Conformité

- Registre de traitement
- Registre des violations
- Administration système
- Charte d’assistance aux personnes concernées

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, nom et prénom, montant et description des versements)

Localisation des données : services bancaires de Wise

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.

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 \
        endscript
        postrotate
                invoke-rc.d nginx rotate >/dev/null 2>&1
        endscript
}
```

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.

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/flarum-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/
- 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

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/flarum/public/assets/avatars
- prime:/srv/flarum/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/flarum/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 suffisament 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:purr_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 virtuel de l'association recourt à dnsdist 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 vérication

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

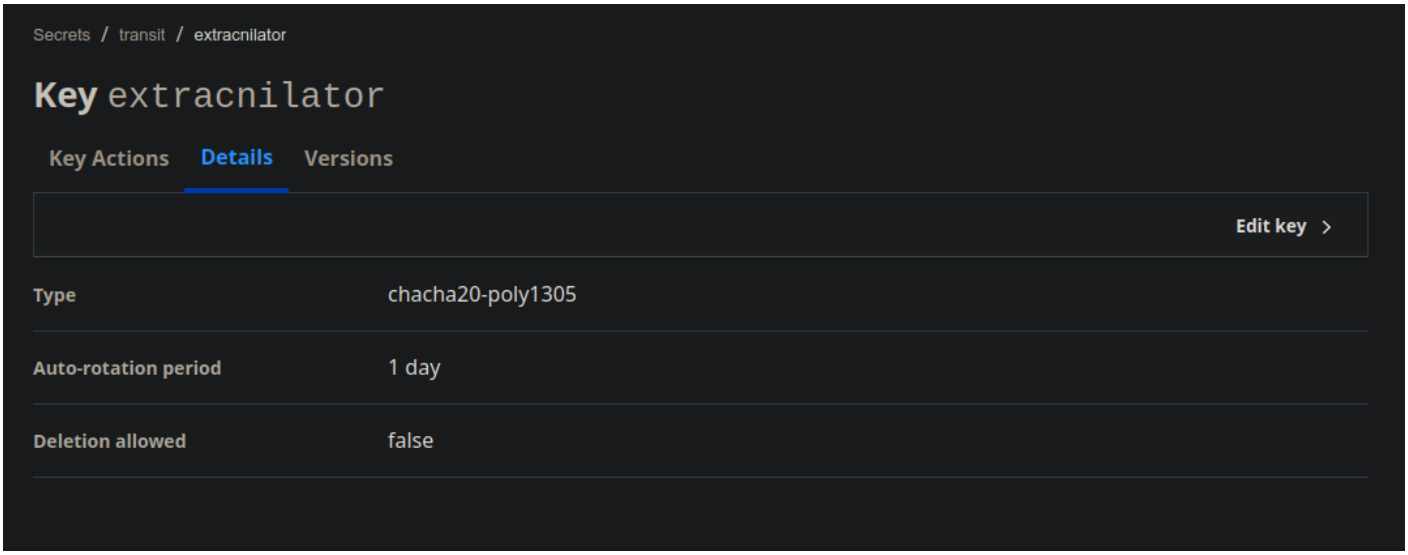
Durée de rétention : suppression dès la fin de la collecte des plaintes

Données concernées : adresse email et mot de passe CNIL

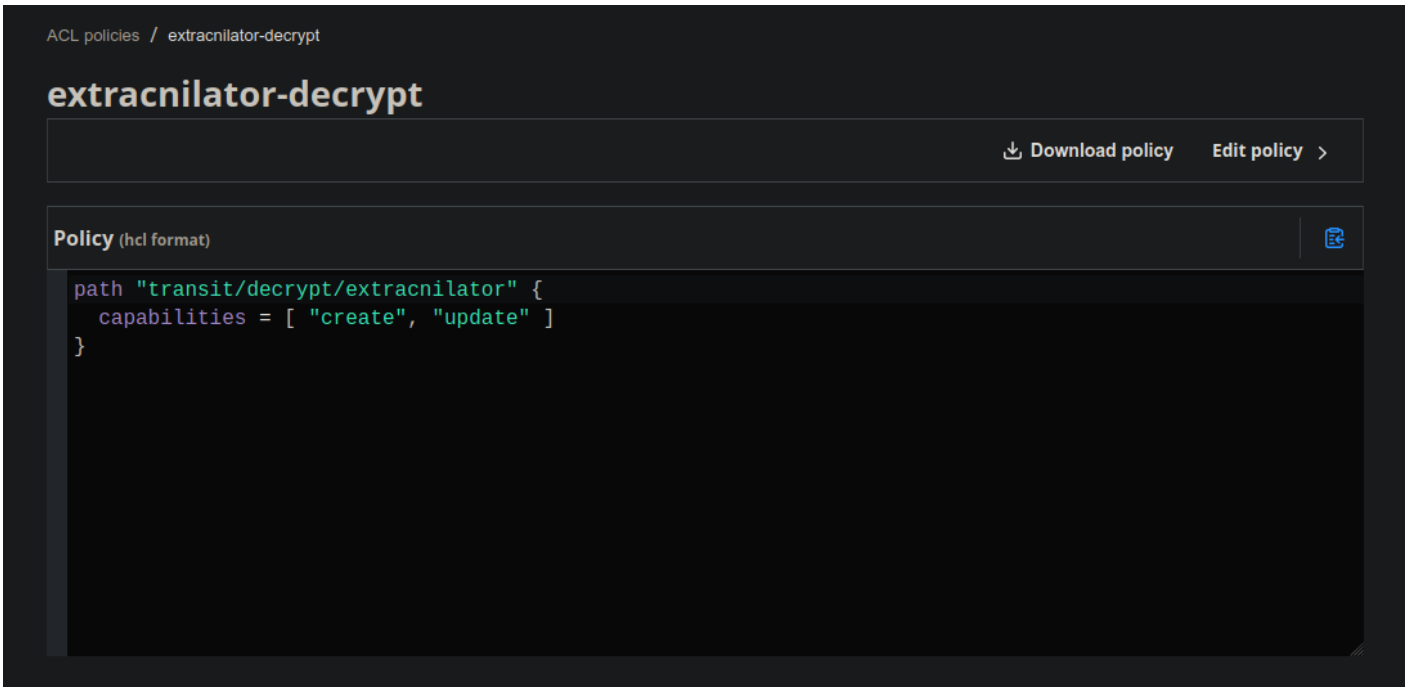
Localisation des données : prime@redis/2

Mesure de sécurité :

- Chiffrement CHACHA20_POLY1305 des données via un HSM Vault avec une rotation de clef à 1 journée



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



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

Localisation des données :

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

Mesure de sécurité :

- chiffrement GPG de @procedures
- stockage sur machine sécurisée du fichier de suivi (disque chiffré, machine non accessible de l’extérieur, préconisation de sécurité standard/ANSSI, etc)

Registre des violations

Violations

Rétention erronée log Caddy

11/10/2023 : Lors de l'audit régulier du système, découverte que Caddy, le serveur web utilisé, ne permet pas de limiter correctement la durée de rétention des logs. Les logs, supposés être conservés pendant 15 jours, conformément à l'arrêt Télé2 de la CJUE, l'ont été en réalité depuis le 15 août 2023 16:49:58. La période concernée correspond à 3101 accès web depuis 289 adresses IPv6 et 591 IPv4 différentes. Tous les accès ne sont pas des personnes concernées au titre du RGPD, la présence de crawler (Fediverse, indexation...) étant notable (70-80%), la distinction précise entre les 2 catégories étant difficile à faire et peu pertinente ici.

