

# Registre de traitement

## Administratif

### Demandes d'adhésion

**Finalité** : traiter les demandes d'adhésion

**Base légale** : intérêt légitime

**Durée de rétention** : jusqu'à traitement par le CA (intégration au registre des membres)

**Données concernées** : email reçu sur la liste `bureau@`

**Localisation des données** : Boîte mail du CA

**Mesures de sécurité** : Chiffrement GPG `schleuder`

### Registre des membres

**Finalité** : lister les membres de l'association, convoquer les AG

**Base légale** : intérêt légitime

**Durée de rétention** : tant que membre de l'association

**Données concernées** : identité (étatique ou pseudo), email, clef GPG, date d'inscription, n° adhérent (uuid4)

**Localisation des données** : Wallet `pass` du CA

**Mesures de sécurité** : Chiffrement GPG

**Point d'attention** : la suppression d'un membre dans le registre conserve par défaut l'historique du fichier dans git. Il sera nécessaire de réécrire l'historique pour effacer définitivement les données. Le cas se posera au 1er départ d'un membre, un script ad-hoc devra être implémenté à cette date (éventuellement manuellement via `bfg`).

# Données bancaires

**Finalité** : récolter des financements pour l'association

**Base légale** : obligation légale (LCB-FT)

**Durée de rétention** : [6 ans](#)

**Données concernées** : données bancaires (IBAN et PAN, nom et prénom, montant et description des versements)

**Localisation des données** : services bancaires de Wise, Mollie et Infomaniak (via Checkout)

**Mesures de sécurité** : PCI-DSS & assimilé côté Wise

**Point d'attention** :

Il n'y a pas de DPA au sens strict avec Wise, parce qu'aucune banque n'en propose en vrai... C'est moins dérangeant pour des services bancaires étant donné la régulation déjà obligatoire du secteur

La politique de confidentialité de Wise est disponible [ici](#)

Le site web est relativement propre et sans tracker ni CDN (hormis un seul appel à Cloudflare pour l'anti-bot...)

Ce choix final de Wise, manquant tout de même d'encadrement légal vis-à-vis du RGPD, reste regrettable pour l'association mais est une des rares solutions honorables pour tout de même permettre l'accès à une offre bancaire. L'association aura dans tous les cas été vigilante sur le choix de ce prestataire et le restera dans le futur. Les usagers ne seront de toute façon pas exposés directement à Wise puisque passent par leur banque personnel pour effectuer un virement. Les seules données échangées relèvent donc uniquement des obligations bancaires de Wise, limitant très fortement les problèmes de conformité.

De même pour Infomaniak/Checkout & Mollie

Des échanges sont en cours avec ces co-responsables de traitement pour tenter d'améliorer la situation.

## Conformité & risques

### Journaux HTTP

**Finalité** : répondre aux obligations légales de l'Association

**Base légale** : obligation légale

**Durée de rétention** : 15 jours (logrotate)

```
# cat /etc/logrotate.d/nginx
/var/log/nginx/*.log {
    daily
    missingok
    rotate 14
    compress
    delaycompress
    notifempty
    create 0640 www-data adm
    dateext
    sharedscripts
    prerotate
        if [ -d /etc/logrotate.d/httpd-prerotate ]; then \
            run-parts /etc/logrotate.d/httpd-prerotate; \
        fi \
    endscrip
    postrotate
        invoke-rc.d nginx rotate >/dev/null 2>&1
    endscrip
}

# cat /etc/caddy/Caddyfile
(logging) {
    log {
        output file /var/log/caddy/{args[0]}.access.log {
            roll_at 00:00
            #backup_time_format 20060102
            backup_time_format 2006-01-02
        }
        format console
    }
}
```

**Données concernées** :

- IP
- date
- user agent
- URL consultée

**Localisation des données :**

- naboo@/var/log/nginx
- prime@/var/log/nginx

**Mesures de sécurité :** Restriction des accès SSH

**Références :**

- [CNIL] Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation

<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044272396>

NB : L'Association utilisait initialement Caddy mais qui ne propose pas d'option gérant correctement la purge des journaux. Les services ont été migrés sous Nginx en espérant une correction côté Caddy. Ce changement a fait l'objet d'une inscription au registre des violations ci-dessous.

