks to individuals;
- determine any additional measures to mitigate these risks.

For more information: CNIL practical guide on DPIA

R14 The need to carry out a Privacy Impact Assessment is identified for each new project and a PIA is carried out if necessary, before the start of the Processing.

The PIA is an **ongoing process** and must be **reviewed regularly** to ensure that the level of **risk remains acceptable** throughout the life of the processing, as the environment, particularly the technical environment, will evolve, requiring the measures implemented to be adapted.

Similarly, if a processing operation does not initially require a DPIA but the processing operations evolve, a DPIA may need to be carried out at a later stage.

R15 The need to update an existing DPIA or to carry out a DPIA is taken into account for each major change in a Processing operation.

After approval by senior management, the DPO **consults the Supervisory Authority** if the DPIA indicates that the processing would result in a high risk to the rights and freedoms of data subjects, i.e. if the **residual risk is still high** once the risk remediation plan has been defined and implemented.

R16 When the DPIA shows that a high residual risk persists, the CNIL is consulted.

4.3 The Processing Register

As Data Controller, AFEJI Hauts-de-France maintains a **processing register** in accordance with the requirements of applicable legislation.

To this end, AFEJI Hauts-de-France determines the key players involved in maintaining and updating the register, as well as their roles and responsibilities.

R17 A register of processing operations carried out is kept up to date.

5. Staff training and awareness

AFEJI Hauts-de-France ensures that all its employees are **aware of the issue of** personal **data protection** and understand the intent and scope of applicable legislation as well as the risks of non-compliance.

Where possible, AFEJI Hauts-de-France also provides **specific training** for employees who are required to process personal data on a daily basis.

Employees are regularly informed and/or trained on legislative and case law developments in the field of personal data protection, as well as updates to applicable internal rules.

All new employees undergo appropriate awareness training/training tailored to their duties and level of knowledge.

R18 All employees are made aware of the principles and issues surrounding personal data protection. More in-depth training is provided to employees who handle personal data on a daily basis.

6. Relations with Data Subjects

AFEJI p is committed to ensuring that Data Subjects can **effectively** exercise their rights under applicable legislation. Applicable legislation grants Data Subjects the following rights:

- **Right to information**: the right to clear, accurate and complete information on the use of Personal Data by AFEJI Hauts-de-France.
- **Right of access**: the right to obtain a copy of the Personal Data that the Data Controller holds on the applicant.
- **Right to rectification**: the right to have Personal Data rectified if it is inaccurate or obsolete and/or to have it completed if it is incomplete.
- **Right to erasure/right to be forgotten**: the right, under certain conditions, to have Data erased or deleted, unless AFEJI Hauts-de-France has a legitimate interest in retaining it retain it.

- **Right to object**: the right to object to the processing of Personal Data by AFEJI Hauts-de-France for reasons relating to the specific situation of the applicant (subject to conditions).
- **Right to withdraw consent**: the right to withdraw consent at any time when processing is based on consent.
- **Right to restriction of processing**: the right, under certain conditions, to request that the processing of Personal Data be temporarily suspended.
- **Right to data portability**: the right to request that personal data be transmitted in a reusable format that allows it to be used in another database.
  .
- **Right not to be subject to automated decision-making**: the right for the applicant to refuse fully authorised decision-making and/or to exercise the additional safeguards offered in this regard.
- **Right to define post-mortem guidelines**: the right for the applicant to define guidelines regarding the fate of Personal Data after their death.

To this end, AFEJI Hauts-de-France defines and implements a **procedure for managing** individuals' **rights** in accordance with the requirements of the applicable legislation. This procedure establishes:

- The standards to be met to ensure transparent information for individuals;
- The legal requirements that must be complied with;
- The authorised means of submitting a request for each right, depending on the category of data subjects;
- The operational processes for handling these requests in accordance with the above requirements;
- The parties involved in these processes, their roles and responsibilities.

Requests submitted by Data Subjects in exercise of their rights are **recorded in a register** for compliance purposes. The aforementioned procedure for managing individuals' rights defines the content and methods of maintaining this register.

R19 A procedure for managing the rights of Data Subjects is established and applied, with eligible requests being recorded in a dedicated register.

7. Management of personal data breaches

In accordance with its security obligation, AFEJI Hauts-de-France defines, documents and implements a **process for detecting, qualifying and responding to** personal data **breaches**. The documented procedure must include:

- a risk assessment matrix for the rights and freedoms of Data Subjects, taking into account the criteria defined by the Supervisory Authority and the European Data Protection Board;
- a distribution of roles and responsibilities among all parties involved in the response plan, including those of AFEJI Hauts-de-France's Subcontractors;
- the conditions, procedures and deadlines for notifying a Data Breach to the competent Supervisory Authority and/or Data Subjects.

Adequate technical and organisational measures are implemented to detect, investigate and report personal data breaches. In addition, in order to better detect and manage breaches,

AFEJI Hauts-de-France employees are made aware of and trained in the procedure to follow in the event of a confirmed or suspected Breach.

R20 A procedure for managing personal data breaches is defined and implemented.

In addition, AFEJI Hauts-de-France keeps a register of personal data breaches for accountability purposes

accountability purposes, to record all breaches, whether notification is required or not.

R21 A register of breaches is kept up to date.

8. Management of third parties

In accordance with applicable legislation, AFEJI Hauts-de-France undertakes to select service providers who offer **sufficient guarantees** regarding the implementation of appropriate technical and organisational measures.

To this end, AFEJI Hauts-de-France checks **in advance the guarantees** provided by any prospective third-party service provider, in particular by means of questionnaires and/or analysis of documentation. This verification must enable **the assessment of the conditions under which the Processing is carried out by the service provider:** methods used to carry out the Processing operations entrusted to them, security and confidentiality of Personal Data, maturity of the third-party service provider on the issue of Personal Data protection.

R22 A check of the guarantees offered by each third-party service provider is carried out prior to the implementation of Processing activities.
implementation of Processing activities.

AFEJI Hauts-de-France ensures that the third party involved is **properly qualified** (separate Data Controller, joint controller or Data Processor) and ensures that a **written contract clearly defines the roles and responsibilities** of each party. This contract includes at least the clauses required by applicable legislation (in particular the GDPR).

When the third party acts as a Subcontractor, the signed contract details the Processing entrusted to the Subcontractor by determining:

- the purpose and duration of the Processing;
- the nature and purpose of the Processing;
- the category or categories of personal data;
- the category or categories of Data Subjects;
- instructions relating to Processing operations.

R23 A written contract is signed with each third party involved in Data Processing. This agreement includes appropriate contractual clauses, in accordance with applicable Legislation.

Subcontractors are **audited regularly** to verify their ongoing compliance with contractual and regulatory obligations, at intervals and in accordance with procedures defined on the basis of the nature and sensitivity of the Processing operations entrusted to them, the necessary costs and the available resources.

R24 Processors are audited regularly to verify their ongoing compliance with contractual and regulatory obligations.

9. Relations with the Supervisory Authority

AFEJI Hauts-de-France cooperates **fully with any supervisory authority** when required and provides all evidence of its compliance with applicable legislation.

The Data Protection Officer of AFEJI Hauts-de-France acts **as the point of contact** for the supervisory authority and, in this capacity, is responsible for:

- Consultation with the relevant supervisory authority in cases where the processing of personal data involves a high residual risk to privacy;
- Reporting a Data Breach to the Supervisory Authority when required;
- Processing all requests (such as requests for access to processing records, requests for information, etc.).

AFEJI Hauts-de-France has defined a **procedure in the event of an audit** by a supervisory authority, which sets out the roles and responsibilities of key players in the context of these controls.

R25 AFEJI Hauts-de-France cooperates with the competent supervisory authority and defines a procedure in the event of an inspection.

10. Compliance monitoring

AFEJI Hauts-de-France guarantees compliance with this General Personal Data Protection Policy as well as with the implementation procedures and additional policies relating to the protection of Personal Data.

To this end, an **annual compliance audit** is carried out to **verify compliance with the rules** laid down and the **consistency of the processing activities** carried out with the processing register. This control mechanism is overseen by the DPO and the COPIL.

When breaches are identified, a **remediation plan** is defined by the DPO and all relevant stakeholders in order to remedy the deficiencies detected, taking into account the risks involved, the costs of implementation, existing and foreseeable operational constraints, and available human resources. The corrective measures in the remediation plan are implemented **without undue delay** by the stakeholders concerned, under the supervision of the DPO.

R26 A compliance monitoring system is put in place.

R27 A remediation plan is defined and implemented to correct any detected non-compliance.

11. Commitments of AFEJI Hauts-de-France as a Subcontractor

11.1 The Subcontractor Processing Register

In accordance with applicable legislation, AFEJI Hauts-de-France undertakes to maintain a **register of processing activities carried out on behalf of third-party data controllers**. This register must contain the following information:

- The name and contact details of the Sub-processor, as well as the Data Controller on whose behalf it processes Personal Data, and the contact details of the DPO;
- The category or categories of processing carried out on behalf of each data controller;

- Where applicable, transfers of personal data to a third country or international organisation, as well as documents certifying the existence of appropriate safeguards;
- A general description of the technical and organisational security measures implemented

.

This Processing Register must be updated as necessary to ensure that it is **accurate and comprehensive**.

R28 A register of processing activities carried out as a processor is kept up to date.

11.2 Additional obligations of AFEJI Hauts-de-France as a Processor

As part of its activities, AFEJI Hauts-de-France acts as a Sub-processor for third-party Data Controllers. As such, AFEJI Hauts-de-France has **specific obligations** under which it must ensure that:

- **Maintain a record of processing activities** carried out on behalf of and for the account of of the Data Controllers (see previous section);
- **Act within the framework of the lawful instructions** of the Data Controller;
- **Establish a contract** with the Data Controller in accordance with the provisions of the applicable legislation;
- **Ensure the application of the principles of personal data protection from the design stage and by default**;
- Subject employees responsible for processing activities to a **confidentiality obligation**;
- Comply with **contractual obligations** regarding the recruitment of a **subsequent subcontractor;**
- Incorporate into the data breach management procedure the necessary measures to **notify any Data Breach to the** relevant Data **Controller(**s);
- Take **appropriate technical and organisational measures to ensure a level of security appropriate to the risks**;
- On the instructions of the Data Controller, **delete or return all of** the Data Controller's Personal **Data**, unless there is a legal obligation to retain it (non-personal data attesting to the proper performance of services may be retained for the duration of the limitation period for commercial actions);
- **Assist, alert and advise** the Data Controller by:
  - Informing them when an instruction is likely to constitute a breach of the Applicable legislation;
  - Assist the Data Controller in responding to requests from Data Subjects (financial compensation may be requested from the Data Controller);
  - Provide the information at its disposal to enable the Data Controller to conduct a Privacy Impact Assessment and comply with its obligations regarding managing Data Breaches (financial compensation may be requested from the Data Controller);
- Provide the Data Controller with **evidence of its compliance** and **allow audits to be carried out** (under the terms and conditions set out in the Contract).

R29 Additional obligations as a Subcontractor are implemented.

Appendix 1 Definitions

Data Protection Impact Assessment (DPIA): assessment to be carried out by AFEJI Hauts-de-France for processing operations likely to result in a high risk to the rights and freedoms of natural persons.

Supervisory authority: an independent public authority established by a Member State pursuant to Article 51 of the GDPR, responsible for monitoring the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data and to facilitate the free flow of personal data within the European Union.

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Protection Officer (or "DPO"): the person appointed by AFEJI Hauts-de-France to be responsible for the protection of Personal Data within AFEJI Hauts-de-France and for AFEJI Hauts-de-France's compliance with the applicable Legislation.

Recipient: natural or legal person, public authority, service or any other body that receives communication of Personal Data, whether or not it is a Third Party.

Personal data: any information relating to a data subject, in particular by reference to an identifier such as a name, identification number, identity card number, salary, health records, bank account information, driving or consumption habits, location data, online identifier, etc. The term "Personal Data" includes Sensitive Personal Data.

Sensitive personal data/Sensitive personal information: refers to Personal Data revealing or based on:

- Racial or ethnic origin, political, religious or philosophical opinions
- Membership of a trade union
- Physical or mental health
- Sexual orientation or sex life
- Genetic and biometric data
- Data relating to criminal convictions, offences or related security measures.

Applicable legislation: set of regulations relating to the protection of personal data and applicable to the processing of personal data carried out by AFEJI Hauts-de-France, namely European Regulation No. 2016/679 on the protection of personal data (GDPR), the amended French Data Protection Act, and any other related regulations applicable to AFEJI Hauts-de-France.

Data subject: an individual to whom the Personal Data relates and who can be identified or identifiable, directly or indirectly, through this Personal Data. This includes customers, prospects, and former and current employees.

Data controller: natural or legal person who, individually or jointly, decides what personal data is collected, why and how it is collected and processed.

GDPR: abbreviation for European Regulation No. 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Processor: any natural or legal person, public authority, agency or other body that processes Personal Data on behalf of the Data Controller and in accordance with its instructions (e.g. service providers or suppliers).

Third party: any natural or legal person, public authority, agency or other body other than the Data Subject, the Data Controller, the Data Processor and persons who, under the direct authority of the Data Controller or Data Processor, are empowered or authorised to process the Data.

Processing: any operation or set of operations performed or not performed using automated processes and applied to Personal Data such as collection, access, recording, copying, transfer, storage, cross-referencing, modification, structuring, provision, communication, recording, destruction, whether automatic, semi-automatic or otherwise. This list is not exhaustive.

Data Transfer: any communication, copying or movement of Data via a network, or any communication, copying or movement of such Data from one medium to another, regardless of the medium, of Personal Data to a third country outside the European Union or to an international organisation which processes or is intended to process such Data after the transfer.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal Data transmitted, stored or otherwise processed.

Procedure for reporting personal data breaches

Effective date	September
Author	DPO Consulting
Issuing department	AFEJI Hauts-de-France – General Management
Validator	DPO Consulting

Distribution		
☐ Confidential	☐Internal	☐Public

Update tracking				
Date	Reference	Author	Subject	Status
12/04/2022	V1	DPO Consulting	Procedure	In progress
27/06/2022	V2	DPO Consulting	Procedure	Completed

Reference documents
Identify here the documents referred to in the deliverable

Table of contents

1. Purpose of the procedure

The purpose of this document is to enable all employees (including permanent and temporary staff) and subcontractors to analyse the impact of personal data breaches and to describe the action plan to be implemented when a security breach occurs within the AFEJI Hauts-de-France information system.

It also specifies the situations in which AFEJI Hauts-de-France must notify the supervisory authority (CNIL) of any breach that may pose a high risk to the rights and freedoms of the individuals concerned within 72 hours of becoming aware of the incident.