Les logs concernés ont été supprimés immédiatement et une migration de l'infrastructure vers Nginx est planifiée avant le 15/10/2023. Le retour à Caddy ne se fera qu'après un correctif permettant de se mettre en conformité.

Les risques pour les droits des personnes concernées étant nuls (correction rapide, pas de perte de confidentialité, aucun usage des données) aucune notification de l'APD n'a été jugée nécessaire ni aucune notification aux personnes concernées.

Non désactivation des logs de debug de dnsdist

06/03/2024 : Dans le cadre d'une mise-à-jour régulière du registre de traitement, un audit des systèmes en place a été conduit pour s'assurer de la cohérence avec les traitements listés. Il a été détecté que le dnsdist déployé en sous-traitance pour relayer le trafic DNS IPv4 vers la machine virtuelle de l'association avait le debug actif, ce qui a conduit à tracer les requêtes effectuées dans les journaux système. Le debug avait été activé le 17/08/2023 pour diagnostiquer un problème de communication DNS, mais n'avait pas été désactivé ensuite.

À la date de la détection du défaut de configuration, 3369 adresses IP, majoritairement des IP sur des plages m2m mais contenant aussi des IP domestiques, étaient encore présentes dans les

journaux. Le sous-traitant a aussitôt notifié l'association et procédé à la désactivation du debug.

Les risques pour les droits des personnes concernées étant nuls (pas d'accès à l'information, rétention limitée à 15 jours, IP essentiellement m2m, données non sensibles) et aucun défaut d'intégrité/disponibilité/confidentialité n'ayant été détecté, aucune notification de l'APD n'a été jugée nécessaire ni aucune notification aux personnes concernées.

Mauvaise configuration de la rétention dans journalctl

19/09/2024 : journalctl avait été configuré de manière à ne conserver les logs systèmes que pour 1 mois. Le paramètre utilisé, `MaxFileSec=1month` n’était pas le bon et ne conduisait pas nécessairement à purger les données passées 1 mois et des données personnelles, en particulier des adresses emails liés à la journalisation de opensmtpd étaient présentes 2 mois de trop (période du 21 juin au 21 août). La configuration a été modifiée pour utiliser `MaxRetentionSec=1month` à la place. Les journaux ont été confirmés comme ne démarant plus qu’à partir du 21 août :