Une PR a été proposée au projet et est dorénavant intégrée à Caddy  
<https://github.com/caddyserver/caddy/pull/7244>

## Journalisation Flarum

**Finalité :** répondre aux obligations légales de l'Association

**Base légale :** obligation légale

**Données concernées :** adresse IP, date

**Durée de rétention :** 15 jours

Extension Flarum pour anonymiser les IP passé la durée de rétention

<https://git.imirhil.fr/aeris/flareum-anonymize-ip>

## Sauvegarde

**Finalité :** assurer la reprise d'activité en cas d'incident d'exploitation sur la production

**Base légale** : intérêt légitime

**Durée de rétention** : 1 an

**Localisation des données** :

- endor@/mnt/backup/snapshots/asso-purr.eu.org/
- endor@/mnt/backup/plakar/
- 2 disques externes en rotation
- Stockage S3 Scaleway

**Mesures de sécurité** :

- Double chiffrement borgbackup
  - chiffrement AES256 AEAD
  - clef privée protégée par un mot de passe haché par blake2
  - clef privée et mot de passe exclusivement détenus par les administrateurs de l'Association
- Chiffrement natif Plakar

NB : les données envoyées chez Scaleway étant chiffrés et sans accès à cette clef par ce sous-traitant, celui-ci ne rentre pas dans le cadre du RGPD et ne nécessite donc pas de signature de DPA

# Fourniture de service

## Forgejo

**Finalité** : héberger le code-source des outils développés

**Base légale** : intérêt légitime

**Durée de rétention** : sans limite, anonymisation possible sur demande dans la mesure de ce que git permet

**Données concernées** :

- nom / prénom / alias
- alias

**Localisation des données** :

- <https://git.asso-purr.eu.org/>

- prime@/srv/forgejo
- naboo@postgresql:purr\_forgejo

# Firefish

**Finalité** : communiquer avec les utilisateurs

**Base légale** : intérêt légitime

**Durée de rétention** : illimité, le logiciel ne permettant pas facilement la purge des données

**Données concernées** :

- nick handle (compte@instance.fqdn)
- contenu des toots
- message privé

**Localisation des données** : prime@postgres:firefish

**Mesures de sécurité** : restriction des accès administrateur, 2FA activée

NB : l'Association utilisait initialement Mastodon via l'instance <https://piaille.fr>. Mastodon ne permet actuellement pas d'identifier tous les usages fait par un administrateur, n'ayant pas de journalisation y compris en lecture seule des actions de modération, ce qui ne permet pas d'être réellement conforme RGPD, d'autant plus dans le cas d'une sous-traitance (aucun contrôle sur les actions de modération de modérateurs tiers). Il aurait été de plus difficile de signer un DPA conforme avec Piaille et de procéder aux audits annuels nécessaires à être conforme RGPD. Il a donc été décidé d'auto-héberger une instance directement par l'Association

# Flarum

**Finalité** : communiquer entre utilisateurs

**Base légale** : consentement

**Données concernées** :

- nom / prénom / alias
- adresse email
- contenu des messages

**Durée de rétention** :

- tant qu'un compte est actif (les utilisateurs peuvent supprimer eux-même leur compte)
- anonymisation des données du compte (login, mdp...) après 12 mois d'inactivité (vérification bi-annuelle)
- la suppression des posts sera faite en « best effort » au cas-par-cas en cas de demande (pour ne pas trop casser les fils)

### Localisation des données :

- naboo@mariadb:purr\_flarum
- prime:/srv/flareum/public/assets/avatars
- prime:/srv/flareum/storage

### Mesures de sécurité :

- Activation obligatoire de la 2FA pour les admins et modérateurs
- Suppression des appels tiers Google Fonts [présents à l'origine dans les sources](#)
- Désactivation de la présence en ligne par défaut et de l'indexation du profil (non documenté ?)