2. What is a personal data breach?

2.1 Definitions

A security incident (hereinafter an "Incident") is an event, potential or actual, that compromises or is likely to compromise the availability, confidentiality or integrity of the AFEJI Hauts-de-France information system.

A data breach (hereinafter referred to as a "Breach") refers to an Incident resulting, accidentally or unlawfully, in the destruction, loss, alteration, unauthorised disclosure of personal data transmitted, stored or otherwise processed, or unauthorised access to such data.

As a reminder, personal data means any information that directly or indirectly identifies an individual. For more information, please refer to the AFEJI Hauts-de-France General Personal Data Protection Policy.

2.2 The different types of data breaches and the associated risks

There are different types of personal data breaches (this list is not exhaustive):

- Breach of confidentiality: an incident resulting in unauthorised access to or disclosure of personal data.
- Integrity breach: an incident resulting in an undesirable change to personal data, which may cause errors or malfunctions in the processing concerned.
- Availability breach: an incident resulting in the loss or unavailability, even momentary, of personal data. This Breach does not apply to planned periods of unavailability, such as scheduled maintenance of an application or system, etc.

The classification of the breach will be recorded in the breach register (see step 5) and is information that is communicated, where applicable, when the breach is notified to the CNIL and/or to the persons affected.

2.3 The difference between a potential data breach and an actual data breach

A distinction can be made between a potential data breach and an actual data breach.

Potential data breaches may include:

- The loss or theft of portable devices or equipment containing personal data (PCs, USB keys, mobile phones, discs, etc.);
- The loss or theft of paper files containing personal data;
- Unauthorised access to a computer;
- A breach in physical security;
- Unsafe or unauthorised destruction of confidential documents;
- Leaving computer equipment unattended when connected to a user account without locking it.

These breaches are considered data privacy violations as long as there is no way to verify that the data has been accessed by an unauthorised third party. However, if it turns out that this personal data has been compromised in any way, then the data breach becomes real.

Actual data breaches can include:

- The disclosure of confidential data by unauthorised persons;
- Controls access controls inappropriate inappropriate enabling the use unauthorised information;
- The alteration or deletion of files containing personal data;
- A virus or other cyberattack on computer equipment or networks when it affects personal data;
- The publication of confidential data on the Internet by mistake and accidental disclosure of passwords;

3. How to manage a security breach within AFEJI Hauts-de-France?

When a security incident is suspected or occurs, AFEJI Hauts-de-France has defined a series of actions to be implemented within a short timeframe (details below).

All employees, interns or third parties of AFEJI Hauts-de-France must report any security breaches that occur. A preliminary analysis will be carried out to detect whether the incident has affected personal data. If this is the case, a risk assessment must be carried out to determine whether the level of risk justifies notification to the supervisory authority.

Step 0: A security incident occurs

A security incident occurs within the AFEJI Hauts-de-France information system and is discovered by an employee, the IT department or someone outside AFEJI Hauts-de-France.

Step 1: Reporting the security incident to the COPIL

Anyone who discovers a security incident must immediately alert the persons in charge of personal data breaches:

- The IT department:serviceinformatique@afeji.org - Head Office telephone number: 03.28.58.99.10;
- The Data Protection Officer by email: dpo@afeji.org

The incident management team is composed of:

- The Information Systems Manager
- The Data Protection Officer
- A member of management whose data was affected by the security incident.

Their role is to assess the damage to personal data caused by the security breach. The DPO will write a report containing all the details of the security breach and the corrective actions taken. It will be documented in the security breach register.

Step 2: Identifying contributors to the investigation

Once alerted, the COPIL must identify the AFEJI Hauts-de-France departments to be involved in the investigation of the Incident, according to their roles within the company.

At the end of the investigation, it is possible that people outside AFEJI Hauts-de-France may be involved in the investigation if the security breach originates from their information system. These external parties may be customers, service providers, subcontractors or suppliers.

The individuals who will contribute to the investigation into the security incident are identified according to two criteria:

- The location where the Incident occurred
- The person(s) who may have played a role in the Incident.

Thus, if the security incident occurred in a supplier's information system and affected the personal data of individuals concerned at AFEJI Hauts-de-France, the supplier will be directly involved in resolving the incident.

If the security incident occurs within the AFEJI Hauts-de-France information system, the relevant internal departments of AFEJI Hauts-de-France and/or the external service provider may be involved in resolving the incident.

Step 3: Preliminary analysis of the Incident

This step consists of determining whether the detected Incident constitutes a Data Breach within the meaning of the applicable regulations.

To this end, the members of the COPIL, accompanied by the DPO and, where applicable, the identified contributors, must carry out a preliminary analysis of the Incident in order to verify whether or not personal data has been affected:

- If the incident does not affect personal data, then it is not a data breach. In this case, the incident will be handled in accordance with the usual IT incident management procedures established by AFEJI Hauts-de-France. It is therefore not necessary to continue with this procedure.

- If the security breach affects personal data, it is considered a Data Breach as defined in paragraph 2. In this case, the steps described below must be followed appropriately.

Step 4: Control and monitoring

Steps 4 and 4a must be handled in parallel.

When a personal data breach is established and has affected personal data, those responsible for incidents must define an action plan. They must inform the DPO of the action plan put in place. The DPO must then monitor this action plan.

Those responsible for incident management must work together to:

- Isolate the incident (e.g. quarantine affected devices, suspend the affected email accounts);
- Take appropriate measures to recover any losses and mitigate risks (retrieve equipment, change access codes);
- Recover or restore affected data;
- Recommend specific actions to stakeholders to mitigate the consequences of the breach. Stakeholders will confirm whether or not they intend to implement the recommended actions.

Step 4a: Risk assessment

This involves assessing the severity of the breach.

When assessing the risk resulting from a data breach, the DPO must take into account the nature and scope of the personal data involved, as well as the nature and scope of the individuals concerned and the potential harm suffered by them.

Particular attention should be paid to the following points:

- The type of data involved, its sensitivity, how it is protected (e.g. encryption) and the likelihood that individuals could be re-identified using this data;
- The cause of the breach;
- The number and categories of individuals affected;
- Risks to individuals:
  - What are the potential negative consequences for individuals?
  - How serious or significant are these consequences?
  - To what extent are they likely to materialise?
- Risks to AFEJI Hauts-de-France:
  - Strategic and operational
  - Compliance/legal
  - Financial
  - Reputation
- The ability (or inability) of unauthorised persons to re-identify individuals;
- Whether the person had an obligation to treat the data confidentially;
- If the personal data was actually acquired or viewed.

A risk assessment matrix is provided in the appendix to paragraph 4.3 of this procedure.

The risk analysis must lead to a result that determines whether the breach should be reported internally (Step 6) or whether it should be reported to the CNIL and the individuals concerned (Step 7).

Step 5: Result of the personal data breach

Following a personal data breach, the DPO must take certain actions.

Firstly, they must keep a register of personal data breaches, in which they record and summarise all breaches that have occurred within AFEJI Hauts-de-France.

Once the results are in, the DPO also issues recommendations for managing the ongoing personal data breach. The crisis unit meets and decides whether to follow the recommendations made by the DPO.

If the DPO's recommendations are not followed, they must be informed. The reasons for this decision must also be communicated to them and documented.

If the risk assessment establishes that there is no risk to the individuals concerned, the DPO will not have to notify the data protection authority. However, they must

record the breach in the personal data breach register, in mentioning that it is a potential data breach.

Following the outcome of the security breach, the DPO must be able to determine whether the personal data breach should be notified internally (Step 6), to the competent data protection authority (Step 7), or to the data subjects (Step 7).

Step 6: Internal notification of the security breach

In the event of a personal data breach, the DPO must draft a document describing the incident and send it as soon as possible to the following recipients:

- Senior management
- The IT service provider of AFEJI Hauts-de-France / the IT department of AFEJI Hauts-de-France

This document must include the following information:

- A description of the incident
- The potential impact on AFEJI Hauts-de-France
- Corrective measures taken to prevent further incidents
- Recommendations for future actions
- Whether or not external notification is required.

Step 7: External notification of the security breach

- Notification to the supervisory authority

Notification to the CNIL is required when the personal data breach poses risks to the rights and freedoms of the individuals concerned.

This notification must be made as soon as possible, and no later than 72 hours after the data controller becomes aware of the breach.
If this deadline is not met, the notification must be accompanied by proof of the delay.

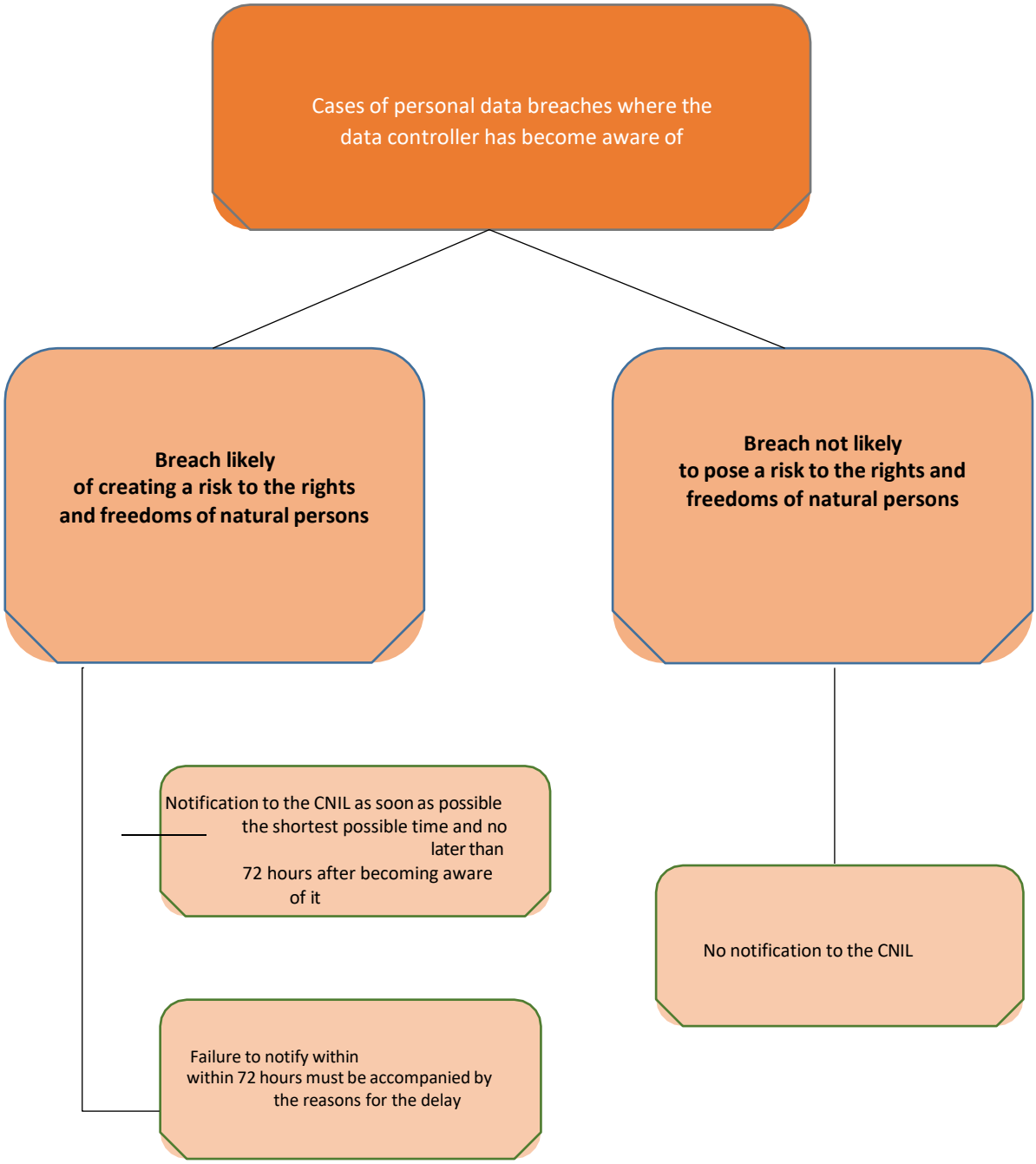
The notification is made by online via the secure secure of the CNIL: https://notifications.cnil.fr/notifications/index.

The notification must contain the following information:

- The nature of the breach;
- The categories and approximate number of individuals affected;
- The categories and approximate number of files affected;
- The likely consequences of the breach;
- The contact details of the DPO;
- Measures taken to remedy the breach and, where applicable, to limit the negative consequences of the breach.

If AFEJI Hauts-de-France does not have all of this information, an initial statement must be made. The remaining information must then be provided as soon as possible.

Notification procedure to the CNIL



- Notification to the persons concerned

Notification to data subjects is only mandatory when the personal data breach is likely to result in a high risk to their rights and freedoms.
personal data is likely to result in a **high** risk to their rights and freedoms. Notification to data subjects must be

provided as soon as possible.

The notification to data subjects contains the same information as the notification
to the supervisory authority (see above: *Notification to the supervisory authority*).