```
# journalctl | head -1
août 21 23:36:17
```

Les risques pour les droits des personnes concernées étant nuls (pas d'accès à l'information, rétention limitée à 3 mois, données non sensibles) et aucun défaut d'intégrité/disponibilité/confidentialité n'ayant été détecté, aucune notification de l'APD n’était donc possible.

Administration système

Infrastructure

Un des fondateurs de l'association héberge une machine virtuelle contenant les services de l'association, entraînant une situation de sous-traitance. Un DPA a donc été signé entre l'association et son fondateur pour la gestion de cet hébergement.

L'hébergement consiste essentiellement à la mise-en-place de reverse-proxy (HTTP, DNS & SMTP) sur les services de l'association située dans une VM LXC.

DNS :

```
/etc/dnsdist/dnsdist.conf
newServer({address="10.0.0.2:53", pool="purr",
        checkName="purr-asso.eu.org.", checkType="SOA",
        healthCheckMode="lazy"})
addAction({'asso-purr.eu.org.'}, PoolAction("purr"))
```

SMTP :

```
/etc/smtpd.conf
action "purr" relay host smtp://10.0.0.2
match from any for domain "asso-purr.eu.org" action "purr"
```

HTTP :

```
/etc/nginx/sites-enabled/org.eu.asso-purr
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name asso-purr.eu.org *.asso-purr.eu.org;
    ssl_certificate /etc/ssl/private/org.eu.asso-purr.crt;
    ssl_certificate_key /etc/ssl/private/org.eu.asso-purr.pem;
    access_log off; # Traffic will already be logged on VM
    error_log off;
    root /var/www/html;
```

