REPUBLIQUE ET CANTON DE GENEVE
Département en charge de la Police
Police

GESTION DES AFFAIRES SENSIBLES	
Type : directive de service	**N°** : DS OSI.02.04
Domaine : organisation et sécurité de l'information	
Rédaction : A. Bondet / O. Sissokho	**Validation** : M. Bonfanti
Entrée en vigueur : 19.07.2017	**Mise à jour** : 28.08.2019

Objectif(s)

Cette directive a pour objectif de fixer un cadre général de gestion des affaires de police sensibles ou devenant sensibles de manière à leur assurer un traitement conforme au niveau de la confidentialité nécessaire.

Champ d'application

- Ensemble des directions et services de la police.

Documents de référence

- Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) RS 120.
- Loi fédérale sur la protection des données (LPD) RS 235.1.
- Code pénal suisse (CP) RS 311.0.
- Code de procédure pénale suisse (ci-après : CPP) RS 312.0.
- Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) RSG A 2 08.
- Loi sur la police (LPol) RSG F 1 05.
- Loi sur les renseignements et les dossiers de police et la délivrance des certificats de bonne vie et mœurs (LCBVM) RSG F 1 25.
- Règlement sur l'organisation et la gouvernance des systèmes d'information et de communication (ROGSIC) RSG B 4 23.03.
- Directive du Procureur général D.4. Directive de police judiciaire.
- Directive du Procureur général D1. Information sans retard du ministère public par la police.
- Directive transversale sur la classification des informations, EGE-10-12.

Directives de police liées

- N.A.

Autorités et fonctions citées

- Commandant de la police (ci-après : CDT).
- Chef d'état-major (ci-après : Chef EM).
- Chef des opérations (ci-après : Chef OP).
- Chef du service des commissaires de police (ci-après : Chef Coms).
- Chef de service.
- Chef de groupe.
- Commissaire de police de service (ci-après : Coms).
- Conseiller d'Etat.
- Diplomate.
- Cadre administratif.
- Dirigeant d'entreprise.
- Elu.
- Etat-major (ci-après : EM).

- Haut fonctionnaire.
- Gardien de prison.
- Lieutenant (ci-après : Lt).
- Magistrat du pouvoir judiciaire.
- Magistrat de la Cour des comptes.
- Policier.
- Procureur.
- Responsable de la chancellerie police.
- Sergent-major (ci-après : Sgtm).
- Sergent-major de service/Opérationnel (ci-après : SMO).

Entités citées

- “Automatisiertes Büro Informationssystem” - données genevoises des personnes et des affaires (ci-après : ABI).
- Aéroport international de Genève (ci-après : AIG).
- Brigade aéroport (ci-après : BAERO).
- Brigade de criminalité informatique (ci-après : BCI).
- Base de gestion des séquestres (ci-après : BGS).
- Brigade d'observation (ci-après : BO).
- Brigade de police technique et scientifique (ci-après : BPTS).
- Brigade routière et accidents (ci-après : BRA).
- Brigade de renseignement criminel (ci-après : BRC).
- Centre de compétences des systèmes d'information police (ci-après : CCSIP).
- Centrale d'engagement, de coordination et d'alarme (ci-après : CECAL).
- Centrale routière H24 (ci-après : CENROUT).
- Centrale des opérations de la PI (ci-après : COPI).
- Centrale de vidéoprotection (ci-après : CVP).
- Chancellerie police (ci-après : chancellerie).
- Direction des opérations (ci-après : DIROP).
- Etat de Genève (ci-après : Etat).
- Forensic trace identification management system (ci-après : FTIMS).
- Groupe de filature technique (ci-après : GFT).
- Ministère public.
- Office cantonal des systèmes d'information et du numérique (ci-après : OCSIN).
- Office cantonal des transports (ci-après : OCT).
- Office fédéral des routes (ci-après : OFROU).
- Police internationale (ci-après : PI).
- Police judiciaire (ci-après : PJ).
- Police de proximité (ci-après : POLPROX).
- Police routière (ci-après : POLROUT).
- Police-secours (ci-après : POLSEC).
- Répondant informatique télécom police (ci-après : RITP).
- Service des pièces à conviction (ci-après : SPEC).
- Secteur de la documentation (ci-après : SDOC).
- Tribunal des mineurs.

Mots-clés

- Affaires sensibles.
- Personnalité politique.
- Procédures sensibles.
- Confidentialité renforcée.