In the following cases, AFEJI Hauts-de-France is exempt from notifying data subjects:

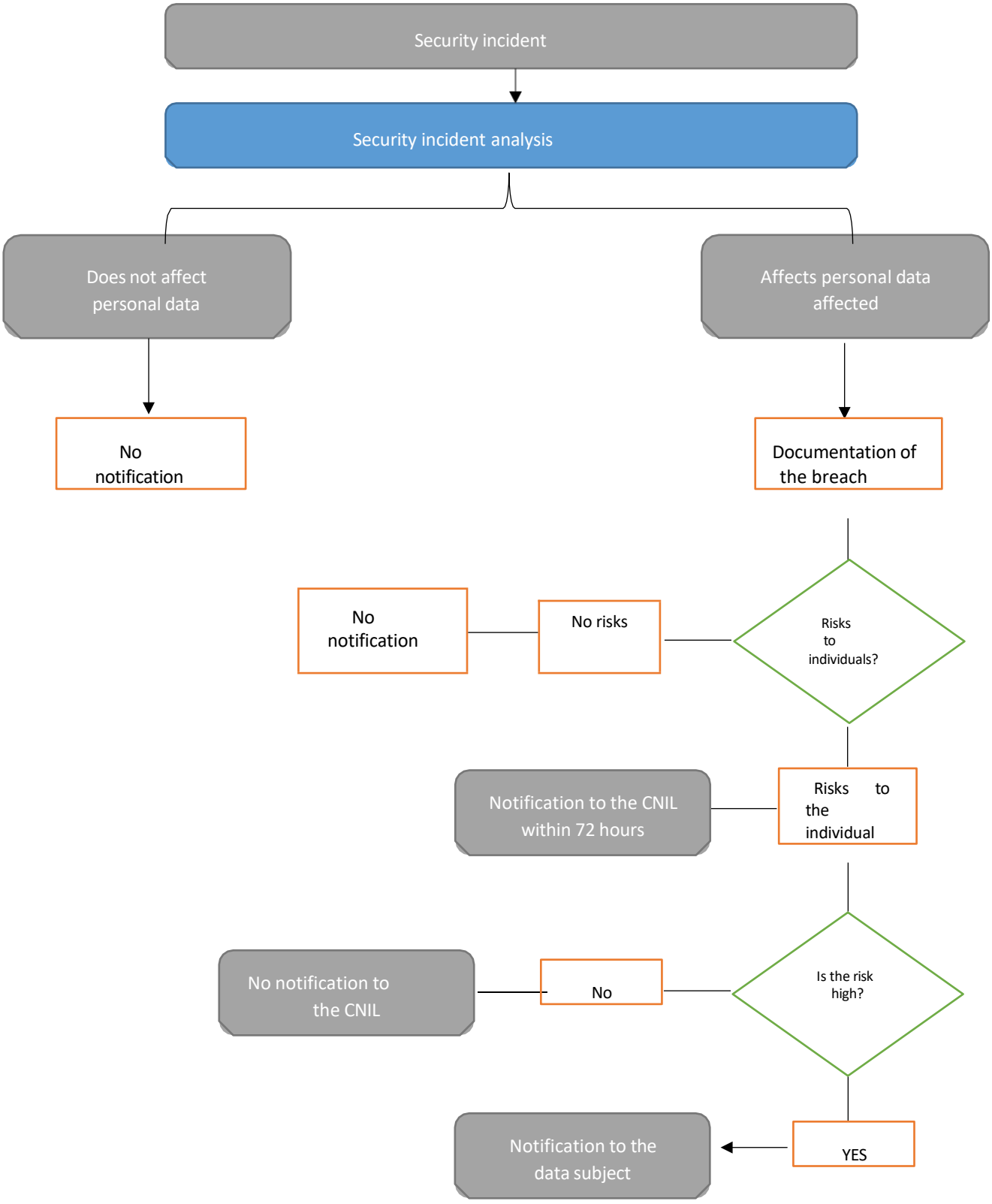
- The data affected is protected by security measures (such as encryption) that render it incomprehensible to persons who are not authorised to access it.
- Notifying the individuals concerned would require disproportionate effort. This is particularly the case where AFEJI Hauts-de-France does not have the information it needs to contact the individuals concerned. In this case, however, AFEJI Hauts-de-France is required to issue a public statement so that the individuals concerned can be informed.

The CNIL may reassess the severity of the risk and ask AFEJI Hauts-de-France to notify
notify the individuals concerned.

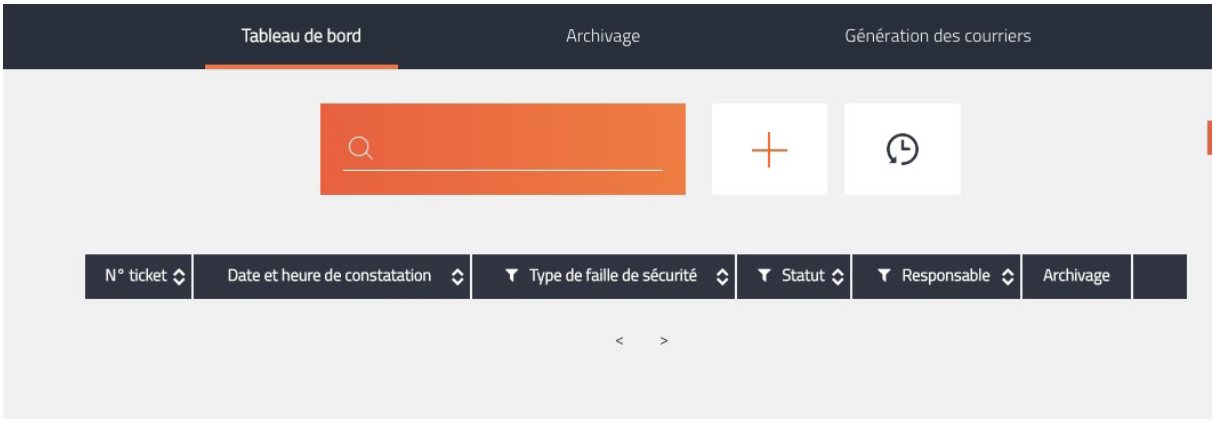
4. Appendices

4.1 Flowchart on the procedure for notifying the supervisory authority and the persons concerned concerned

Security incident management procedure



4.2 Personal data breach register template



4.3 Risk analysis of the breach to determine whether notification is required

The risk materialises when the breach could cause physical, moral or material damage to the individuals whose data is affected. Examples include discrimination, identity theft, fraud, financial loss or damage to reputation.

When the breach involves data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health data, data concerning sex life, offences or convictions, the impact on the data subjects is considered to be significant.

1. Level of impact

All personal data affected by the breach must be classified according to the following table. This classification is divided into three levels:

- Physical impact: What is the potential physical impact on the data subject in the event of a breach of their personal data? For example, if data relating to the person's age has been stolen, the person will not be physically affected. However, they will be affected if the stolen data is medical data.
- Moral impact: What is the potential moral impact on the person concerned in the event of a breach of their personal data? For example, if the family situation of an employee going through a divorce is revealed, this could affect their relationships with their colleagues.
- Material impact: What is the potential material/financial impact on the individual concerned in the event of a breach of their personal data? For example, if the If salary-related data is changed, the person concerned may not receive their usual amount.

It should be noted that this analysis takes into account the type of data breach: modification, loss or unauthorised disclosure. The same data can have different impacts depending on whether it is modified, lost or disclosed to the public. For example, the disclosure of a payslip will have a moral impact on the person concerned, but there will only be a material impact when this data is lost or modified.

	Level of impact on the individuals concerned				
	Level of risk	Description	Impact physical	Moral impact	Impact material/financial
1	Negligible	Those affected are not impacted or experience minor inconveniences that are easily overcomeable	Frustration	Frustration	Spam, wasted time, small unexpected payment
2	Limited	Those affected experience significant inconvenience, which they can overcome with some difficulties	Minor physical ailment or medical treatment	Temporary disorders, feeling of invasion of privacy	Financial loss, missed promotion, frozen accounts
3	Significant	Those affected could face significant consequences that they will find very difficulty overcoming	Serious physical condition	Damage to reputation, depression, serious psychological condition	Non-temporary financial difficulties, loss of employment or housing
4	Maximum	Those affected could face significant consequences that they may not be able to overcome. overcome	Long-term or permanent physical impairment, death	Permanent psychological condition, criminal punishment, loss of family ties	Financial hardship, inability to work or pay off debts

2. Number of people affected

Once the level of impact has been established with regard to modification, loss and disclosure, it will be necessary to determine and take into account the number of individuals affected whose data has been impacted by the breach.

	Number of individuals
A	More than 100,000 people affected
B	10,001 to 100,000 individuals affected
C	1,001 to 10,000 people affected
D	0 to 1,000 people affected

3. Initial analysis

After determining the two levels above, it is possible to deduce the following risk level risk:

	M	I	L	H
A	4	4	3	3
B	4	4	2	2
C	4	3	2	1
D	4	3	1	1

Meaning:

		Supervisory authority – CNIL	Data subjects
4	Maximum impact	Mandatory notification	Mandatory notification
3	Significant impact	Mandatory notification	Notification strongly recommended
2	Limited impact	Notification recommended	Notification recommended
1	Negligible impact	Notification not required	Notification not required

4. Aggravating and mitigating factors

Certain factors may impact the initial analysis, reducing or increasing the risk.
Aggravating factors:

➔ **The volume of compromised data (for the same person)**

The volume of data must be considered in terms of time and content. For example, in terms of time, if the credit card history of B2C customers of AFEJI Hauts-de-France customers has been disclosed, the impact of the breach would be even greater (for the same individual) if this data covers a period of one year rather than one week. In terms of content, if the customer file containing invoices, contracts and purchase orders had been disclosed, the impact of the breach would be even greater if the entire contents of the file had been revealed rather than a single document.

➔ **Characteristics related to the data controller**

The nature and role of the data controller and its activities could affect the level of risk resulting from a breach. For example, a data breach affecting a customer list would be riskier if the list belonged to a pharmacy rather than a stationery shop. In the case of AFEJI Hauts-de-France, a data breach will have more impact if it occurs on B2B or B2C customer data.

➔ **Characteristics related to the data subjects**

The level of impact on individuals will also depend on the category of people concerned. The consequences may be more serious if the compromised data belongs to a minor or other vulnerable persons. For example, a breach affecting a list of telephone numbers will be more serious if it concerns members of the AFEJI Hauts-de-France Management Committee rather than other employees.

Mitigating factors:

➔ **Invalid/inaccurate data**

The impact of a breach of certain personal data may be reduced if the data controller is aware that the data is invalid or inaccurate (e.g. data that has not been updated or contains errors). For example, a breach of archived data belonging to former AFEJI Hauts-de-France customers who probably no longer have the same address or telephone number would not pose a risk to individuals.

➔ **Unintelligible data**

Unintelligible data (e.g. due to enhanced encryption with a secure key) can significantly reduce the impact on individuals, as it reduces the possibility for third parties to access the data and cross-reference it with other information in order to identify the individuals concerned.

➔ **Public availability**

The impact of a breach may also be reduced if the affected data was already publicly available prior to the breach, or if it can be easily retrieved from publicly available sources.

➔ **Nature of personal data**

The nature of the data can sometimes play a mitigating role. This is the case for data that is sensitive in nature, but whose breach would not be as serious because of the information it reveals about the individual. For example, a medical certificate that simply certifies that the individual is in good health and does not reveal any other medical information. In this case, although the breach concerns health data, its impact would be limited as it does not pose a risk to the individual concerned

Ensure the implementation of a system for managing adverse events, whether minor (Adverse Event - AE) or serious (Serious Adverse Event - SAE), within AFEJI Hauts-de-France establishments.

Ensure that information is reported and escalated within the institution when an adverse event (AE or SER) occurs.
Define the procedures for internal handling of adverse events (AE or AIE) occurring within the establishment.
Ensure the traceability of the handling of adverse events (AE or AIE) within the establishment itself.
Ensure feedback to stakeholders (including the reporting party) regarding the treatment provided.
In the case of EIG, define the procedures for reporting information within the Association and to the Pricing and Control Authorities (and other third parties), as well as the procedures for processing and analysis.

The purpose of the AE and SAE reporting process is not to establish possible fault, but to analyse the causes of the events and to make recommendations to prevent them from happening again.

This guidance note applies to all AFEJI Hauts-de-France establishments.

Reference documents

- Articles L.331-8-1, P-331-8 to -10 of the Social Action and Families Code, relating to the obligation to report serious malfunctions and events impacting or threatening the safety and health of persons receiving care,
- Articles P.1413-ó7 Ò P.14l 3-73 relating to the reporting of serious adverse events associated with care,
- Article P22ó-2-2 of the CASF: Information of concern,
- Articles Ll 4l 3-14, Pl 413-ó7 ò 70 of the Public Health Code: Reporting of serious adverse events associated with healthcare,
- High Authority for Health, Manual for assessing the quality of social and medico-social establishments and services, March 2022.

References specific to healthcare establishments

- Decree No. 2010-1408 of 12 November 2010 on the prevention of adverse events associated with healthcare in healthcare establishments,
- Decree 2010-1000 of 25 November 2010 on the reporting of serious adverse events associated with healthcare and regional structures supporting healthcare quality and patient safety,
- Decree No. 2017-415 of 27 March 2017 on the procedures for informing the users' committee about serious adverse events associated with healthcare,

- Haute Autorité de Santé (French National Authority for Health), Certification Manual for Healthcare Facilities for Quality of Care, Version 2023.

Related documents

Serious Adverse Event (SAE):

- Reporting forms for the Pricing and Control Authorities (ATC)
  (—— OëÖiës forms sent by the ATC: APS. DDETS. C:059 Autonomy Directorate. C:D59 DEFJ. DTPJJ. Ö to be used in accordance with their guidelines).

Adverse Event (AE):

- Adverse event reporting form template (AGEVAL and paper formats)
  (—— internal declaration to the institution),
- Standard template for reporting and handling adverse events (AGEVAL and paper formats),
- Template for recording adverse events (paper format — also available in AGEVAL format),
- Awareness-raising material for professionals in institutions: managing adverse events.

Adverse event (AE): A situation that deviates from procedures or expected results.
and which is or could potentially be a source of damage *(simple undesirable event).*

Serious adverse event (SAE): Any event falling under Article L.331-8-1 of the CASF and one of the 11 categories of events that must be reported to the administrative authorities (see list in Appendix 1 of the guidance note).

Serious adverse event associated with care (SAEC) An unexpected event in view of the person's state of health and pathology, the consequences of which are death, a life-threatening situation, or the probable occurrence of a permanent functional deficit, including a congenital anomaly or malformation.

AEI: Adverse Event Report.

Concerning information (CI) ' Information sent to the departmental unit to alert the president of the Departmental Council to the situation of a minor, whether or not receiving support, which may give rise to fears that their health, safety or morality are in danger or at risk of being so, or that the conditions of their education or physical, emotional, intellectual and social development are seriously compromised or at risk of being so (P22ó-2-2 of the CASF).

The purpose of this referral is to assess the situation of a minor and to determine the protective measures and assistance that this minor and their family may benefit from.

1. Preamble:

School principals (or their delegates) are responsible for ensuring the safety of property and persons welcomed and present in their establishments and are required to take all necessary measures to ensure this safety.

As such, the management function includes risk assessment and, consequently, the nature of those risks that must be reported (this may include, among other things, any information that must be brought to the attention of a third party (town hall, ALS, gendarmerie, etc.)) in accordance with the regulatory framework and guidelines set by the administrative authorities.

As a reminder, certain incidents subject to additional regulated reporting requirements give rise to specific reporting (workplace accidents, health alerts, serious adverse events related to healthcare, notifiable diseases, etc.).

> In the event of an incident that could give rise to civil and/or criminal liability on the part of the association, one of its employees, a user or a third party, the director of the establishment (or his delegate) shall take all necessary protective measures and immediately inform the Chief Executive Officer or his representative. In this context, any external communication must first be approved by the Chief Executive Officer or his representative.