```
        location / {
                proxy_pass https://10.0.0.2;
                proxy_ssl_verify on;
                proxy_ssl_trusted_certificate /usr/share/ca-certificates/mozilla/ISRG_Root_X1.crt;
                proxy_ssl_name $host;
                proxy_ssl_server_name on;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto https;
                proxy_set_header Proxy "";
                proxy_pass_header Server;
                proxy_buffering off;
                proxy_redirect off;
                proxy_http_version 1.1;
        }
}
```

À noter que dans le cas de HTTP, la clef privée de chiffrement des services a nécessairement du être recopiée sur la machine de virtualisation.

L'association met à disposition une url interne de PKI pour récupérer le certificat mis-à-jour via ACME :

```
/etc/nginx/sites-enabled/pki
server {
        listen 443 ssl http2;
        listen [::]:443 ssl http2;
        server_name pki;
        ssl_certificate /etc/ssl/certs/ssl-cert-snakeoil.pem;
        ssl_certificate_key /etc/ssl/private/ssl-cert-snakeoil.key;
        ssl_stapling off;
        access_log /var/log/nginx/pki.log;
        error_log /var/log/nginx/pki.log;
        root /etc/ssl/public;

        allow  10.0.0.1;
        deny   all;
}
```

Les certificats sont de toute façon destinés à être publics, mais une solution plus idéale sera développée par la suite pour récupérer le certificat depuis l'URL public du site et procéder aux vérifications d'usage (non expiration, bon domaine, TLSA…) pour s'assurer qu'un certificat verrolé n'est pas déployé lors de son renouvellement.

Hardening

SSH

```
/etc/ssh/sshd_config/security.conf
Port xxx

PermitRootLogin prohibit-password
PubkeyAuthentication yes
PasswordAuthentication no
PermitEmptyPasswords no

Ciphers chacha20-poly1305@openssh.com
KexAlgorithms curve25519-sha256@libssh.org
MACs umac-128-etm@openssh.com

AllowUsers xxx yyy
```

Nginx

```
/etc/nginx/conf.d/security.conf

server_tokens off;

ssl_protocols TLSv1.2 TLSv1.3;
ssl_ciphers EECDH+CHACHA20:EECDH+AESGCM:EECDH+AES:!SHA;
ssl_prefer_server_ciphers on;
ssl_session_timeout 1d;
ssl_session_cache shared:SSL:50m;
```

```
ssl_session_tickets off;
ssl_stapling on; # Need because Let's Encrypt OCSP = Schrems II
ssl_stapling_verify on;
ssl_trusted_certificate /etc/ssl/certs/ca-certificates.crt;
resolver 127.0.0.1;

more_set_headers "Strict-Transport-Security: max-age=31536000; includeSubDomains; preload";
more_set_headers "X-Frame-Options: DENY";
#more_set_headers "X-XSS-Protection: 1; mode=block";
more_set_headers "X-Content-Type-Options: nosniff";
#more_set_headers "Content-Security-Policy: default-src 'none';";
more_set_headers "Referrer-Policy: same-origin";
more_set_headers "Expect-CT: max-age=86400, enforce, report-uri=\"https://aeris.report-
uri.com/r/d/ct/enforce\"";
more_set_headers "Permissions-Policy: interest-cohort=()";
```

Knot

```
                1w      CAA             0 issue "letsencrypt.org"
                ;1w     CAA             0 issuewild ";"
                1w      CAA             0 iodef "mailto:admin@purr-asso.eu.org"
```

Liste de diffusion & mail

Les listes de diffusion de l'association sont hébergées par un Schleuder afin d'être intégralement chiffrées pour les seuls destinataires des listes de diffusion. Les clefs GPG associées sont diffusées ici.

Dans le cas où un lanceur d'alerte ou autre personne sensible voudrait contacter l'association, il devrait d'abord récupérer cette clef et laisser dans les journaux son IP et la date de récupération de la clef GPG. L'association pourrait ultérieurement être perquisitionnée pour obtenir ces informations. La journalisation HTTP est donc désactivée pour cette URL :