<https://github.com/flareum/framework/blob/2.x/framework/core/src/User/UserServiceProvider.php#L124-L125>

```
User::registerPreference('discloseOnline', 'boolval', false);
User::registerPreference('indexProfile', 'boolval', false);
```

- Isolation des pages d'administration derrière le VPN

```
server {
    server_name forum.asso-purr.eu.org;
    location /admin { deny all; }
}

server {
    server_name forum.priv.asso-purr.eu.org;
    ssl_client_certificate /etc/ssl/private/org.eu.asso-purr.ca.crt;
    ssl_verify_client on;
    allow 100.64.0.0/16;
    allow fd7a:115c:a1e0::/48;
    deny all;
}
```

# IRC libera.chat

**Finalité** : Communiquer avec les utilisateurs

**Base légale** : consentement

**Politique de confidentialité** : <https://libera.chat/privacy/>

**Données concernées** : adresse IP, nick

Cas intéressant, la plupart des personnes concernées risquent d'être déjà sur Libera pour d'autres raisons, l'usage par PURR ne traite « théoriquement » pas plus de DCP. Les utilisateurs d'IRC étant souvent déjà informés que tout y est plus ou moins public, l'association le rappelant en plus à côté de tout lien amenant au canal de l'association. Libera est en no-log côté IRC, constitue un réseau réputé, avec une privacy policy très correcte. En attendant peut-être à terme l'auto-hébergement d'un service IRC par l'association (ce qui pourrait être aussi un frein à l'adoption de ce moyen de communication, joindre un réseau spécifique étant plus rebutant que de joindre un canal supplémentaire sur un réseau important), il est considéré que ce service est suffisamment conforme et de plus non critique pour ne pas nécessiter de formalisation de DPA avec Libera, sinon veiller à l'actualité du réseau pour être informé en cas de problème. Nos utilisateurs ont suffisamment d'autres moyens simples et accessibles à disposition (Fediverse, adresse de courriel avec GPG implicite et explicite...) pour pouvoir considérer que l'usage de Libera se fait sous le régime du consentement, le refus d'utiliser IRC ne conduisant pas à d'effet négatif (autre que de ne pas pouvoir joindre IRC, bien entendu).

## Dokuwiki

**Finalité** : documenter la vie de l'Association

**Base légale** : intérêt légitime

**Durée de rétention** : illimité, anonymisation si possible sur demande

**Données concernées** :

- nom d'utilisateur, mot de passe
- contenu et date des pages éditées

**Localisation des données** : prime@/srv/dokuwiki

**Mesures de sécurité** : restriction des accès administrateur

# Mattermost

**Finalité** : s'inscrire sur le Mattermost

**Base légale** : consentement

**Durée de rétention** : purge du compte à la suppression

**Données concernées** : email, pseudo, mot de passe

**Localisation des données** : naboo@postgres:purr\_mattermost

---

**Finalité** : communiquer en interne

**Base légale** : intérêt légitime

**Durée de rétention** : best effort (contacter Mattermost pour voir pour la data retention sur les chans critiques)

**Données concernées** : contenu des posts

**Localisation des données** : naboo@postgres:purr\_mattermost

**Mesures de sécurité** :

- restriction des accès administrateur
- 2FA
- (mTLS envisagé, actuellement non supporté par le client desktop)

# Bookstack

**Finalité** : documenter la vie de l'Association

**Base légale** : intérêt légitime

**Durée de rétention** : illimité, anonymisation si possible sur demande

**Données concernées** :

- nom d'utilisateur, mot de passe
- contenu et date des pages éditées

**Localisation des données** :

- prime@/srv/bookstack
- naboo@mysql:purr\_bookstack

### Mesures de sécurité :

- restriction des accès administrateur
- désactivation de Gravatar ( AVATAR\_URL=false )
- désactivation des services tiers ( DISABLE\_EXTERNAL\_SERVICES=true )
- retrait des exceptions CSP des services tiers ( ALLOWED\_IFRAME\_SOURCES= )
- réduction de la précision des logs IP ( IP\_ADDRESS\_PRECISION=2 )
- isolation des pages d'admin derrière le VPN

```
server {
    server_name wiki.asso-purr.eu.org;
    location /settings { deny all; }
}

server {
    server_name wiki.priv.asso-purr.eu.org;
    ssl_client_certificate /etc/ssl/private/org.eu.asso-purr.ca.crt;
    ssl_verify_client on;
    allow 100.64.0.0/16;
    allow fd7a:115c:a1e0::/48;
    deny all;
}
```