Reminder: The distinction between an incident and an undesirable event (separate entrance and separate circuit):

Example: Cost of children cared for in MECS

- *Incident reports are sent to or refer to ASE. i esponsoöle Or child services and concern the individual situation of the child. The reports sent are detailed and circumstantial. They contribute to decision-making regarding the evolution of the child's individual situation.*
- *Forms relating to undesirable events should be sent to the DEFJ establishments department at the generic email address Oêdiêe."*

2. The management of undesirable events (EIGJ) requires the director of the establishment to make an external declaration to the AFEJI Hauts-de-France.

2.1. External reporting:

Depending on the type of EIG *(see list of reportable events in Appendix I — page II)*

- This is carried out systematically with the Pricing and Control Authorities (APS, Departmental Council, .)
    - Using the dedicated declaration form,
    - By email (see email address indicated on the dedicated declaration form and list of ATC contact details appended on pages 14 and 15 of the note),
    - With information from the Regional Director (in the absence of a response from the latter First level: contact the association's on-call number 03 28 59 99 25}.
    - It is essential to comply with the reporting deadline specified by the relevant ATC (—— within 48 hours). At the same time, it is essential to ensure that the events are accurate and complete before reporting them.

- If necessary
    - Report to the public prosecutor (if you believe there is a danger or risk of danger to the person).
        - Any report made to the Public Prosecutor must first be brought to the attention of the Regional Director: The head of the institution may request a meeting with the Regional Director in this context if necessary
        - The report will be made by the prison governor
    - Filing a complaint with the gendarmerie or police (e.g. physical assault within the institution / malicious acts committed within the institution — theft, deliberate damage to premises, equipment or materials, etc.)
        - Any complaint filed on behalf of the establishment is subject to information from the director from Territory or prior notification: The director Establishments that may request an exchange with the director of territory within this framework if necessary
        - Complaints will be filed by the school principal
        - The establishment director or their representative may also be required to accompany a user/employee who wishes to file a complaint on their own behalf
    - Concerning information (CI)
        - Information of concern (IP) aimed at alerting the president of the Departmental Council to the situation of a minor, whether or not they are receiving support, which may give rise to fears for their health,
          If a child's safety or morality is in danger or at risk, or if the conditions of their education or physical, emotional, intellectual and social development are seriously compromised or at risk, this must be reported by letter on headed paper.

- All reports are subject to prior notification to the Territory Director of the establishment may request an exchange with the regional director in this context if necessary The director

2.2. Principles to be observed in the context of the external declaration of an EIG

- Prior to making the declaration:
  - The school principal informs the regional director by telephone and/or email of the nature of the EIG and the measures taken or still to be taken, as well as the report he will make to the ATC.
  - The establishment director shall request the support functions required to deal with the EIG. Requirements

- Report to be made
  - The establishment director shall request assistance from the Quality & Evaluation Department (quality director and/or quality manager for the sector) if assistance is required in formalising the report.
  - The school principal sends the completed declaration form to the ATCs by email. He informs the members of the COMSTPAT by copying them into this email via the generic email address "Incident reports" incidentÀafeii.org
  - As a reminder, the declaration to the ATC must include the following information in the relevant sections of the form
    - A detailed description of the nature of the events and the circumstances in which they occurred chronology of events, roles of persons involved, etc.
    - A detailed description of the measures (emergency and post-emergency) taken or still to be taken to deal with the incident and the follow-up to be given to it. current situation,
    - A detailed description of the measures taken by the head teacher (or their representative) to inform the relevant parties about the event: quality of the parties involved, methods of communication used,
    - All the information mentioned in the report and in the body of the email must guarantee the anonymity of all those involved.

- Following the declaration:
  - The school principal's will monitor the handling of the EIG and inform the ATCs or others,
  - A crisis unit may be convened, either within the institution or elsewhere, to deal with adverse events identified as serious (AEs) — *if necessary, at the discretion of the institution director, the regional director or the quality director.*
  - The establishment director may be required to formalise a detailed report at the request of the regional director or any other member of the COMSTPAT DG.
  - IF NECESSARY, the regional director informs the COMSTPAT.
  - The facility director informs the CVS (CDU for the Château Maintenon Day Hospital) of the occurrence of a serious adverse event and the measures taken.

- IF NECESSARY, the school principal shall inform the local CSE, via the regional director, of the occurrence of a serious adverse event and the measures taken.
- IF NECESSARY, the establishment director shall inform the occupational physician of of the occurrence of a serious adverse event and the measures taken.
- IF NECESSARY, the ElG declared externally must be the subject of an insurance declaration by the establishment director to the establishment's insurance company.
- Experience review (Petex) IF NECESSARY, as part of the institution's quality assurance process, the institution's director shall organise a Petex {= *Debriefing/Analysis meeting with the EIG. in a multidisciplinary team. This will take place after the event, i n o r d e r t o identify the root causes a t the source of* the E/G *and any fundamental changes that may need to be implemented. This Petex must be the subject of a written report and contribute to the quality action plan in AGE\/AL.*
  With *the support of the Quality & Evaluation Department at the request of the Establishment Director, the Regional Director or the Quality Director.*
- At the association level, an annual review of EIGs reported to the ATCs will be carried out by the Quality Director for presentation to COMSTPAT.

2.3. Traceability of SER monitoring:

When the Serious Adverse Event concerns a person receiving support
The director of the establishment guarantees the traceability of the entire process of handling the situation, which is recorded in writing, at a minimum, in the file of the person accompanied who is affected by the adverse event, from the initial handling of the situation to the review of any consequences in terms of adjustments to the personalised plan for the person accompanied.

When the Serious Adverse Event concerns an employee/volunteer/intern
The director of the establishment shall ensure the traceability of the handling of any situation involving the responsibility of an employee/volunteer/intern of the establishment, which shall be recorded in writing, at a minimum, in the employee/volunteer/intern's file.

3. The reporting system in AFEJI Hauts-de-France establishments

The establishment director shall implement a system within the establishment to ensure the proper management of adverse events (whether considered simple or serious adverse events). *(See Haute Autorité de Santé. Manual for the evaluation of the quality of social and medico-social establishments and services. March 2022.*
"OBJECTIVE 3.73 — The ESSMS collects and processes data on incidents."

To do so, it can rely on the members of the Quality Monitoring Committee (COSUI) and the Establishment Quality Advisor, where applicable.

In this capacity, it defines and organises the process for reporting, processing, classifying/archiving, informing and analysing adverse events (AEs and SIs) in its establishment.

3.1. Reporting

Provide professionals with an adverse event reporting form.

- Option to use the FEI form in AGEVAL: online reporting
- *Or* Option to use the FEI PAPIE form

Special cases within nursing homes. Falls and worrying disappearances involving residents are recorded in the NETSoins computerised user file for follow-up care. In addition to completing an FEI.

3.2. Processing:

- Identify the person(s) responsible for receiving and processing FEIs (e.g. N+1? / On-call manager?).
- Establish EFFECTIVE traceability of the processing of the adverse event. For all Traceability, on the declaration form, of the immediate corrective actions taken,

3.3. The Classification

of FEI Cases under AGEVAL

- Save the processed FEI,
- Dashboard / Declaration Module.

Paper FEI cases

- Identify the person(s) responsible for classifying FEIs,
- Number and file the processed FEIs in a dedicated folder,
- Sign the adverse event recording table.

3.4. Information

- Ensure regular monitoring (weekly or fortnightly) of FEIs within the framework of the establishment's management committee, in order to ensure that they are handled correctly.
- Ensure that a sustainable organisation is put in place to systematise feedback, at a minimum to the reporting person and more broadly if necessary, concerning the handling of the reported situation. The traceability of this feedback will be ensured at a minimum on the FEI.

3.5. Analysis:

Ensure "statistical" monitoring of adverse events within the COSUI framework

- Use the adverse event recording table/dashboard on AGEVAL as a basis.
- Monitoring every six months if possible, or at least annually, with a view to preparing the annual activity report
- Adverse events can be analysed *based on their frequency or occurrence* (e.g. if an adverse event accounts for 80% of reports over a period, it would be appropriate to set up a working group to identify its root causes).
- "Examine" *the name Oe FEI* (e.g. in the event of a low or very low declaration, it will be appropriate to raise awareness among professionals again).
- The corrective actions to be taken, identified as part of the analysis of adverse event reports, are formalised in the Quality Action Plan (QAP).

- ☐ A procedure defining the reporting and handling process for adverse events implemented within the establishment is distributed and brought to the attention of the professionals working there
- ☐ An adverse event reporting form (paper or electronic)
- ☐ A system for recording and monitoring adverse events
- ☐ An annual review of adverse events in the activity report
- ☐ For establishments concerned by the implementation of a CVS/CDU
  - ☐ Information on the existence of the adverse event management system in place at the establishment
  - ☐ Systematic inclusion on the agenda of a presentation of adverse events reported during the quarter
  - ☐ Inclusion on the agenda at the end of the year of the annual review of adverse events
- ☐ A standardised form for reporting an EIG (see the dedicated ATC reporting form) — To be reported within 48 hours & Inform the General Management immediately
  - ☐ A ftETEX to be organised, if necessary, following the reporting of an EIG

The examples cited in the categories below are not exhaustive, but are intended to help the organisation identify malfunctions and events that must be reported to the competent administrative authorities.

1	Disasters and exceptional weather events exceptional	Floods, storms, fires, disruption to electricity or water supply, etc.
2	Accidents or incidents related to failures technical equipment failures at the facility Environmental health events	Prolonged power, heating, lift... Epidemics, poisoning; Legionnaires' disease, infectious diseases...
3'	Disruptions to work organisation and human resources management	Prolonged job vacancies, particularly management positions, recruitment difficulties, unexpected absences of several staff members, staff turnover, strikes, etc., making it difficult to provide effective care or ensure the safety of those receiving care
4º	Accidents or incidents related to an error or lack of care or supervision	Errors in the distribution of medication, inappropriate treatment, delay in care or treatment provided, etc.
5°	Situations disrupting the organisation or functioning of the facility due to recurring relationship difficulties with the family or relatives of a person in care, or due to other persons outside the organisation	Significant conflict over the care of a person, repeated threats, inappropriate demands, mistrust of staff, illegal activities, etc.
ò°	Accidental deaths or deaths resulting from a failure to supervision or care of a person	Following a fall, a restraint accident, etc.
7°	Suicides and attempted suicides, or within structures, persons under care or staff	
8'	Situations of abuse towards persons in care or under supervision	Physical, psychological or moral violence, sexual assault, serious neglect, deprivation of rights, theft, controlling behaviour, isolation from loved ones, failure to adapt equipment necessary for people with reduced mobility, etc.
9º	Disappearances of persons accommodated in accommodation or reception facilities, once the police or gendarmerie are alerted	Disappearance leading to the mobilisation of police or gendarmerie services to search for the person
10º	Violent behaviour on the part of users, ò towards other users or professionals, or within the facility Serious breaches of the rules of the accommodation or reception facility that compromise the care of these persons or that of other users	Aggression, threats, physical violence, sexual assault, etc. Failure to comply with the rules of community life, inappropriate or criminal practices or behaviour, etc.
11°	Acts of malice within the facility	Deliberate damage to premises, equipment or materials, theft...

Reports are made via the national reporting portal https://signalement.social-sante ciouv fr

Article Πl 4l 3-ó7 of the Public Health Code defines a serious adverse event associated with healthcare (SAEH) as "an unexpected event in view of the person's state of health and pathology, the consequences of which are death, a life-threatening situation, or the probable occurrence of a permanent functional deficit, including a congenital anomaly or malformation ."

Any adverse event associated with healthcare that meets at least one of the following criteria for seriousness must therefore be reported

- unexpected death in view of the patient's foreseeable condition,
- Life-threatening situation (e.g. unscheduled resuscitation, emergency surgery, etc.),
- Risk of permanent or potential sequelae related to the adverse event.

The report is made in two stages:

- A "section l" form, which must be submitted without delay and includes
  - The nature of the event and the circumstances surrounding its occurrence
  - A statement of the initial measures taken locally for the benefit of the patient and to preventing the recurrence of similar events
  - A mention of the information provided to the patient and, where appropriate, to their family, relatives close relatives or the person they have designated as their trusted representative

- A "section 2" to be sent within three months at the latest, containing
  - Description of event management
  - Feedback from an in-depth analysis of the causes of the event carried out by the healthcare professionals concerned (with the assistance of the regional support structure for healthcare quality and patient safety, where applicable)
  - A corrective action plan including implementation and evaluation deadlines

1. Principles of information reporting

The follow-up to an EIG report depends in particular on the quality of the facts gathered. It is therefore essential to be vigilant about the quality of the writing in this document.

The drafting of an EIG report is based on the following four principles

- *Objectivity:* The report is based on facts. It is not a matter of accusing individuals of being the perpetrators of acts, nor of interpreting the facts.
- *Anonymity and confidentiality*. The information collected is processed in a manner that respects the anonymity of the individuals receiving assistance and the staff, as well as the confidentiality of information relating to the event. Each professional undertakes to respect an obligation of discretion with regard to the information brought to their attention in the course of this process.
- *Effectiveness:* The reporting of information must strive to be as comprehensive as possible by identifying all the risks associated with the event or malfunction identified and preventing these risks from recurring.
- *Simplicity and clarity:* Prefer computerised writing (typed document) to handwritten documents.

2. Methodology for describing the facts

The aim is to provide as much information as possible and to present the facts, the place and date on which they occurred, and the consequences in as much detail as possible, without interpreting the facts.

The writer can use the 5W1H method (Who, What, Where, When, Why, How), a tool that can be adapted to various issues, to gather accurate and comprehensive information about a situation and assess the level of knowledge available.

3. Writing principles

The text will not necessarily relate everything that is known or everything that has been done. It should relate facts and objective elements, while supporting the assessment with well-founded arguments. This requires the use of logical connections, linear discourse without backtracking, and precise vocabulary.

It is advisable to use

- Direct style for observed elements and facts, with indication of places and dates where possible possible: *I observed...*
- Quotation marks for reported speech, using the exact words and expressions used by the person recounting the story, without rewriting them or putting them into correct language. *The child said* '...'
- Indirect style for stating information from informants: *the professional told me said that...*
- The conditional tense to express hypotheses: *the resident would have left the establishment around 10 p.m.*
- The indicative to express what has been seen, heard, understood: I *saw the person hurt themselves hurt themselves — I heard the person scream...*

Establishments and services under the jurisdiction of the A0S:

The local point is the single point of entry for user complaints, reports and alerts, and declarations of events with health and medico-social consequences in the Hauts-de-France region. It is available 24 hours a day, seven days a week, so that events posing a health risk can be reported and managed.