```
/etc/nginx/sites-enabled/org.eu.asso-purr
location /.well-known/ {
    root /var/www/public/;
```

```
    access_log off;
}
```

Ces URL n'étant pas modifiable et ne servant pas de contenu à destination directe d'un utilisateur standard, cette modification ne met pas en défaut l'association de son obligation de conservation des journaux de trafic. L'association a procédé aussi à la vérification que la machine virtualisant ses services ne loggait pas non plus ces informations de consultation.

Les clefs ne seront pas publiées dans un annuaire de clefs, ceux-ci étant difficilement compatibles avec le RGPD (voir ici (⚠ trackers google syndication) et là (⚠ trackers Medium)), l'association ne souhaite pas les mettre en avant d'autant plus qu'ils sont notoirement défectueux depuis plusieurs années.

Les clefs sont aussi disponibles via WKD.

```
gpg --auto-key-locate wkd --locate-key <xxx>@asso-purr.eu.org
```

Un script permet la synchronisation des clefs depuis Schleuder :

```
#!/usr/bin/env bash
set -e
schleuder-cli lists list | while read LIST; do
        FINGERPRINT="$(schleuder-cli lists show "$LIST" fingerprint)"
        echo "$LIST" "$FINGERPRINT"
        NAME="${LIST%%@*}"
        DOMAIN="${LIST##*@}"
        KEY="$(schleuder-cli keys export "$LIST" "$FINGERPRINT")"
        WKD_DIR=hu
        ORIG="$DOMAIN/$NAME"
        echo "$KEY" | gpg --dearmor > "$LIST.asc"
        echo "$KEY" | gpg --show-keys --with-wkd-hash | \
                sed -En 's/^ +(\w{32})@.*/\1/p' | \
                while read WKD_HASH; do
                        ln -nfs "../$LIST.asc" "$WKD_DIR/$WKD_HASH"
        done
done
```

Hébergement des mandats

L’association a vocation à collecter et à stocker des mandats de représentation afin de mutualiser des plaintes à la CNIL pour plusieurs personnes concernées. La signature d’un tel mandat nécessite la communication de pièces d’identité pour procéder à une vérification d’identité et éventuellement répondre aux demandes de responsables de traitement ou autorités de contrôle sans nécessité de reprendre contact avec la personne concernée. Les pièces d’identité étant des données extrêmement sensibles, les données associées seront stockées sous 2 formats :

- en chiffrement end-to-end dans un redis temporaire, pour permettre aux modérateurs de vérifier la conformité du mandat et la véracité des pièces d’identité transmises. Ces données seront détruites à l’issue de la vérification, ce qui ne devrait pas dépasser quelques jours. De par le chiffrement e2e, seuls les modérateurs habilités pourront avoir accès aux données en clair. La consultation de ces documents ne pourra se faire que via une interface d’administration accessible après double authentification forte (authentification TLS cliente + TOTP).
- en chiffrement symétrique (chacha20-poly1305) via Vault Transit, pour du stockage longue durée pour les besoins de gestion des plaintes et la réponse aux demandes des RT ou APD. La durée de rétention sera celle de la durée de traitement de la plainte associée.

Vault

Le vault est scellé par Shaamir, nécessitant l’intervention d’au moins 2 administrateurs pour relancer les services, ceci afin d’éviter toute véléité de contrainte sur l’association.

Les premières tentatives de scellement du Vault ont échoué pour une raison inconnue et un message d’erreur cryptique. L’association aurait pu générer les secrets de Shaamir en clair et les chiffrer par la suite, mais il aurait alors existé une possibilité non nulle d’avoir un des administrateurs en possession de suffisamment d’information pour déverrouiller seul le Vault, ce qui aurait été contraire aux objectifs fixés initialement. Après debug, il s’avère que Vault attend obligatoirement des clefs GPG ayant les 2 flags `encrypt storage` et `encrypt communication`. Une des clefs des administrateurs désignés ne contenait que `encrypt storage` et pas `encrypt communication`, ce qui aurait du être pourtant suffisant pour Vault. La clef GPG en question a été modifiée et le scellement du Vault a pu être réalisé :