# Hedgedoc

**Finalité** : organiser la rédaction collaborative de contenu

**Base légale** : intérêt légitime

**Durée de rétention** : destruction à la fin de la préparation

**Données concernées** :

- contenu et date des pages éditées

---

**Finalité** : créer un compte

**Base légale** : consentement

**Durée de rétention** : suppression des données par l'utilisateur

**Données concernées :**

- email, mot de passe

**Localisation des données :**

- prime@/srv/hedgedoc/public/uploads
- naboo@postgres:purrr\_hedgedoc

**Mesures de sécurité :**

- activation du TLS sur la connection à la base

```
# git diff lib/config/default.js
diff --git a/lib/config/default.js b/lib/config/default.js
index f7df8f99e..8922fcf2a 100644
--- a/lib/config/default.js
+++ b/lib/config/default.js
@@ -38,7 +38,11 @@ module.exports = {
   forbiddenNoteIDs: ['robots.txt', 'favicon.ico', 'api', 'build', 'css', 'docs', 'fonts',
'js', 'uploads', 'vendor', 'views'],
   defaultPermission: 'editable',
   dbURL: '',
- db: {},
+ db: {
+   dialectOptions: {
+     ssl: { require: true, rejectUnauthorized: true, ca:
fs.readFileSync('/etc/ssl/certs/postgresql.crt').toString(), }
+   }
+ },
   // ssl path
   sslKeyPath: '',
   sslCertPath: '',
```

- désactivation des services tiers

```
"csp": {
  "enable": true,
  "directives": {
    "defaultSrc": ['"none"'],
```

```
"styleSrc": ["'self'", "'unsafe-inline'"],
"scriptSrc": ["'self'"],
"imgSrc": ["'self'"],
"fontSrc": ["'self'"],
"connectSrc": ["'self'"]
},
"upgradeInsecureRequests": "auto",
"addDefaults": false,
"addDisqus": false,
"addGoogleAnalytics": false
},
"allowGravatar": false,
```

# DNS

**Finalité** : héberger la zone DNS de l'association

**Base légale** : intérêt légitime

**Durée de rétention** : aucune

**Données concernées** :

- adresse IP des entités demandant une résolution du nom de domaine
- requête DNS effectué

**Localisation des données** :

- dnsdist : naboo (sous-traitant aeris)
- ns1 : prime

**Mesures de sécurité** : restriction des accès administrateur

NB : À noter que les IP traitées ne sont pas stockées et ne sont pour la plupart que des IP de FAI servant de résolveurs cache pour leurs propres clients. Cependant ce n'est pas supposé être le cas dans le fonctionnement nominal d'Internet et l'association devrait voir ici des IP de personnes physiques, donc des DCP. L'association ne pouvant qu'encourager toute personne concernée à utiliser un résolveur DNS local, par exemple pour supporter proprement DNSSec, l'hébergement d'une zone DNS est donc considéré comme un traitement de DCP, aucune information n'est persistée sur disque (pas de log).

NB : l'hyperviseur hébergeant la machine virtuelle de l'association recourt à dnsmasq pour propager les requêtes en IPv4 au serveur de l'association