Regional Focal Point 55ó
avenue Willy Brandt 59777
Euralille
Tel : 03 62 72 77 77
Email: ars-hdf-siclnal@ars sante fr

Establishments and services under the jurisdiction of the DDETS du Nord:

Ms Sandrine PINOCHEAU - Yassine KPOUCHI — Complaints and Reports Unit
Tel : 03 20 18 34 72 / 0ó 08 25 ó3 03
Email: ddets-signal@nord.gouv.fr
Postal address: Direction Départementale de l'Emploi, du Travail et des Solidarités du Nord (Nord Departmental Directorate for Employment, Labour and Solidarity).
Cité Administrative. 175, rue Gustave Delory - B.P. 82008 - 59011 LILLE Cedex

INFORMATION from the DDETS: In accordance with Article P 331-8 of the CASF, the person in charge of the facility must submit the form within the specified time limit. If the DDETS has been notified in advance, the document may be submitted up to 48 hours later. Outside opening hours (after 6 p.m. and at weekends), the DDETS can be contacted by calling the switchboard of the Préfecture du Nord or 03 20 30 59 59.

The DDETS emphasises the importance of INFORMING the emergency services: they are often the first to respond to the most serious situations. It is essential that they are able to quickly contact the association on duty, whose contact details must be easily accessible (displayed in the accommodation, business cards, etc.).

In addition to sending the form dedicated to the DDETS (see above), in the context of particularly serious events (fire, homicide, media coverage, etc.), it is advisable to notify the relevant authorities. it is advisable to notify the

- DDETS representative — Avesnes-sur-Hêpes district Ms Déborah BPULANT (deborah brulantÂnord ciouv fr)
- DDETS representative — Lille and Dunkirk districts + Association Ms Martine BEAUMONT (martine beaumontÂnord ciouv fr)
- When the adverse event concerns a migrant user, inform the sub-prefecture and Mr Abdelkader HAPIZI (abdelkader.harizi@nord.nouv.fr)

Establishments and services under the jurisdiction of the Nord Departmental Council

Nord:

Mr President
NORTHERN DEPARTMENTAL COUNCIL
Hôtel du Département 51,
rue Gustave Delory 59047
LILLE Cedex

For establishments and services under the jurisdiction of the Departmental Council of Nord's *Directorate for Children, Families and Youth*, reports must be sent by email to the following address: defi-evenementindesirable@lenord.fr

For establishments and services under the jurisdiction of the Departmental Council of Nord's *Directorate for Autonomy (PH establishments, establishments for disabled persons, SAAD, intermediate services)*, reports must be sent by email to the following address: Infos-siclnalement-autonomie59@lenord fr

Establishments and services under the jurisdiction of the Northern Regional Directorate for Judicial Youth Protection:

DTPJJ
Address 194, rue Nationale - BP 1213 - 59013 Lille Cedex Tel. 03 20 57 5ó ó7
Fox ' 03 20 42 97 1ó

Adverse event forms (= Reported Incident Forms - FIS) to be sent to Email: dtoii-lille@justice.fr
Email - for on-call duty (Friday 8 p.m. to Monday 9 a.m.): on-call dutydtDÎÎ-lille@iustice.fr

In the event of an occurrence falling within one of the categories of events listed in Article L331-8-1 of the CASF.
categories of
events mentioned in Article L331-8-1 of the CASF.

Phase 1 - Event management: Provide initial emergency responses based on the situation

Immediately

Professionals present	☐ Assess the need for emergency services (fire brigade, ambulance, police) and call them if the situation requires it. ☐ Ensure that the incident does not cause a secondary accident (worsening of the situation). ☐ Take the necessary immediate measures to ensure continuity of support or care. ☐ Implement internal risk management procedures. ☐ Remove the victim(s) or alleged perpetrator(s) from the scene of the incident. ☐ Inform the school principal/duty manager/on-call manager as soon as possible, once everyone has been taken to safety and the emergency services or police have been called, if necessary. If the situation occurs in a group setting ☐ Supervise the rest of the group, keeping them away from the incident. ☐ Reassure as much as possible the other people in the group who have been directly confronted with the event. In the event of a reported absence or worrying disappearance} ☐ Search for and/or contact the places the person usually frequents (within and outside the facility) or their family members and/or friends. ☐ Question other people who were with them.

Director of Establishment / Duty Manager / Duty Manager	☐ Ensure that the usual preventive measures (as set out in the protocols) have been implemented. ☐ In the event of an emergency, go to the site. ☐ Assess the relevance of the initial actions taken and readjust them if necessary (adaptation of the environment, implementation of strategies, etc.). ☐ Determine the severity of the event or malfunction and whether the situation requires immediate intervention: relay within the team, reinforcement of personnel, recourse to law enforcement or emergency services. ☐ Support professionals in difficulty and encourage other professionals (not involved in the event) to take over. ☐ As soon as the situation allows, liaise with management on the joint steps to be taken by contacting - The site manager or the manager with delegated authority - And/or, if there is no response from the latter, the regional director territory If you do not receive a response from these first two levels, contact the association's on-call number: 03 28 59 99 25 The regional director or the association's on-call service will then also assess the need to provide initial information to the pricing and control authorities without delay. ☐ Forward the instructions agreed with senior management to the teams and monitor the implementation of these instructions. Additional specific provisions when the victim is a professional: ☐ Assess the need to end the professional's shift and arrange for a medical consultation or return home. ☐ Offer psychological support/counselling to the professional concerned. In the event of a runaway or worrying disappearance: ☐ Report any runaways or worrying disappearances no later than two hours after noticing their absence during the day, and within one hour during the night.

FORM FOR REPORTING INFORMATION RELATING TO EVENTS THAT THREATEN THE HEALTH, SAFETY OR WELL-BEING OF RESIDENTS

Ref: Decree No. 2016-1813 of 21 December 2016 on the reporting obligation of social and medico-social structures and Order of 28 December 2016 on the reporting obligation of social and medico-social structures

This form is intended to facilitate the exchange of information between the Department of the North and the medical and social establishments and services under the jurisdiction of the Department of the North. It must be sent to the following structural email address: defj-evenementindesirable@lenord.fr

Establishment, service, place of residence, reception centre
Date of report: Time of declaration:
Name of the facility:
Name of managing body: EPDSAE
Address of the organisation:
Telephone number:
Email:
Name and position of the declarant:
Administrative authority(ies) informed: ☐ ARS Notified on: ☐ Prefect informed on ☐ DDETS informed on: ☐ DTPJJ/DIRPJJ informed on:

Nature of the facts:

The examples cited in the categories below are not exhaustive, but are intended to help the organisation identify malfunctions and events that fall under Article L. 331-8-1 of the Social Action and Families Code.

1. **Disaster or weather event** *(e.g. flood, storm, fire, power or water supply failure, etc.)*	☐
2. **Accident or incident related to a technical failure** *(e.g. prolonged power cuts, heating failures, lift breakdowns, etc.)* **and environmental health events** *(e.g. epidemics, poisoning, Legionnaires' disease, infectious diseases, etc.)*	☐ ☐
3. **Disruption in work organisation and human resources management** *(e.g. prolonged vacancy of a position, particularly a management position, recruitment difficulties, unexpected absence of several staff members, staff turnover, strikes, etc., compromising the effectiveness of care or the safety of residents)*	☐
4. **Accident or incident related to an error or lack of care or supervision** *(e.g. errors in the distribution of medication, inappropriate treatment, delays in care or treatment, etc.)*	☐
5. **Disruption to the organisation or operation of the facility due to recurring relationship difficulties with a family or relatives or due to other persons outside the facility** *(e.g. serious conflict over the care of a person, repeated threats, inappropriate requests, mistrust of staff, illegal activities, etc.)*	☐

6. **Accidental death or death resulting from a failure to supervise or care for a person** *(e.g. following a fall, a restraint accident, etc.)*	☐ Accidental death ☐ Death resulting from a lack of supervision ☐ Death resulting from failure to provide care for a person
7. **Suicide or attempted suicide**	☐ Suicide ☐ Attempted suicide ☐ Suicidal remarks
8. **Abuse of users** *(e.g. physical, psychological or moral violence, sexual assault, serious neglect, deprivation of rights, theft, controlling behaviour, isolation from loved ones, failure to adapt facilities for people with reduced mobility, etc.)*	☐ Physical violence ☐ Sexual violence ☐ Psychological violence ☐ Domestic violence Serious ☐ neglect Harassment ☐ Acts of violence involving a professional from the facility
9. **Disturbing disappearance** *(disappearance requiring the police or gendarmerie to be called in to search for the person)*	☐ Running away ☐ Other: please specify
10. **Violent behaviour by users towards other users or staff within the facility** *(e.g. aggression, threats, physical violence, sexual assault, etc.)* **as well as serious breaches of the rules of conduct** *(e.g. failure to comply with community rules, inappropriate or criminal practices or behaviour, etc.)*	☐ Verbal violence by a young person towards a professional Physical ☐ violence by a young person towards a professional Verbal violence ☐ between young people ☐ Physical violence between young people ☐ Verbal violence by legal representative(s) towards a professional ☐ Physical violence by legal representative(s) towards a professional ☐ Serious breach of the rules of operation ☐ Other: please specify...
11. **Acts of malice within the facility** *(e.g. deliberate damage to premises, equipment or materials, theft, etc.)*	☐

Adverse event related to: *(see drop-down list)*

UI not related

Circumstances and sequence of events:

DATE OF THE ESTABLISHED FACTS	
TIME OF THE ESTABLISHED FACTS	

Territorial Directorate(s) responsible for the young person(s) concerned

Child victim of violence Y / N	Young person(s) concerned	Gender	Age	Relationship between victim and perpetrator	Youth welfare service responsible for the young person(s)	MNS (to be specified)	Date of information	Identity of the person informed
☐	☐							
☐	☐							
☐	☐							
☐	☐							
☐	☐							
☐	☐							
☐	☐							

Tick if perpetrator	Author of the facts	Gender	Age
☐			
☐			

When submitting the form to the administrative services, please ensure that the young people remain completely anonymous (no initials, use pseudonyms if necessary <u>and specify this explicitly</u>).

The facts:

Number of victims or exposed persons

NUMBER OF YOUNG PEOPLE WHO ARE VICTIMS OR EXPOSED TO INCIDENTS	

Were the victims or exposed persons informed of their right to file a complaint?

- ☐ **YES**
- ☐ **NO**
- ☐ **NOT RELEVANT TO THE FACTS**

Is support offered to victims and those exposed to violence to help them file a complaint?

- ☐ **YES**
- ☐ **NO**
- ☐ **NOT RELEVANT TO THE FACTS**

Consequences observed at the time the information was transmitted

For the person(s) receiving care *(e.g. death, hospitalisation, injury, deterioration in health, change in behaviour or mood, etc.)*	
For staff *(e.g. inability to come to work, sick leave, requisition, etc.)*	
For the organisation and operation of the facility *(e.g. supply difficulties, difficulty accessing the organisation or the place where the person is cared for, need to move residents, suspension of activity, etc.)*	

Request for emergency services

Fire brigade, ambulance service, police, gendarmerie, etc.

Yes (specify): No

Immediate measures taken by the organisation

- Fire brigade intervention Police
- intervention Call to the on-call
- manager
- On-call manager dispatched
- Refocusing meeting with the young person accompanied
- Hospitalisation of the young person accompanied
- Hospitalisation of the injured professional Complaint filed
- Activation of a crisis unit
- Sheltering in case of danger to buildings
- Isolation of the young person in a suitable or quiet space
- Reporting a runaway
- Other immediate measures

Informing the persons concerned, families and relatives

Subject to the consent of the person concerned, depending on the nature of the facts, were the families or relatives of the young people concerned informed of the situation by the organisation?

YES

NO

Date on which families/relatives were informed:

Measures taken by the organisation

Concerning users or residents *(e.g. adaptation of care or treatment, revision of the care plan, support, transfer, end of treatment, etc.)*	☐ Immediate withdrawal of visiting rights ☐ Support group for young people exposed to the situation ☐ Proposal for psychological counselling ☐ Request for referral of the young person(s) to another location ☐ Removal of the young person(s) in care for their safety ☐ Other corrective actions
Concerning staff *(e.g. training, awareness-raising, support, protective measures, disciplinary measures, etc.)*	☐ Proposal for employee counselling ☐ Implementation of awareness-raising/prevention measures ☐ Implementation of specific training programmes ☐ Disciplinary measures taken against the employee Other corrective actions ☐
Concerning the organisation of work *(e.g. revision of schedules, procedures, etc.)*	☐ Additional staffing (day/night) ☐ Replacement of broken equipment ☐ Reporting the incident to the public prosecutor ☐ Revision of procedures Other corrective actions ☐

Administrative or legal proceedings

ADMINISTRATIVE/LEGAL FOLLOW-UP	COURT(S) INVOLVED	SPECIFY DATE
ADMINISTRATIVE INVESTIGATION		
DISCIPLINARY PROCEDURE *(warning, suspension, dismissal, etc.)*		
POLICE INVESTIGATION		
FILING A COMPLAINT		
REPORT TO THE PUBLIC PROSECUTOR		

Foreseeable developments or expected difficulties

Media coverage

Can the malfunction or event referred to in Article L. 331-8-1 of the Social Action and Families Code have an impact on the media?	☐ Yes ☐ No
Have the media already been informed of these facts?	☐ Yes ☐ No
Has communication been made or is it planned? If yes, please specify:	☐ Yes ☐ No

Information provided to the CVS or discussion groups

Pursuant to Article R.331-10 of the Social Action and Families Code (**1**), have these items been communicated to the Social Life Council(s) of the establishment/service(s) or, failing that, to the existing discussion group(s):

☐ **Yes**

☐ **No**

☐ **Included on the agenda for the next CVS or next discussion group**

[1] **Article R.331-10 of the Social Action and Families Code**: "The social life council of the establishment, service, living space or reception centre concerned or, failing that, the discussion groups provided for in 1° of Article D. 311-21 shall be notified of any malfunctions and events mentioned in Article L. 331-8-1 that affect the organisation or functioning of the structure. The director of the establishment, service, living space or reception centre or, failing that, the person in charge of the structure shall inform these bodies of the nature of the malfunction or event and, where applicable, the measures taken or envisaged by the structure to remedy the situation and prevent it from recurring."

CERTIFICATE OF INFORMATION PROVIDED
ASSOCIATIVE GUIDANCE NOTE RELATING TO THE MANAGEMENT OF INDESII2ABLE EVENTS

I, the undersigned,

 Mrs. NAME Mr

SURNAME

Currently working at AFEJI Hauts-de-France as a

. ..... at the following establishment:

I hereby certify that I have received ..... all the information and instructions relating to the management of undesirable events within the establishments and services of AFEJI Hauts-de-France

- The association's guidance note " tendance of undesirable events".
- Standard templates for internal procedures for reporting and handling an adverse event (paper and Agéval format)
- The standard template for internal adverse event reports within the establishment.
- Serious Adverse Event (SAE) reporting forms from the various regulatory and pricing authorities: APS, DDETS, DEFJ Department
  DEFJ, Department of Adult and Juvenile Justice .
- The standard template for the adverse event recording table.
- Awareness-raising material on the management of adverse events.