```
vault operator init -key-shares=3 -key-threshold=2 -pgp-keys=a.asc,b.asc,c.asc
```

Administration système

- 24/01/2024 Un disque dur de la grappe RAID est HS. Retrait du disque + `shred -vz /dev/sdd` (triple passe + zeroed) avant retour fournisseur pour éviter accès aux données. Le disque est de toute façon chiffré intégralement.
- 31/01/2024 Mise-à-jour du serveur pour fixer CVE-2023-6246.

https://security-tracker.debian.org/tracker/CVE-2023-6246 2.36-9+deb12u4 fixed

```
# apt update && apt dist-upgrade
20:Réception de :3 http://security.debian.org/debian-security bookworm-security/main amd64 libc6-dev amd64 2.36-9+deb12u4 [1 897 kB]
25:Réception de :8 http://security.debian.org/debian-security bookworm-security/main amd64 libc6 amd64 2.36-9+deb12u4 [2 748 kB]
95:Préparation du dépaquetage de .../libc6-dev_2.36-9+deb12u4_amd64.deb ...
96:Dépaquetage de libc6-dev:amd64 (2.36-9+deb12u4) sur (2.36-9+deb12u1) ...
101:Préparation du dépaquetage de .../libc6_2.36-9+deb12u4_amd64.deb ...
105:Dépaquetage de libc6:amd64 (2.36-9+deb12u4) sur (2.36-9+deb12u1) ...
106:Paramétrage de libc6:amd64 (2.36-9+deb12u4) ...
275:Paramétrage de libc6-dev:amd64 (2.36-9+deb12u4) ...
```

L’hyperviseur a été aussi patché (confirmation du ST).

- 01/07/2024 : Mise-à-jour du serveur pour fixer CVE-2024-6387 (regeSSHion)

https://security-tracker.debian.org/tracker/CVE-2024-6387 1:9.2p1-2+deb12u3 fixed