- Affaires confidentielles.
- Sécurité renforcée.
- Information sensible.
- Journaliste.
- Evènement sensible.
- Diplomate.
- Immunité.

Annexes

- Annexe 1 : procédure de détection d'une affaire sensible.

1. PREAMBULE

La police traite d'évènements généralement confidentiels. Dans des cas particuliers, en raison des personnes impliquées ou selon la nature intrinsèque des faits en cause, un évènement de police ordinaire peut se révéler sensible.

Dans une telle situation, la question du traitement des données doit être prise en charge de manière pragmatique, rapide et selon des principes et critères précis et connus de chaque service de la police.

2. ENJEUX

Pour la police, l'enjeu principal tient à l'impact d'un accès non autorisé à des informations sensibles protégées et par conséquent, à son image, à sa propre réputation mais également à celle de l'Etat. Toutefois au-delà de ce risque d'image, il peut y avoir des conséquences en termes de responsabilité juridique puisque la police est responsable des données confidentielles de l'Etat et des citoyens qu'elle détient.

À ces enjeux s'ajoutent l'attractivité de l'information policière et l'intérêt des médias pour les affaires de police. Comme facteur aggravant, il sied de rappeler la curiosité de certaines personnes autorisées à accéder à l'information et la possibilité de monnayer l'information.
Certes, la violation du secret de fonction est sanctionnée, mais les conséquences d'une violation du secret de fonction ne sont pas toujours facilement rattrapables.

Les risques de fuite par une personne autorisée à manipuler l'information ou de vol par une personne externe, non autorisée à accéder à l'information, doivent être pris en charge de manière efficace et rapide.

3. DELAI

Dans la mesure où cette directive vise à limiter l'accès aux informations lors d'affaires sensibles, toutes les actions doivent être réalisées rapidement, sans délai. L'atteinte des objectifs de haute confidentialité dépend fortement de la célérité avec laquelle la sensibilité de l'affaire est détectée par les primo intervenants sur l'affaire et les mesures d'urgence exécutées.

4. DEFINITIONS

Dans la présente directive, on entend par :

- **évènement** : tout fait ayant donné lieu à une intervention ou une action de la police;

- **affaire de police** : évènement ou intervention de police donnant lieu à une poursuite d'office, sur dénonciation, ou suite à un dépôt de plainte, et faisant l'objet d'une inscription dans le fichier central des affaires de police (P2K ABI affaires);

- **évènement ou affaire de police sensible** : tout évènement ou affaire de police traitant d'informations dont l'attractivité et la particularité sont telles que ces dites informations sont exposées à un risque élevé de fuite, de vol ou de divulgation. Est réputée sensible toute affaire de police dont l'évocation en public ou la connaissance par le public peut inspirer un sentiment de peur, de colère ou provoquer des troubles à l'ordre public;

- **données personnelles sensibles** : toutes les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles, la santé, la sphère intime ou l'appartenance ethnique, des mesures d'aide sociale, des poursuites ou sanctions pénales ou administratives;

- **niveau de protection** : un ensemble d'exigences destinées à assurer la protection d'une information ou d'une catégorie d'information et qui satisfait les besoins spécifiques du propriétaire ou du responsable du fichier; le niveau de protection détermine les mesures de protection et de contrôle à appliquer;

- **classification** : attribution d'un niveau de protection adapté à la valeur et à l'importance d'une donnée ou d'un bien détenu par une organisation, selon la directive transversale sur la classification des informations.

5. IDENTIFICATION D'UNE AFFAIRE SENSIBLE

Un évènement peut être sensible par nature ou devenir sensible en raison du contexte et/ou des circonstances de son avènement ou en raison de la qualité des personnes impliquées.

Sans être suffisant, le caractère sérieux (au sens de l'article 307 CPP) de l'évènement est également un indice à prendre en compte.

5.1. Affaires ou évènements sensibles par nature ou en raison du contexte et/ou des circonstances de l'évènement

Une affaire ou un évènement peut être sensible par nature pour au moins une des raisons ci-dessous :

- elle concerne la sécurité intérieure;

- elle peut alarmer la population ou susciter la crainte publique car révélant une menace réelle ou fictive (pollution, accident chimique, etc.) ou relevant de procédés de chantage ou une annonce fallacieuse d'un danger pour la vie, la santé ou la propriété;

- elle dévoile ou traite des informations stratégiques policières ou politiques, ou couvertes par des secrets spéciaux (fiscal, médical, etc.);

- elle concerne certains milieux extrémistes ou alternatifs violents;

- elle peut nuire à la réputation du canton ou de la Suisse ou porter durablement atteinte à des intérêts économiques privés ou publics protégés.