Signature

Persons concerned by the signature Or document.

Director. Deputy Director. Document Ö to be signed and ö sent ö to your Management Oe Territory for inclusion Oons your employee file.
Please submit this document to your Director for inclusion in your employee file.

Charter of Rights and Freedoms of the Person Received

Article 1 Principle of non-discrimination

In accordance with the specific conditions of care and support provided for by law, no one may be discriminated against on the basis of their origin, in particular their ethnic or social origin, their physical appearance, their genetic characteristics, their sexual orientation, their disability, their age, their opinions and beliefs, in particular their political or religious beliefs, when receiving social or medico-social care or support.

Article 2 Right to appropriate care or support

The person must be offered care or support that is individualised and as appropriate as possible to their needs, in line with the continuity of care.

Article 3 Right to information

The person receiving benefits or services has the right to clear, understandable and appropriate information about the care and support requested or received, as well as about their rights and the organisation and functioning of the establishment, service or form of care or support. The person must also be informed about user associations working in the same field.

The person has access to information concerning them under the conditions provided for by law or regulations. The communication of this information or these documents by persons authorised to communicate them by law is carried out with appropriate psychological, medical, therapeutic or socio-educational support.

Article 4 Principle of free choice, informed consent and participation of the individual

In accordance with legal provisions, court decisions or judicial protection measures, as well as referral decisions:

1° The person has free choice between the appropriate services offered to them, either as part of a home care service, as part of their admission to an institution or service, or as part of any form of support or care:

2° The person's informed consent must be sought by informing them, by any means appropriate to their situation, of the conditions and consequences of the care and support and ensuring that they understand.

3° The right to participate directly, or with the help of their legal representative, in the design and implementation of the care and support plan concerning them is guaranteed.

When the person is unable to express a choice or informed consent due to their young age, this choice or consent shall be exercised by the family or legal representative with the establishment, service or other form of care and support. This choice or consent shall also be made by the legal representative when the person's condition does not allow them to exercise it directly. With regard to the care services provided by medical and social establishments or services, the person shall benefit from the conditions of expression and representation set out in the Public Health Code.

The person may be accompanied by a person of their choice during the procedures required for care or support.

Article 5 Right to renunciation

The person may at any time renounce in writing the services they receive or request a change in the conditions of capacity, listening and expression, and communication provided for in this charter, in accordance with court decisions or judicial protection measures, guidance decisions and existing review procedures in these areas.

Article 6 Right to respect for family ties

Care or support must promote the maintenance of family ties and seek to avoid the separation of families or siblings in care, in accordance with the wishes of the person concerned, the nature of the service they are receiving and court decisions. In particular, establishments and services providing reception, care or support for minors, young adults or individuals and families in difficulty or distress shall, in conjunction with the competent public authorities and other stakeholders, take all necessary measures to this end.

In accordance with the individualised care and support plan and the wishes of the person concerned, the participation of the family in everyday activities shall be encouraged.

Article 7 Right to protection

All staff or persons providing care or support shall guarantee the person, their legal representatives and their family the confidentiality of information concerning them within the framework of existing laws.

The person shall also be guaranteed the right to protection, the right to safety, including health and food safety, the right to health and care, and the right to appropriate medical follow-up.

Article 8 Right to autonomy

Within the limits defined in the context of their care or support and subject to court decisions, contractual obligations or obligations related to the services they receive, and measures of guardianship or enhanced guardianship, individuals are guaranteed the possibility of freedom of movement. In this regard, relations with society and visits to and from the institution are encouraged.

Within the same limits and subject to the same reservations, residents may, during their stay, keep their personal belongings and effects and, if they are of legal age, dispose of their assets and income.

Article 9 Principle of prevention and support

The emotional and social consequences that may result from care or support must be taken into consideration. This must be taken into account in the individual care and support objectives.

The role of families, legal representatives or relatives who care for the person in care must be facilitated by the institution, with their consent, in accordance with the individualised care and support plan and court decisions.

The end of life must be accompanied by appropriate care, assistance and support, in accordance with the religious or denominational practices and beliefs of both the person and their relatives or representatives.

Article 10 Right to exercise the civil rights granted to the person accommodated

The effective exercise of all civil rights granted to persons in care and of individual freedoms shall be facilitated by the institution, which shall take all necessary measures to this end, in compliance, where necessary, with court decisions.

Article 11 Right to religious practice

The conditions for religious practice, including visits by representatives of different faiths, must be facilitated, without these practices hindering the missions of the establishments or services. Staff and beneficiaries undertake to respect each other's beliefs, convictions and opinions. This right to religious practice shall be exercised with respect for the freedom of others and provided that its exercise does not disrupt the normal functioning of the establishments and services.

Article 12 Respect for human dignity and privacy

Respect for the dignity and integrity of the individual is guaranteed.

Except where strictly necessary and objectively required for the provision of care or support, the right to privacy must be preserved.

Image rights concern photographs and videos.

The processing of voice recordings is included in this note but is treated separately for the sake of clarity and ease of implementation.

In accordance with the relevant regulatory provisions, the use of a person's image or voice is organised within a defined framework that allows their consent to be obtained in advance. Consent gives individuals a high degree of control over their data.

This note sets out the procedures for obtaining consent for both AFEJI Hauts de France employees and beneficiaries, i.e. individuals supported by the association's establishments and services.

This note applies to all establishments and services, the General Management, Sector Management and Regional Secretariats of AFEJI Hauts-de-France for employees and beneficiaries.

Reference documents:

- Law No. 78-17 of 6 January 1978 on information technology, files and freedoms,
- General Data Protection Regulation (GDPR),
- High Authority for Health, Manual for assessing the quality of social and medico-social establishments and services, March 2022.

Related documents:

- Image rights authorisation form template for employees,
- Image rights authorisation form template for worker-users,
- Image rights authorisation form template for adult beneficiaries,
- Image rights authorisation form template for adult beneficiaries under protective measures,
- Image rights authorisation form template for minors,
- Authorisation form template for voice rights.

GDPR: General Data Protection Regulation

Any filming (photography and video) requires the prior written consent of the employee or beneficiary. To be valid, this consent must be

- Free ' : no one is influenced or coerced in their choice.
- Specific: consent is obtained for a specific purpose.
- Informed: consent must be obtained after the person has been informed in advance of the purpose of the processing, i.e. the objectives for which the images will be used and the length of time they will be stored, enabling them to make their choice in full transparency.
- Unambiguous: consent is given by a clear positive act, such as ticking a box.
- Double ' the person must and may give their consent to the taking of photographs or video and also to their publication or broadcast.

Consent obtained in this manner is valid for a maximum period of five years and must be renewed in the same manner once the five-year period has expired.

Consent must be able to be withdrawn at any time by the person requesting it, in a simple manner. This involves having the employee, beneficiary, legal representative, guardian or curator fill out a new form, rendering the previously completed form null and void.

Thus, the collection of consent or image rights must be organised according to these principles.

- Upon admission of the beneficiary accompanied by the establishment/service,
- Upon signing the employment contract for salaried professionals,
- The completed image rights authorisation form is included in the file of the person (beneficiary or employee).

It is the responsibility of the institution, senior management or departmental management, as applicable, to organise the monitoring of consents, both from employees and beneficiaries, and to respect each individual's choice.

For example, a person may only give their consent for some of the uses mentioned in the form (e.g. consent given to be photographed or filmed but not given for the external publication of the images). It is therefore necessary to be extremely vigilant in this regard.

Furthermore, photographs and videos depicting several people may be used provided that those who have not given their consent are not identifiable (blurred faces).

Image rights authorisation form templates are available. Before use, they should be adapted (name of the establishment/service, etc.) and referenced in your @ualité document management system (under AGEVAL — @ualité software deployed within the association's establishments).

These different forms are tailored to the profiles of the persons concerned: salaried professionals, beneficiaries who are worker-users, adult beneficiaries, adult beneficiaries under protective measures and minor beneficiaries. In the latter two cases, legal representatives, guardians or curators will be consulted in this context.

Checkboxes allow the person to give their consent or notify their refusal regarding the use of the images.

As with images, the use of voice recordings must also be subject to the person's prior consent. The principles for implementation are identical.

As this is not common practice, it is advisable, where applicable, to have the person sign a prior authorisation form if you wish to use their image (see dedicated form). The consent thus given will only be valid for a specific event mentioned in the form.

Image rights authorisation

(Minor beneficiary)

Subject: request for authorisation to photograph, film and publish images

We, the undersigned, legal representatives of the child ……..

Surname: First name:	Surname: First name:
Address:	Address:
Telephone:	Telephone:

☐ We authorise Afeji Hauts de France and [Name of establishment] to photograph, film, edit and reproduce images of the above-named child on all types of media in order to communicate about their activities.

☐ We authorise Afeji Hauts de France and [Name of establishment] to publish these images in their internal publications for the purpose of informing users, their families and employees about the activities carried out: newsletters, activity reports, association magazines, association brochures, internal displays, presentation materials for teams, photo directories, internal events with families, for example, greetings, general meetings and birthdays.

☐ We authorise Afeji Hauts de France and [Name of the establishment] to publish these images on their external publications for the purpose of informing administrators, authorities funding and partners: newsletter, activity report, association magazine, association brochure.

☐ We authorise Afeji Hauts de France and [Name of establishment] to publish these images on the Afeji Hauts de France website for the purposes of providing information and communicating about its activities.

☐ We authorise Afeji Hauts de France and [Name of establishment] to publish these images on the following media or networks: Facebook, Instagram, YouTube, X (formerly Twitter), LinkedIn, Vimeo, Press (e.g. SeniorMag, Voix du Nord, etc.) for non-profit purposes and in order to communicate about its activities.

☐ We do not authorise Afeji Hauts de France and [Name of establishment] to photograph, film, edit and reproduce images of the above-mentioned child on any type of media for the purpose of communicating about its activities.

☐ We do not authorise Afeji Hauts de France and [Name of the establishment] to publish these images. on its internal publication tools for the purpose of informing users, their families and employees about the activities carried out: newsletter, activity report, association magazine, association brochure, internal displays, presentation materials for

teams, internal events with families, for example, greetings, general meetings and anniversaries.

- ☐ We do not authorise Afeji Hauts de France and [Name of the establishment] to publish these images. on their external publication tools for the purpose of informing administrators, funding authorities and partners: newsletters, activity reports, association magazines, association brochures.

- ☐ We do not authorise Afeji Hauts de France and [Name of establishment] to publish these images on the Afeji Hauts de France website for information and communication purposes about its activities.

- ☐ We do not authorise Afeji Hauts de France and [Name of establishment] to publish these images on the following media or networks: Facebook, Instagram, YouTube, X (formerly Twitter), LinkedIn, Vimeo, press (e.g. SeniorMag, Voix du Nord, etc.), for non-profit purposes and in order to communicate about its activities.

We are expressly informed that we may withdraw our consent at any time by sending a written request to Afeji Hauts de France, 26 rue de l'Esplanade, 59140 Dunkirk.

Afeji Hauts de France or any other duly authorised person may make changes to the framing, colour and density that may occur during reproduction.

This authorisation is granted free of charge and for a period of 5 years from the date of collection. This authorisation applies only to the media and modes of distribution explicitly mentioned above. The use of these images for purposes other than those indicated above will require a new request for authorisation.

The images thus obtained may not be used for purposes other than those covered by this agreement.

Afeji Hauts de France expressly refrains from using the images images in any way that is contrary to public decency.
Afeji Hauts de France shall not be held liable for any use made by a third party via the aforementioned media and networks.

The information collected through this form is recorded and allows us to process and administratively monitor the authorisations and refusals issued by the persons concerned regarding the use of their image for communication purposes. The legal basis for the processing is your consent. The data is digitised and stored for 5 years from the date of collection and is only transmitted to the internal departments of Afeji Hauts de France. In accordance with the European Data Protection Regulation (Regulation EU 2016/679 of 27 April 2016 - hereinafter "GDPR") and Law No. 78-17 of 6 January 1978 as amended, you have the right to access, rectify, oppose, limit the processing and erase your data. For more information on the use of your data, please consult our data protection policy or contact our DPO at the following address:dpo@afeji.org .

Afeji Hauts-de-France TOUTES LES VIES ONT LA MÊME VALEUR

Signature of legal representatives

Done at	Done at

The satisfaction of individuals is testament to the quality of the support provided in our establishments. The analysis of complaints and claims helps to evaluate and improve our practices.

The process for collecting and handling complaints and claims must be subject to an appropriate procedure that formalises the system in place. It will also enable us to identify new areas for improvement and respond to the requests of the people we support.

This guidance note defines the procedures for managing complaints and claims in establishments and the formal requirements expected in this context.

The note applies to all AFEJI Hauts-de-France establishments and services.

Reference documents:

- Law No. 2002-2 of January 2002 reforming social and medico-social action,
- Article L.3111-5 of the CASF relating to qualified persons,
- Haute Autorité de Santé PBPP: Supporting and encouraging user engagement in the social, medico-social and health sectors, *2020*
- Ministry of Health, Youth and Sports Methodological guide "Complaints and claims in healthcare establishments: a lever for improving user care"
- High Authority for Health ' Manual for assessing the quality of medical and social establishments and services, *Mcirs 2022*
- High Authority for Health: Manual for the certification of healthcare establishments for quality of care, *September* 2027.

Related documents:

- Charter of Rights and Freedoms of the Person Receiving Care,
- Standard procedure template for "Collecting and processing complaints and claims",
- Standard template for satisfaction/dissatisfaction and complaint register,
- Standard template for complaints/claims tracking table.

Complaint: A request, grievance or complaint made by a user or their family or friends, questioning the quality of service provided by a healthcare or medical-social institution.

Qualified person: The qualified person informs and helps users to assert their rights. In this capacity, they can act as a mediator between the user and the establishment.

In accordance with the relevant legislation and good professional practices defined by the Haute Autorité de Santé (French National Authority for Health), AFEJI Hauts-de-France establishments implement all appropriate means to enable the people they support and/or their families and friends to assert their grievances and complaints.