```
# apt update && apt upgrade
36:Préparation du dépaquetage de .../01-openssh-sftp-server_1%3a9.2p1-2+deb12u3_amd64.deb ...
37:Dépaquetage de openssh-sftp-server (1:9.2p1-2+deb12u3) sur (1:9.2p1-2+deb12u2) ...
38:Préparation du dépaquetage de .../02-openssh-server_1%3a9.2p1-2+deb12u3_amd64.deb ...
39:Dépaquetage de openssh-server (1:9.2p1-2+deb12u3) sur (1:9.2p1-2+deb12u2) ...
40:Préparation du dépaquetage de .../03-openssh-client_1%3a9.2p1-2+deb12u3_amd64.deb ...
41:Dépaquetage de openssh-client (1:9.2p1-2+deb12u3) sur (1:9.2p1-2+deb12u2) ...
91:Paramétrage de openssh-client (1:9.2p1-2+deb12u3) ...
107:Paramétrage de openssh-sftp-server (1:9.2p1-2+deb12u3) ...
109:Paramétrage de openssh-server (1:9.2p1-2+deb12u3) ...
110:rescue-ssh.target is a disabled or a static unit not running, not starting it.
111:ssh.socket is a disabled or a static unit not running, not starting it.
```

L’hyperviseur a été aussi patché (confirmation du ST).

Charte d’assistance aux personnes concernées

Un grand pouvoir implique de grandes responsabilités

En tant que personne allant assister des personnes concernées dans leurs démarches administratives, vous allez avoir accès à des documents très personnels de tiers engagés dans des procédures suite à des violations de leurs droits.

Cette charte a pour objectif d’encadrer ce traitement de données à caractère personnel, certaines pouvant relever de l’article 9 du RGPD (données sensibles).

1. Les échanges avec la personne concernée doivent être dans la mesure du possible chiffrés avec GPG (si elle en a fait la demande ou possède une clef). Les communications internes par mail doivent être obligatoirement chiffrées avec GPG (Schleuder s’en occupe pour vous côté réception extérieure). Attention à votre fournisseur d’email : les emails personnels US/GAFAM & cie seront bien entendus non utilisables côté association pour ce type de communication. Faites éventuellement valider votre fournisseur par un administrateur en cas de doute.
    1. : Infomaniak, Scaleway, Hertzner, AlwaysData, Proton, RiseUp
    2. : Google, Apple, Microsoft
2. Les documents dont vous pourrez avoir connaissance ne doivent être communiqués à des tiers non habilités sous aucun prétexte. L’association a pour vocation à être transparente sur ses dossiers et à communiquer autant que possible sur ceux-ci, mais l’anonymat d’éventuelles communications publiques sur un dossier doit être garanti.
3. Lors des réponses à une personne concernée ou d’échange interne à l’association, assurez-vous avant envoi du destinataire afin d’éviter de communiquer des informations à la mauvaise personne
4. Les échanges de coordination/relecture ne doivent passer que par des canaux sécurisés approuvés par l’association
    1. liste de diffusion procedures@
    2. canal dédié Mattermost
    3. section dédiée restreinte du forum

    Sur des échanges personnels concernant un dossier, l’usage de canaux sécurisés est aussi obligatoire
    1. Signal, Matrix :
    2. Whatsapp, Telegram, SMS :

    Le chan IRC #purr-procedures n’est pas suffisamment fiable (contrôle par un tiers et communications non chiffrées) pour véhiculer des informations précises concernant un dossier et doit servir uniquement pour la coordination générique et les échanges plus

informels.

5. Les documents fournis par les personnes concernées ou produits par l'association doivent être stockés sur des machines sécurisées pour éviter toute communication à un tiers. L'association n'intervient pas dans un environnement aussi contrôlable qu'en entreprise, et il s'agit bien sûr de vos machines personnelles, mais les éléments suivants sont à vérifier :
    1. De préférence disque chiffré (FDE LUKS), sinon conteneur VeraCrypt chiffré
    2. Mot de passe de session conforme aux standards ANSSI
    3. Verrouillage du poste ou du conteneur chiffré hors utilisation
    4. Idéalement sur matériel non nomade et non partagé
    5. En cas de matériel nomade ou partagé, l'usage de conteneur Veracrypt ou équivalent est nécessaire pour éviter qu'une personne ayant aussi accès à votre machine puisse accéder aux données sensibles en votre possession.
6. La 2FA doit être activée dès que possible sur vos comptes liés aux outils de coordination (forum, IRC, etc)
7. Des précautions toute particulières doivent être prises dans le cas de contact avec des lanceurs d'alerte. Signalez par un canal sécurisé à un administrateur de l'association tout dossier ou personne dans ce cas, afin de prendre les mesures adéquates à chaque situation.
8. En cas de rupture de confidentialité, même mineure, vous devez en informer un administrateur de l'association dans les meilleurs délais, pour prendre les mesures correctrices adéquates et permettre les déclarations légales obligatoires le cas échéant. Commettre une erreur arrivera à tout le monde.
9. N'hésitez jamais à poser une question en cas de doute.

TODO possible à faire côté association :

- fournir des boîtes mails
- ~~Mattermost~~
- Instance Matrix

Pour signer la charte :

```
curl https://wiki.asso-purr.eu.org/books/conformite/page/charte-dassistance-aux-personnes-concernees/export/pdf -o charte.pdf
gpg --detach-sign --armor charte.pdf
```

et envoyer les 2 fichiers (`charte.pdf` et `charte.pdf.asc`) par mail à `bureau@`