Les affaires sensibles par nature sont généralement régies par des dispositions légales spécifiques ou par d'autres directives police *ad hoc*. La présente directive ne sera alors applicable à ces affaires qu'à titre accessoire pour compléter les règles spécifiques.

Les circonstances dans lesquelles se produit un évènement peuvent également lui conférer un caractère sensible. Une affaire ordinaire peut devenir sensible lorsqu'elle survient dans un contexte ou des circonstances particulières.

5.2. Affaires sensibles en raison des personnes impliquées

Le caractère sensible d'une affaire doit être envisagé lorsqu'une au moins des catégories de personnes listées ci-dessous est directement concernée, que celle-ci soit lésée, auteure, complice ou témoin :

- un conseiller d'Etat, un magistrat du pouvoir judiciaire, un magistrat de la Cour des comptes ou un élu;
- un fonctionnaire titulaire de la force publique, notamment un policier ou un gardien de prison;
- un diplomate ou un haut fonctionnaire suisse ou étranger;
- un cadre administratif membre du corps de police;
- une personne particulièrement connue ou célèbre, notamment une personnalité politique ou médiatique;
- un dirigeant d'une entreprise particulièrement connue.

Le degré d'implication de la personne dans l'affaire et le motif de cette implication sont également à prendre en compte.

De même, l'âge de la personne, son état de santé ou son état physique peuvent, dans certaines circonstances, justifier le caractère sensible de l'affaire et doivent par conséquent être pris en compte.

6. ROLES ET RESPONSABILITES

6.1. Tout collaborateur de la police

Tout collaborateur de la police engagé dans une opération, une réquisition ou une intervention est tenu de prêter attention à l'existence ou non d'indices pouvant laisser présumer qu'il est en présence d'une affaire potentiellement sensible.

Il informe sans délai son supérieur immédiat de tout indice lui paraissant justifier du caractère sensible de l'affaire.

Lorsque le cas est soumis au Coms, le risque lié au caractère sensible de l'affaire doit être annoncé.

L'appréciation du caractère sensible doit s'effectuer pendant tout le déroulement de chaque affaire.

6.2. Autorité de décision

Le Coms décide selon son propre constat ou d'après les indices qui lui sont rapportés, du caractère sensible de l'affaire.

S'il décide que l'affaire est sensible, il ordonne les mesures urgentes et avise sans délai le :

- CDT.
- Chef EM.
- Chef OP.
- Chef Coms.
- Chef du service directement concerné selon la typologie de l'affaire.

7. MESURES GENERALES DE PROTECTION A PRENDRE

7.1. Renforcement du niveau de classification de l'information

Le niveau ordinaire de classification d'une affaire de police est, selon la directive transversale EGE-10-12, le niveau confidentiel.

Lorsque l'analyse des personnes impliquées et des circonstances de l'affaire justifie qu'elle soit qualifiée comme étant sensible, le niveau de classification est immédiatement relevé de confidentiel à confidentiel-renforcé (paragraphe 4.2. Directive transversale sur la classification des informations, EGE-10-12).

La qualification confidentiel-renforcé exige la prise de mesures immédiates de sécurisation des informations (photos, documents, etc.) telles que définies dans le tableau ci-dessous.

L'officier en charge de la procédure concernant les affaires sensibles s'assure du strict respect de ces mesures.

7.2. Mesures de sécurité

Accès à l'information	Stockage de l'information	Sécurisation des données	Diffusion	Traçabilité
Verrouillage et confinement de l'information à un cercle restreint et fermé d'autorités avec pouvoir de décision et de collaborateurs policiers et/ou administratifs affectés au traitement de l'affaire.	Chiffrement des informations. Pas de stockage sur support amovible. Pas de stockage des informations hors des moyens fournis par	Transfert vers les espaces sécurisés et suppression définitive de toutes les données après transfert. Effacement définitif	Strictement limitée au cercle restreint autorisé. Sécuriser les documents papier à communiquer (enveloppes sous scellée, valises à clé, etc.).	Enregistrement (log) systématique des accès et traitement de l'information. Journalisation des accès

Caviardage des informations si nécessaire. Extraction et suppression des images de vidéosurveillance le cas échéant.	l'Administration. Prohibition des BAL de service et utilisation exclusive des BAL personnelles en mode sécurisé et chiffrement des fichiers à joindre. Stockage dans l'**espace de stockage *ad hoc.***	des supports de données ou destruction des supports de données dans tous les cas où l'effacement définitif s'avère techniquement impossible.	Restreindre au minimum et maîtriser les copies effectuées. Chiffrement des informations lors de transfert de données. Prohibition de l'utilisation des BAL de service.	physiques aux locaux dédiés au traitement de l'affaire, le cas échéant.