1. The main principles governing complaints/claims

The management of complaints and claims is the responsibility of the facility director. In this capacity, he or she ensures the proper functioning and implementation of a system for collecting and processing complaints that is tailored to the needs of the individuals receiving care. A procedure must define the planned organisation and must be brought to the attention of users and/or their entourage and professionals. *A standard protocol form is available and covers the main points to be taken into account.*

The establishment must ensure that the persons receiving care, their families and professionals are informed of the provisions implemented internally. Thus, the treatment process and possible remedies in the event of complaints/claims must be included in the user welcome booklet.

The welcome booklet must also include a list of qualified persons and the charter of rights and freedoms of persons receiving care. These two documents must also be displayed in designated areas.

The Social Life Council (in ESSMSJ) and the Users' Commission (in healthcare establishments) must be informed and involved in the handling of complaints and claims. A presentation of grievances is organised every quarter so that they can give their opinions and suggest improvements.

The improvement actions identified are included in the institution's Quality Action Plan (PAØ) and are monitored by the Quality COSUI.

A review of complaints and claims is to be formalised each year in the institution's activity report. The complaints/claims tracking table template, if used, allows graphs to be generated automatically. The review of complaints and claims must be discussed at the CVS meeting.

2. The complaints/claims handling process: Collecting complaints/claims

The establishment must pay particular attention to the overall satisfaction level of the people it supports. While this can be measured through annual satisfaction surveys, complaints/claims must be heard and taken into account by professionals (whether verbal or written).

To facilitate user feedback, the establishment may, if it wishes, implement simple and appropriate formalisation tools (dissatisfaction forms, complaint and satisfaction letter boxes, etc.). Only nursing homes are required to keep a register of satisfaction, dissatisfaction and complaints (model: Berger-Levrault or AFEJI Hauts-de-France template). This register must be made available to people at the establishment's reception desk.

Processing and analysis of complaints/claims

All complaints/claims must be recorded and followed up. A *standard complaint and claim tracking table template is available to establishments. It allows situations to be recorded and analysed.*

Depending on the seriousness of the complaint/claim, the establishment director will organise an internal investigation and may arrange a meeting with the complainant. In all cases, the complainant must be informed that their complaint has been recorded.

In order to receive assistance with the process, the user may request the intervention of a qualified person. Improvement measures may be identified in this context.

The traceability and archiving of complaints/claims

Complaints/claims are archived for a minimum period of 5 years. The archived file includes the various exchanges and reports made with the person being supported and/or their family and friends.

Specific features applicable to healthcare establishments (HÖpital de Jour Château MaintenonJ in the context of handling complaints and claims

Any person who has made a complaint/claim must be informed of the processing of their request by registered letter with acknowledgement of receipt within 8 days of the date of submission of their complaint.

If a mediator is involved, the Users' Commission (CDU) must be informed. The minutes of the meeting between the mediator and the complainant must be sent to the CDU within 8 days so that it can issue its recommendations in the report that will be sent to the complainant.

- ☐ A procedure defining the process for collecting and handling complaints/claims implemented within the establishment
- ☐ A register of satisfaction, dissatisfaction and complaints for nursing homes:
- ☐ A system for recording and tracking complaints and claims:
- ☐ An annual review of complaints/claims in the activity report
- ☐ A notice displayed in reception areas
  - ☐ of the Charter of Rights and Freedoms of the Person Received,
  - ☐ the list of qualified persons,
- ☐ A welcome booklet,
  - ☐ Describing the treatment process implemented in the establishment and the possible remedies in the event of a complaint/claim,
  - ☐ Attaching the Charter of Rights and Freedoms of the Person Received,
  - ☐ Attaching the List of Qualified Persons,
    - ☐ For establishments concerned by the implementation of a CVS or CDU
  - ☐ Systematic inclusion on the agenda of a presentation of complaints/claims collected during the quarter,
  - ☐ Inclusion on the agenda at the end of the year of the annual review of complaints and claims.

Procedure for managing individuals' rights

Date of application	September 2022
Author	DPO Consulting
Issuing department	AFEJI Hauts-de-France – General Management
Validator	DPO Consulting

Distribution		
☐ Confidential	☐Internal	☐Public

Update tracking				
Date	Reference	Author	Subject	Status
20/04/2022	V1	DPO Consulting	Procedure	In progress
27/06/2022	V2	DPO Consulting	Procedure	Completed

Table of contents

1. Objectives and scope

The terms used in this procedure for managing the rights of individuals beginning with a capital letter (hereinafter the "Procedure") are defined in the Appendix "Definitions" of the AFEJI Hauts-de-France General Personal Data Protection Policy.

1.1. Objectives of the Procedure

As Data Controller, AFEJI Hauts-de-France undertakes to ensure that data subjects are informed of their rights and how they can exercise them, in accordance with the applicable Regulations.
The purpose of this procedure is to determine:

- The means used to inform the persons concerned
- Legal requirements that must be complied with
- The means used to respond to requests made by data subjects
- The operational processes to be put in place internally to respond to such requests
- The parties involved in the response process, their roles and responsibilities

1.2. Scope of the Procedure

This Procedure for managing requests from data subjects applies to all AFEJI Hauts-de-France employees. It also applies to all processing activities carried out by AFEJI Hauts-de-France.

All requests to exercise rights made by persons affected by the processing
carried out by AFEJI Hauts-de-France are subject to this Procedure.

In the event of any conflict between this Procedure and the applicable legislation, the following rules shall apply
shall apply:

- If the Procedure provides greater protection, it shall take precedence over the applicable legislation.
- If the applicable legislation provides greater protection, it shall apply to the points concerned in place of the Procedure.

If any doubt remains, the AFEJI Hauts-de-France employee will seek advice from the DPO.

1.3. Communication and Revision of the Policy

This Procedure is communicated to all employees in all departments of AFEJI Hauts-de-France, as well as to all service providers likely to process data that may be subject to a request to exercise rights. Employees responsible for applying it must undergo appropriate training to ensure its effective implementation. It must be made available to AFEJI Hauts-de-France employees at all times.

This procedure will be updated regularly in line with changes to AFEJI Hauts-de-France's internal processes.
of AFEJI Hauts-de-France. It must be consulted regularly. The Procedure is updated by the DPO
of AFEJI Hauts-de-France in the event of:

- Significant changes in the business context or in AFEJI Hauts-de-France's personal data protection strategy;
- Significant changes in risk exposure (e.g. new threats, new trends, etc.);
- Significant changes in applicable legislation.

These changes are subject to approval by the GDPR Steering Committee. Appropriate communication will be provided to AFEJI Hauts-de-France employees in the event of any changes.

2. Rights of data subjects

The applicable legislation grants data subjects the following rights:

1. **Right to information**: the right to clear, accurate and comprehensive information on the use of personal data by AFEJI Hauts-de-France.
2. **Right of access**: the right to obtain a copy of the Personal Data that the Data Controller holds on the applicant. Data Controller holds about the applicant.
3. **Right to rectification**: the right to have Personal Data rectified if it is inaccurate or obsolete and/or to have it completed if it is incomplete.
4. **Right to erasure/right to be forgotten**: the right, under certain conditions, to have the data erased or deleted, unless AFEJI Hauts-de-France has a legitimate interest in retaining it.
5. **Right to object**: the right to object to the Processing of Personal Data by AFEJI Hauts-de-France for reasons relating to the applicant's particular situation (subject to conditions).
6. **Right to withdraw consent**: the right to withdraw consent at any time when Processing is based on consent.
7. **Right to restriction of processing**: the right, under certain conditions, to request that the processing of Personal Data be temporarily suspended.
8. **Right to data portability**: the right to request that Personal Data be transmitted in a reusable format so that it can be used in another database.
9. **Right not to be subject to automated decision-making**: the right for the applicant to obtain human intervention, express their point of view and contest the decision taken in their regard.
10. **Right to define post-mortem guidelines**: the right for the applicant to define guidelines regarding the fate of Personal Data after their death.

Additional rights may be granted to data subjects by local regulations.

3. Details on the implementation of rights

In accordance with the principle of transparency, AFEJI Hauts-de-France is required to provide clear, accessible and intelligible written information on how the Personal Data processed is collected and on the rights of the Data Subject.

3.1. The right to information

Under Article 13 of the General Data Protection Regulation, the Data Controller must provide certain information to the Data Subject.

In the case of direct collection, the information must be provided at the latest at the time of collection of personal data.

R01 Prior to the collection of personal data, AFEJI Hauts-de-France provides comprehensive information to the data subject, in accordance with the applicable legislation.

This information may be provided through information notices (on a website, in job offers), within the various policies and procedures put in place, or by means of a notice that is sufficiently accessible to all Data Subjects.

R02 Data subjects are informed by appropriate means that guarantee transparent processing of personal data.

In the case of indirect collection, there are several ways to inform the Data Subject:

- AFEJI Hauts-de-France shall provide the information within a reasonable period of time and no later than one month after obtaining the Data.
- If the Personal Data is to be used for communication with the Data Subject, the information must be provided no later than at the time of communication.
- If the Data is to be shared with a Third Party, the information must be disclosed no later than the first disclosure of Personal Data.

In certain cases, the obligation to provide information does not apply (e.g. the Data Subject already has the information, AFEJI Hauts-de-France is required by law to obtain or disclose the Personal Data, etc.). Any use of these exceptions must be validated and documented by the DPO of AFEJI Hauts-de-France.

If AFEJI Hauts-de-France wishes to process the Personal Data collected for one or more purposes other than those for which it was initially processed, the Data Controller must provide the Data Subject with adequate additional information before the further processing is carried out.

R03 Information notices are regularly reviewed and updated as necessary.

3.2. Right of access

In accordance with Article 15 of the GDPR, the Data Subject has the right to ask the Data Controller whether it holds Personal Data about them and to request a copy of this data in an understandable format.

AFEJI Hauts-de-France must provide Data Subjects, in the context of their exercise of their right to access their data, the following information:

- The identity and contact details of AFEJI Hauts-de-France as Data Controller
- The source of the Personal Data;
- The purpose(s) of the processing;
- The legal basis for the processing and, where the processing is based on legitimate interest, details of the interest pursued by AFEJI Hauts-de-France;
- The contact details of the Data Protection Officer (DPO);
- The retention period for Personal Data or the criteria for determining this period;
- The recipients or categories of recipients, where applicable;
- The rights of Data Subjects (right of access, right to rectification, erasure, restriction, objection and portability);

- The existence of a Data Transfer outside the European Union, as well as the related information (country, entity) and guarantees (Adequacy Decision, standard contractual clauses, Binding Corporate Rules, etc.);
- The fact that the provision of Data depends on a regulatory or contractual requirement or is a condition for the conclusion of a contract, the existence of an obligation for the Data Subject to provide their Data and the consequences of not providing the Data;
- The existence of an automated decision and related information;
- The existence of further Processing for another purpose and the information relating thereto ;
- The right to withdraw consent, if the Processing is based on consent;
- The right to lodge a complaint with the supervisory authority (CNIL).

A Data Subject who exercises their right of access must obtain disclosure of all Personal Data concerning them, whether stored in an active database or archived.

Limits to the right of access: The right of access must be exercised in accordance with the rights of third parties. It is not possible for a Data Subject to request access to Personal Data concerning, for example, their spouse or colleague. Each Data Subject may only obtain their own Personal Data. In practice, this may, for example, lead to the identity of third parties or elements that could indirectly identify them being concealed in the information sent to the Data Subject.

Similarly, the right of access may not infringe on business confidentiality or intellectual property (e.g. copyright protecting software) of AFEJI Hauts-de-France.

In the event of a request for access, all Personal Data stored in all IT tools must be disclosed, in particular:

- All Personal Data provided by the Data Subject;
- All Personal Data contained in the Data Subject's customer file, whether in paper or electronic form;
- All Personal Data resulting from the Data Subject's activity;
- All exchanges with the Data Subject.
- All personal data contained in the free comment fields;
- All telephone recordings (scripts) of conversations with the Data Subject;

The fact that Personal Data is contained in a document does not make it non-communicable. Personal Data contained in a document (letter, note, report, voice or video recording, etc.) may be communicated by copying the document itself or by faithfully transcribing it onto another medium. Personal Data recorded in business software (CRM, HR management, etc.) may be communicated by transmitting screen prints or an accurate transcription on another medium.

If the Data Subject considers that the Personal Data provided is incomplete, they have the right to ask AFEJI Hauts-de-France to complete the information provided. Failing this, they may lodge a complaint with the CNIL.

3.3. Right of rectification

In accordance with Article 16 of the GDPR, the Data Subject has the right to request that the Data Controller rectify or update their Personal Data if it is inaccurate or incomplete. The Data Subject also has the right to complete their Personal Data by providing additional information.

If the personal data has been communicated to third-party Processors, AFEJI Hauts-de-France, in its capacity as Data Controller, is obliged to inform each Recipient/Processor of the rectification, as far as possible. In this case, AFEJI Hauts-de-France must:

- Rectify the Personal Data of the Data Subject;
- Update and/or complete the information as soon as it becomes aware that the personal data has become inaccurate; has become inaccurate;
- Inform the Data Subject that their Personal Data has been rectified.

3.4. Right to object

In accordance with Article 21 of the GDPR, the Data Subject must be able to object at any time to the Processing of their Personal Data on grounds "relating to their particular situation" without having to provide justification.

Not all Processing may be subject to objection. Objection is possible
only for the following types of processing:

- Processing based on legitimate interests
- Direct marketing, including profiling
- Processing for scientific, historical and statistical research purposes.
- Processing related to automated decision-making.

When the objection request concerns commercial prospecting, the request does not need to be
justified. AFEJI Hauts-de-France must comply with it immediately.

If the right to object is exercised, AFEJI Hauts-de-France must delete the email address of the data subject from all commercial prospecting databases.

When the objection request does not concern commercial prospecting, AFEJI Hauts-de-France may refuse to comply with the request on the grounds that:

- There are legitimate and compelling reasons for processing the Personal Data or that it is necessary for the establishment, exercise or defence of legal claims;
- A contract binds the person to AFEJI Hauts-de-France;
- There is a legal obligation to process the Personal Data of the Data Subject;

Please note: The right to object is not a right to the simple and definitive deletion of the Personal Data of the Data Subject or the customer account associated with it.

Furthermore, a functional unsubscribe link must be included in all commercial communications to enable Data Subjects to effectively exercise their right to object to commercial prospecting. The unsubscription must be effective for all campaigns and not only for the one from which the Data Subject has unsubscribed, unless the person is clearly informed of the means to unsubscribe from all campaigns.

3.5. The right to restriction of processing

In accordance with Article 18 of the GDPR, a Data Subject may request the restriction of the Processing of their Personal Data by AFEJI Hauts-de-France. Where the Data Subject contests the accuracy of the Personal Data collected or objects to the processing of their Personal Data, they may request the Data Controller, when submitting their request for rectification or objection, to freeze the use of their data while their request is being examined. The Data Subject may also request the restriction of processing when access to their Personal Data requires additional time.