# Signature des lettres ouvertes

## Signature

**Finalité** : Faire signer des lettres ouvertes

**Base légale** : consentement

**Durée de rétention** : 6 mois passé la remise de la lettre ouverte

**Données concernées** :

- identité, qualité, adresse email

**Localisation des données** :

- naboo@postgresql:purr\_demarches

## Déduplication et vérification

**Finalité** : Détecter d'éventuel doublon ou abus

**Base légale** : intérêt légitime

**Durée de rétention** : 6 mois passé la remise de la lettre ouverte

**Données concernées** :

- adresse IP, user agent

**Localisation des données** :

- naboo@postgresql:purr\_demarches

## Collecte des plaintes CNIL

# Authentification auprès de la CNIL

**Finalité** : Pouvoir se connecter au site de la CNIL pour en extraire les plaintes du plaignant

**Base légale** : consentement

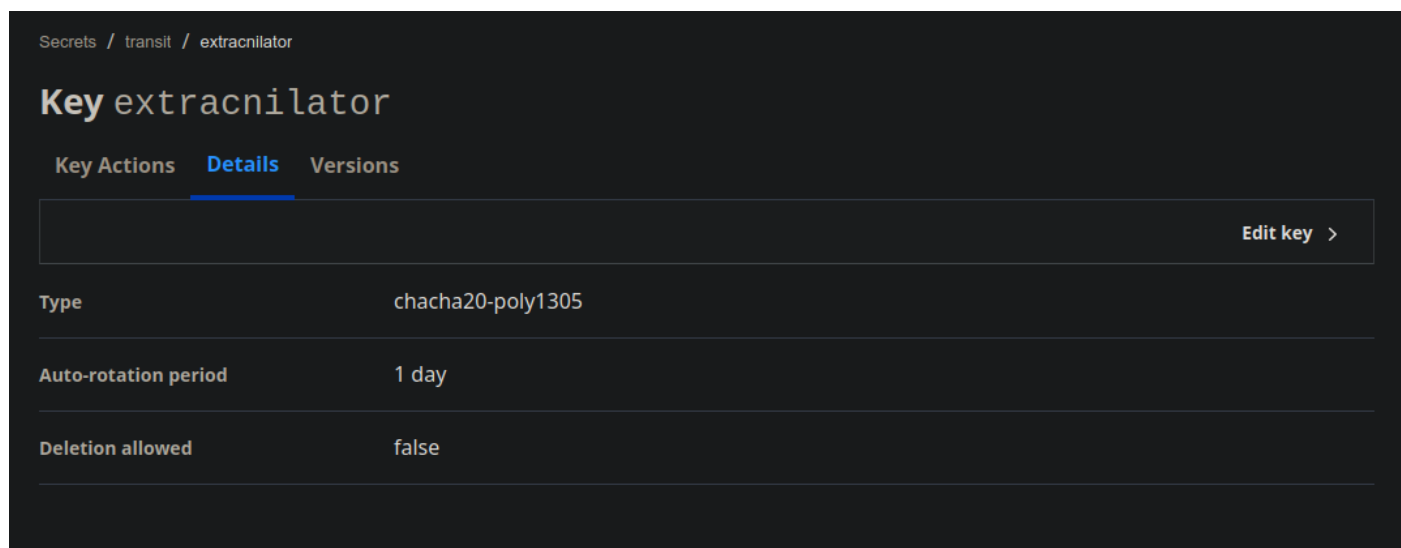
**Durée de rétention** : suppression dès la fin de la collecte des plaintes

**Données concernées** : adresse email et mot de passe CNIL

**Localisation des données** : prime@redis/2

**Mesure de sécurité** :

- Chiffrement CHACHA20\_POLY1305 des données via un HSM Vault avec une rotation de clef à 1 journée



The screenshot shows the Vault interface for a key named 'extracnilator'. The breadcrumb path is 'Secrets / transit / extracnilator'. The key name is displayed in a large font. Below the key name, there are three tabs: 'Key Actions', 'Details' (which is selected), and 'Versions'. A large redacted area covers the key's value, with an 'Edit key >' button to its right. Below this, a table lists the key's configuration:

Type	chacha20-poly1305
Auto-rotation period	1 day
Deletion allowed	false

- Token Vault dédié pour le déchiffrement, effectué dans un processus séparé non exposé sur Internet

## extracnilator-decrypt

[Download policy](#) [Edit policy >](#)

Policy (hcl format)



```
path "transit/decrypt/extracnilator" {  
  capabilities = [ "create", "update" ]  
}
```

# Conservation des données collectées

**Finalité** : conserver les données collectées pour analyses manuelles

**Base légale** : consentement

**Durée de rétention** :

- maximum 1 an, jusqu'à retrait du consentement ou fin d'utilité des données
- une fiche synthétique (responsable de traitement, résumé du cas, décision obtenue...) anonymisée est conservée à des fins d'archivage et de statistiques pour des usages ultérieurs (recroisement des responsables de traitement concernées, identification d'antécédents sur une nouvelle plainte, statistiques des problèmes rencontrés, etc)

**Données concernées** : archive Extracnilator contenant les plaintes effectuées auprès de la CNIL

**Localisation des données** :

- initialement sur prime@/srv/demarches/tmp/archives
- dès disponibilité d'un administrateur ayant les accès requis, mise hors ligne des données sur disque chiffré externe