Les mesures de sécurité ci-dessus sont appliquées aussi bien aux documents numériques qu'aux documents physiques, notamment à ceux au format papier.

7.3. Principes d'application des mesures

Ces principes s'appliquent à :

- une affaire en cours où la personnalité du prévenu ou de la victime impose un verrouillage total ou partiel des informations;
- une affaire ancienne où la personnalité du prévenu ou de la victime, devenue sensible suite à l'actualité, impose un verrouillage total ou partiel des informations.

Les mesures d'urgence à appliquer sont :

- créer un espace sécurisé dédié à l'affaire sensible et y stocker systématiquement toutes les données concernant l'affaire;
- réduire au strict minimum l'accès aux données sensibles telles que la photographie "détenu", le dossier de police et la fiche signalétique;
- pour toutes les données déjà saisies :
    - extraire les données sensibles des systèmes d'information et bases de données et les transférer dans l'espace de stockage *ad hoc* dédié à l'affaire;
    - supprimer les données dans les systèmes d'information et bases de données. Les données d'enquête provenant de la brigade en charge de l'affaire et des investigations de la BPTS sont également concernées par cette mesure. Ceci, en particulier pour les affaires anciennes où une récolte systématique des données doit être faite ou a été faite.
- Pour toutes les nouvelles saisies de données :
    - le responsable de l'enquête donne accès à l'espace sécurisé dédié à l'affaire sensible, aux collaborateurs directement concernés (nombre restreint) et uniquement à ces derniers;
    - toutes les données sont saisies dans l'espace sécurisé dédié à l'affaire et uniquement dans ce dernier.

7.4. Création d'un espace de stockage *ad hoc* dédié à l'affaire

La création et la gestion de l'espace dédié à l'affaire sensible sont régies par la procédure idoine.

8. SYSTEMES D'INFORMATION

Les personnes en charge du traitement de l'affaire doivent identifier tous les systèmes d'information où des données (fichiers, images, vidéos, etc.) peuvent être stockées.

L'environnement de production est principalement concerné, mais la vérification doit aussi porter sur les autres instances de chaque système d'information qui contiennent des données réelles, telles que l'instance de recette.

- Applications bureautiques :
    - Dossiers fichiers bureautiques standards (C:\ D:\ S:\ V:\).
    - Dossiers fichiers bureautiques spécifiques (BCI, GFT, BO, etc.).
- Bases de données bureautiques :
    - Fichiers FileMakerPro.
    - Bases de données Access ou OpenBase.
    - etc.
- Bases de données centralisées :
    - Applications SIRE (développement CCSIP).
    - RAD (développement OCSINir).
- Systèmes centraux (Clients-serveurs) :
    - P2K – JOURNAL.
    - P2K – ABI Affaires – Personnes.
    - P2K – TPAO.
    - BGS.
    - I/Netviewer (SAE).
    - Mercure.
    - etc.

L'extraction et le transfert de données sensibles contenues dans certains systèmes d'information ou bases de données feront l'objet d'une procédure séparée car elles :

- nécessitent l'intervention de personnel spécialisé (OCSIN, CCSIP, etc.);
- sont d'un accès très restreint.

Le personnel spécialisé doit être contacté dans le but :

- d'extraire les données sensibles et de les remettre à l'enquêteur afin que ce dernier les transfère dans l'espace sécurisé dédié à l'affaire sensible;
- de supprimer les informations sensibles de l'emplacement initial.

Chaque responsable d'application ou propriétaire de système d'information s'assure qu'un mode d'emploi indiquant la manière d'extraire, de transférer et, en cas de besoin, de supprimer les données, soit disponible et régulièrement mis à jour.

9. PROCEDURE DE MISE EN OEUVRE

Chaque entité de la police concernée, soit notamment la DIROP, la PI, la PJ, la POLPROX, POLROUT et POLSEC, applique la procédure affaires sensibles en veillant à respecter les particularités propres à chaque service.

Les services sont chargés de mettre à jour la procédure de mise en œuvre de cette directive affaires sensibles en fonction de l'évolution des systèmes d'information, de manière à continuer d'atteindre les buts visés.