A request does not necessarily have to include the words "request for restriction or limitation" or Article 18 of the GDPR, provided that one of the conditions listed below applies:

- The request must specify which processing is to be restricted and why.
- Requests that are not justified and/or descriptions that are vague or general must be returned to the person (or their representative) with a request to indicate why they are requesting this restriction.
- If the request is not sufficiently clear, additional information is requested from the Data Subject and/or their representative.
- The data subject disputes the accuracy of their personal data and AFEJI Hauts-de-France verifies the accuracy of the data.
- The data has been processed unlawfully and the data subject objects to its erasure and requests restriction.

The GDPR suggests various methods that can be used to restrict data, such as:

- Temporarily transferring the personal data to another processing system;
- Making the personal data unavailable to users;

Once the use of Personal Data has been "frozen", it may only be used by AFEJI Hauts-de-France in the following cases:

- The Data Subject has once again given their consent to the processing of their Personal Data,
- For the establishment, exercise or defence of legal claims,
- For the protection of the rights of another natural or legal person,

3.6. The right to erasure

In accordance with Article 17 of the GDPR, the Data Subject must be able to obtain the erasure of their Personal Data at any time in the following cases:

- The Personal Data is not or is no longer necessary for the purposes for which it was originally collected or processed;
- They have withdrawn their consent to the use of their Personal Data;
- Their Personal Data must be erased to comply with a legal obligation.

Exercising this right does not necessarily result in the simple and definitive deletion of all personal data relating to the Data Subject and held by the Data Controller. For example, a request to delete photos from a website will not result in the deletion of the personal account. Similarly, a request to delete a customer account

does not necessarily result in the deletion of invoices and other accounting documents relating to purchases for which there is a legal obligation to retain them.

The Data Controller may refuse to erase the Personal Data of a Data Subject when it is necessary:

- To comply with our legal obligations,
- the establishment, exercise or defence of legal claims,
- For scientific or historical research purposes or for statistical purposes for use in the public interest.

When the request for deletion of Personal Data concerns the data of a prospect who is not bound by any contract with AFEJI Hauts-de-France**,** the Personal Data must be completely deleted.

When a Data Subject makes a request to AFEJI Hauts-de-France, their Personal Data must be deleted from all AFEJI Hauts-de-France databases, including those held by service providers or Subcontractors.

3.7. The right to portability

In accordance with Article 20 of the GDPR, the Data Subject must be able to obtain a copy of the Personal Data that they have provided in the context of a contract or that has been collected with their consent in a structured, commonly used and machine-readable format.

The Data Subject also has the right to request that their Personal Data be transferred to another organisation, provided that this transfer is technically possible. If the Data Subject wishes to have their Personal Data transferred to a third party, it must first be verified whether this is technically possible. If this transfer is technically impossible, the reasons must be explained to them.

Personal data must be provided in a structured, commonly used, machine-readable, open and interoperable format. Some examples of authorised formats are: Word, Excel, vCard, CVS.

PDF format is not permitted as it requires the acquisition or use of different software in order to reuse the data.

This right applies when the Data Subject has provided the Personal Data by giving their consent or if the processing is necessary for the performance of a contract. It applies to Personal Data provided voluntarily by the Data Subject, data generated by the use of AFEJI Hauts-de-France's product or service, and Personal Data resulting from the observation of their behaviour.

4. General information on the management of requests

4.1. Verification of the quality of the Applicant

Requests to exercise rights must be made by a natural person only. All natural persons concerned by one or more Data Processing operations carried out by AFEJI Hauts-de-France may submit a request to exercise their rights.

The request may be made:

- By the data subject themselves
- By a third party making the request on behalf of the Data Subject. The request must be accompanied by a **valid mandate** signed by the Data Subject, serving as authorisation.

For each request made, the Data Controller is required to systematically verify the identity and status of the requester. In case of reasonable doubt, the Data Controller may request a copy of proof of identity (e.g. copy of identity card, copy of passport, etc.).

R04 The status and identity of the applicant are systematically verified.

4.2. Response time

All requests to exercise rights must be processed within one month of the receipt of the request.

If the request is made on site and cannot be fulfilled immediately, the Data Subject shall be redirected to another means of exercising their rights, such as sending a letter or email to the postal and email addresses provided in advance.

If the request is unclear or incomplete, the one-month period may be suspended in order to obtain the information necessary to process the request. The request for clarification must be sent without undue delay.

If the request proves to be complex or if the number of requests being processed is high, the one-month period may be extended by two additional months. In all cases, AFEJI Hauts-de-France must ensure that the data subject has been informed of the extension within one month of receiving their request.

R05 All requests shall be processed within one month, unless an extension is justified and notified to the applicant.

4.3. Exercise of rights free of charge

The exercise of rights is in principle free of charge and cannot give rise to any invoicing. However, AFEJI Hauts-de-France may require the payment of reasonable fees when the Data Subject requests an additional copy or when the Data Subject's request is manifestly excessive and/or unfounded.

R06 The management of requests is, in principle, free of charge and any payment of fees must be justified and proportionate.

4.4. Language of contact

Where possible, AFEJI Hauts-de-France must respond to requests made by data subjects in the language used to submit the request.

R07 Requests shall be handled, as far as possible, in the language used by the applicant.

4.5. Data security

AFEJI Hauts-de-France shall ensure that appropriate measures are in place to guarantee the security and confidentiality of Personal Data processed in connection with the request(s) made by the Data Subject, according to the channel selected by the Data Subject when making the request, while ensuring the required security and confidentiality.

R09 The security of data transmitted as part of the application is ensured by appropriate means.

5. Application management

5.1. Receipt of the request

All requests must be received by the DPO of AFEJI Hauts-de-France. If the request is received by an employee or subcontractor of AFEJI Hauts-de-France, it must be forwarded without delay to the DPO, accompanied by all relevant information concerning the request. The employee or subcontractor shall contact the DPO in case of doubt about the nature of the request.
When a member of staff is questioned verbally by a Data Subject about the exercise of their rights, the Data Subject must be redirected to the other means of contact available, namely the postal and email addresses dedicated to requests for the exercise of rights by Data Subjects.

5.2. Identity of the applicant

Data subjects are not required to justify their desire to exercise their rights. However, the request can only be properly processed if the rights to be exercised are clearly specified and the data subject's identity can be proven.
In the event of reasonable doubt as to the identity of the data subject, AFEJI Hauts-de-France may require proof of the data subject's identity (ID card, passport, etc.). When verifying the identity of the data subject, the statutory one-month time limit is suspended during this period.

- If the person concerned **appoints a representative of their choice**, certain formalities must be observed:
  - A letter specifying the purpose of the mandate
  - The identity of the principal and the agent
  - Proof of identity of the principal and the representative

  If one or more of these items are missing, the DPO reserves the right to request the missing documents from the applicant. If the missing documents are not provided, the request will be declared inadmissible.

- If the data subject is **a minor**, the legal guardian (parent, holder of parental authority, etc.) must submit the request. legal guardian) must carry out the procedure. Their identity must be verified, as well as their relationship relationship with the minor must be verified. In the case of guardianship, curatorship or judicial protection, the identity and powers of the legal representative, as well as the order to change legal representatives, must be verified.

- If the applicant is **the heir of the person concerned**, in the absence of instructions provided during their lifetime, the heirs have the option of exercising certain rights, such as the right of access.

  during their lifetime, the heirs may exercise certain rights, such as the right of access if it is necessary for the deceased's estate or the right to object to the closure of the deceased's user accounts and to object to the processing of Data concerning him or her.
  The DPO must then verify the identity of the rights holders and the purpose of exercising their rights.

5.3. Acknowledgement of receipt of the request

Once the request to exercise rights has been received, an acknowledgement of receipt must be sent to the applicant, indicating the estimated time frame for a response. If the information provided is not sufficient to respond to the request, a letter requesting additional information must be sent to the data subject. The legal time frame will only begin to run once they have provided all the necessary information.
Letters of acknowledgement of receipt and requests for additional information must only be sent by the DPO within a maximum of 5 working days of the request being submitted.

5.3.1. If the request does not require any additional information

Once all the checks have been carried out, an acknowledgement of receipt must be sent to the data subject by post or letter, indicating the estimated time frame for a response.
Acknowledgements of receipt must only be sent by the DPO within a maximum of 20 working days of the request being submitted.

5.3.2. If the request requires additional information

If the information provided by the person concerned is not sufficient to process the request, it is then necessary to request all the information required to process the request.
In this case, the legal response period shall only commence once she has provided all the necessary information.
Requests for additional information must only be sent by the DPO and within a maximum of 20 working days following the submission of the request.
If the request is considered complex, AFEJI Hauts-de-France may request additional time to process the request.

5.4. Processing of the request by the department concerned

Once the request has been received, the DPO must identify and contact the teams or departments concerned by the request. The following departments are involved in processing requests to exercise rights:

- The GDPR Steering Committee
- IT Department
- Relevant Business Department
- The General Management or Regional Management to refer to the establishment and/or relevant department

5.5. Response to the request

The DPO is responsible for responding to the request made by the data subject. They must take into account:

- Applicable exemptions;
- For access requests, if third-party information is included in the information covered by the request, they will examine whether the third party in question has consented to the information concerning them be affected by the request;
- The format of the information provided: data subjects may specify the format in which they wish to receive their response(s) (e.g. hard copies, electronic document, etc.). AFEJI Hauts-de-France must take these preferences into account to the extent that this is reasonable and without compromising the security of the information.

The response to the request must be presented in the same form as the request made.
Where the request concerns the exercise of the right of access, the information must be communicated to the data subject in an intelligible form.
The sensitivity of the information in question and the need to retain proof that the request has been processed must be determining factors in the choice of method of access to the information.

The DPO is responsible for determining what information should be disclosed in response to a request for access to data and for preparing the files/documents submitted by the teams and departments concerned for disclosure to the applicant.

Particular attention must be paid to the information that can be disclosed to the data subject. Information about third parties must therefore be redacted so that it is not transmitted without their authorisation.

When data is sent via postal services, the document must be:

- sealed in a sturdy envelope;
- marked "Private and confidential, for the attention of the addressee only";
- sent to a specific person;
- sent by registered post with the registered number recorded by the DPO.

When the information must be delivered by hand or collected in person, the identity of the requester must be verified before any information is disclosed. The person concerned will also be asked to sign a receipt, which will be kept by the DPO.
If requests are considered manifestly abusive due to their number or systematic nature, or if the data has not been retained, it is possible not to respond to them.
If AFEJI Hauts-de-France does not wish to comply with the request, this decision must be justified. The person concerned must also be informed of the means and time limits for appealing against this decision.

5.6. Recording and closing of the request

AFEJI Hauts-de-France must be able to prove that a response has been provided to all requests made by the persons concerned, particularly in the event of a complaint by the person to the CNIL or legal action.

To this end, the AFEJI Hauts-de-France DPO keeps a register of all requests received and processed and retains all correspondence and documents enabling the history of the request's processing to be traced. This register is available on the myDPO tool.
The register specifies the following information for each request:

- Type of request (right exercised)
- Data subject (surname, first name, contact email address)
- Identity verification (yes/no)
- The department concerned by the request
- Date and method of receipt
- Request expiry date
- Status of the request
- Processing history (free comments on exchanges with the applicant, follow-up to the application, etc.)
- Complexity of the request and, where applicable, justification for its complexity

This register is also entered in the AFEJI Hauts-de-France processing register. This record may be used in the event of a dispute with the data subject, particularly in the event of a refusal to grant access, with the burden of proof resting with the data controller.

All requests must be received by the DPO of AFEJI Hauts-de-France. If the request is received by an employee or subcontractor of AFEJI Hauts-de-France, it must be forwarded without delay to the DPO, accompanied by all relevant information concerning the request. The employee or subcontractor shall contact the DPO in case of doubt about the nature of the request.

5.7. RACI

The implementation of the key steps detailed in this section is carried out within AFEJI Hauts-de-France, according to the following responsibility matrix:

	DPO	Department concerned
Registration of the request	AR	R
Verification of the applicant's identity + request for proof of identity	AR	R
Analysis of the admissibility of the application	AR	R
Execution of the request	C	AR
Response to the applicant	AR	R

Caption:

- A: Responsible Person - The person responsible for carrying out the action. the action
- A: Accountable – Person who bears the for carrying out the action
- C: Consulted – Person consulted in the context of carrying out the action. They may participate in carrying it out
- I: Informed – Person informed of the implementation and progress of the action. They are not expected to participate in the action.

6. Follow-up on requests

Since AFEJI Hauts-de-France must be able to prove that a response has been provided to all requests made by the persons concerned, it is necessary for AFEJI Hauts-de-France to record all requests in a register, but also to keep all correspondence and documents enabling the history of the response to be traced.

In this context, AFEJI Hauts-de-France keeps an up-to-date register of requests, indicating the following information for each request:

- Type of request,
- Where applicable, details relating to the complexity of the request
- Person concerned (surname, first name, internal identification number where applicable)
- Date of receipt
- Date of dispatch of the acknowledgement of receipt
- Response deadline
- History of exchanges with the applicant
- Date of processing of the request (closure of the procedure)
- Response provided (Accepted, Rejected)
- Information regarding possible follow-up action (complaints, etc.)

This register must be made available to the CNIL upon request.

This record may be used in the event of a dispute with the data subject, particularly in the event of refusal to grant access, with the burden of proof resting with the data controller.

R10 A register of requests is kept up to date by AFEJI Hauts-de-France.

Children in danger? Parents in difficulty?

The best thing to do is talk about it!

Need help?

On our website:

www.allo119.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

DÉPARTEMENTS DE FRANCE

Good Eye' D 01 45 46 06

IDEA FORM / COMPLAINT FORM

☐ I have an idea/suggestion ☐ I have a complaint

This concerns

☐ My room	☐	☐
☐ The meal	☐	☐
☐ The outings	☐	☐ Other
☐ My rights	☐	
☐	☐	

Please describe your idea or complaint here

You are in the unit: ☐ Estan ☐ Lighthouse ☐ Belfry

☐ Large ☐ Farmhouse ☐ DPM

Your name (you don't have to specify)

How does it work?

You fill in the form.

Put it in the Ideas & Complaints Box.

xxxxxx collects the box every Monday

The forms are reviewed by professionals during a

on Tuesday

If you have put your name on your form, you will receive a reply directly.

If you have not put your name on it, the subject will be discussed during (a group meeting with the children on Wednesday?).

Not all of your requests can always be fulfilled. If this is not possible, we will explain why. However, we can work with you to find another suitable solution.

Thank you for your participation!