**Données possiblement sensibles au sens article 9** :

- les données collectées peuvent révéler les habitudes de vie des personnes concernées ayant du saisir la CNIL, les applications mobiles utilisées, leurs banques, la presse ou sites Internet consultés, etc

- dans tous les cas, données sensibles (hors article 9) puisque liés à des contentieux juridiques et administratifs, contenant l'identité d'agent de la CNIL

### Mesures de sécurité :

Les données sont chiffrées avec les clefs GPG des administrateurs de l'association et mis hors réseau dès que possible (extraction au minimum hebdomadaire)

Le répertoire de stockage temporaire des archives n'est lui-même accessible que du processus d'extraction (non exposé sur Internet) et des administrateurs (`chown demarches-sidekiq: && chmod u=rwX,og=`)

Les données brutes ne peuvent être accéder que par eux seuls, et une analyse préliminaire des données sera réalisée pour jauger de la sensibilité de celles-ci avant communication aux équipes d'analyse, avec anonymisation éventuelle si nécessaire

Les équipes d'analyse ne peuvent être constituées que de personnes ayant approuvé la [Charte d'assistance aux personnes concernées](#) et soumis à un encadrement strict

# Signature qualifiée

Outil utilisé : [Documenso](#)

### Localisation des données :

- prime@postgresql:documenso

### Mesures de sécurité :

- désactivation de la télémétrie au build (`NEXT_TELEMETRY_DISABLED` et `TURBO_TELEMETRY_DISABLED`)
- restriction de l'API et des interfaces administrateurs sur l'instance public
- seconde instance administration Documenso branchée sur la même base de donnée
  - accès restreint par VPN
  - authentification par certificat
  - authentification TOTP

```
server {
    server_name sign.asso-purr.eu.org;
    location / { deny all; }
    location /api/ {
        allow ::1;
    }
}
```

```
allow 127.0.0.1;
deny all;
try_files $uri @app;
}

location ~ /(_next/static/|sign/|pdf.worker.min.js) {
    try_files $uri @app;
}
}

server {
    server_name sign.priv.asso-purr.eu.org;
    ssl_client_certificate /etc/ssl/private/org.eu.asso-purr.ca.crt;
    ssl_verify_client on;
    allow 100.64.0.0/16;
    allow fd7a:115c:a1e0::/48;
    deny all;
}
```

# Signature d'un documents

**Finalité** : Permettre la signature électronique de documents

**Base légale** : consentement

**Durée de rétention** : sauf mention contraire, 6 mois passé la fin de validité du document signé

**Données concernées** :

- nom de l'utilisateur
- email
- date de signature
- document signé

# Preuve de signature

**Finalités** :

- S'assurer de l'identité du signataire
- S'assurer de l'unicité du signataire

**Base légale** : intérêt légitime

**Durée de rétention** : sauf mention contraire, 6 mois passé la fin de validité du document signé

- user agent
- adresse IP
- document signé

# Signature & collecte des mandats

**Finalité** : Faire signer des mandats de représentation

**Base légale** : nécessaire à la fourniture du service

**Durée de rétention** : durée de traitement du dossier

**Données concernées** :

- nom, prénom
- adresse email
- mandat
- justificatif d'identité (imposé par la CNIL)

**Localisation des données** :

- liste de diffusion @procedures pour transmission à l'association
- fichier de suivi des plaintes

**Mesure de sécurité** :

- chiffrement GPG de @procedures
- chiffrement E2E [AGE](#) des justificatifs d'identité
- stockage sur machine sécurisée du fichier de suivi, mandat et justificatif (disque chiffré, machine non accessible de l'extérieur, préconisation de sécurité standard/ANSSI, conteneur [VeraCrypt](#) dédié)

# Reçus fiscaux

**Finalité** : Délivrer des reçus fiscaux

**Base légale** : Obligation légale

**Durée de rétention** : 3 ans

**Localisation des données** :

- Nextcloud

**Mesure de sécurité** :

- 2FA
- Authentification par certificat
- Chiffrement Nextcloud
- FDE

---

Revision #22

Created 2024-08-15 19:39:17 UTC by aeris

Updated 2026-04-06 21:00:29 UTC by aeris