Politique de Sécurité du Système d'Information (PSSI) du BIA

Version 1 du 24/09/2012

SOMMAIRE

1. Introduction

1.1 Contexte général

Afin de se mettre en conformité avec ses obligations légales, le BIA a décidé de protéger les données à caractère personnel dont il a la charge au travers la mise en œuvre d'un processus d'amélioration continue conforme aux recommandations de la norme ISO 27001.

Cette norme internationale définit les conditions et les directives d'établissement, de mise en œuvre, d'exploitation, de surveillance, de réexamen, de tenu à jour et d'amélioration d'un système de management de la sécurité de l'information (PSSI).

Ce document décrit l'approche stratégique retenue dans le cadre de la mise en œuvre de ce processus au sein du BIA et le champ d'applicabilité de la démarche.

1.2 Objectif de la Politique de Sécurité du Système d'Information (PSSI)

La Politique de Sécurité du Système d'Information (PSSI) a pour objectifs de :

- décrire les rôles et les responsabilités en matière de gestion et de protection des données à caractère personnel ;
- fournir des indications ou des instructions sur les règles et les principes que le BIA entend mettre en application pour assurer la protection des données à caractère personnel ;
- se mettre en conformité avec les obligations légales et notamment la loi du **8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel**, modifiée par la loi du 11 décembre 1998.

Ce document de référence intitulé « **Politique de Sécurité du Système d'Information (PSSI)** » du BIA est destiné à être diffusé à l'ensemble des acteurs du BIA impliqués directement ou indirectement dans la protection du patrimoine informationnel et des systèmes d'information.

1.3 Domaine d'application de la PSSI

Le domaine d'application de la PSSI du BIA s'applique au **traitement de données à caractère personnel des salariés, des clients du CT et des clients du PC,** automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.
Les autres données traitées par le BIA sont exclues du périmètre d'application de la présente Politique.

La politique et les principes généraux de la PSSI s'applique à :

- Tous les moyens (matériels, logiciels et structurels) qui contribuent à toutes les opérations ou tous les ensembles d'opérations portant sur des données à caractère personnel.
- Tous les personnels du BIA en tant qu'utilisateurs des moyens de traitements automatisés et les informaticiens du Bureau Central.
- Tous les partenaires, fournisseurs et intervenants externes dès lors qu'ils utilisent les système d'information du BIA, s'y connectent, y hébergent ou y gèrent des ressources, des systèmes ou des données.

Au titre de la présente PSSI, on entend par :

«personne concernée»: une personne physique identifiée ou une personne physique qui peut être identifiée, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne physique ou morale, notamment par référence à un numéro d'identification, à des données de localisation, à des identifiants en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

«données à caractère personnel»: toute information se rapportant à une personne concernée;

«traitement de données à caractère personnel»: toute opération ou ensemble d'opérations effectuée(s) ou non à l'aide de procédés automatisés, et appliquée(s) à des données à caractère personnel, telle(s) que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation du traitement, l'effacement ou la destruction;

«limitation du traitement»: le marquage de données à caractère personnel mises en mémoire, en vue de limiter leur traitement futur;

«fichier»: tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique;

«responsable du traitement »: Personne, autorité publique, service ou organisme qui détermine les finalités et les moyens de traitement de données à caractère personnel; Au BIA, il s'agit du Directeur Administratif.

«sous-traitant»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

«destinataire»: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication des données à caractère personnel;

«violation de données à caractère personnel»: une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière;

«données concernant la santé»: toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne ;

2. Rôles et Responsabilités

2.1 Engagement de la Direction du BIA

La non-application de la Politique de Sécurité du Système d'Information (PSSI) constitue une menace pour le bon fonctionnement du BIA, pour la qualité des services rendus à ses clients et vis-à-vis des obligations légales qui s'imposent au BIA. A ce titre, la responsabilité du BIA peut être engagée.

La Direction du BIA montre son engagement dans la démarche de protection des données à caractère personnel au travers des actions spécifiques de gouvernance suivantes :

- La nomination d'un **Responsable de la Sécurité de l'Information (RSI)** qui est le coordinateur qualité du BIA ;
- La nomination d'un **Conseiller** en **Sécurité Informatique** (CSI) en charge du management de la sécurité du système informatique du BIA qui est le chef de service du BIA ;
- La création d'un **Comité de Sécurité des Données (CSD)** composé des membres de la revue de direction qui se réunit au moins une fois par an.

La Direction du BIA montre également son engagement au travers des actions suivantes :

- L'affectation de **budget d'investissement et d'exploitation pluriannuel** pour renforcer les dispositifs de protection existants ;
- La participation active aux décisions et aux choix d'orientation stratégique en matière de protection des données à caractère personnel ;
- **L'affectation des ressources humaines** nécessaire à la mise en œuvre des dispositifs de protection ;
- L'appui des démarches de sensibilisation des personnels du BIA ;
- L'affectation des **ressources** qui ont pour rôle d'identifier et **de traiter les exigences légales** et réglementaires, ainsi que les **obligations de sécurité contractuelles**;
- La **vérification que le personnel** à qui ont été affectées les responsabilités définies dans la protection de l'information, **a les compétences nécessaires** pour exécuter les tâches requises.

2.2 Rôle du responsable de traitement ou du sous-traitant

Le responsable du traitement (Directeur Administratif) ou son sous-traitant adopte des règles internes et met en œuvre les mesures appropriées pour garantir que le traitement des données à caractère personnel sera effectué dans le respect des dispositions adoptées conformément à la présente PSSI.

Il met également en œuvre des mécanismes pour vérifier l'efficacité des mesures énoncées dans la PSSI et sous réserve de la proportionnalité d'une telle mesure, fait appel à des auditeurs indépendants internes ou externes pour procéder à cette vérification (voir PROCBIA12).

Le responsable du traitement (Directeur Administratif) ou son sous-traitant met en œuvre des mécanismes visant à garantir que, par défaut, seules les données à caractère personnel nécessaires aux finalités du traitement seront traitées.

Le responsable du traitement (Directeur Administratif) , lorsque une opération de traitement est effectué pour son compte, doit choisir un sous-traitant qui présente des garanties suffisantes de mise en œuvre des mesures et procédures techniques et organisationnelles appropriées, de manière à ce que le traitement soit conforme aux dispositions adoptées conformément à la présente politique et garantisse la protection des droits de la personne concernée.

La réalisation de traitements en sous-traitance doit être régie par un acte juridique qui lie le sous-traitant au responsable du traitement (Directeur Administratif) et qui prévoit notamment que le sous-traitant n'agit que sur instruction du responsable du traitement (Directeur Administratif), en particulier lorsque le transfert des données à caractère personnel utilisées est interdit.

S'il traite des données à caractère personnel d'une manière autre que celle définie dans les instructions du responsable du traitement (Directeur Administratif), le sous-traitant est considéré comme responsable du traitement à l'égard de ce traitement.

Le sous-traitant, ainsi que toute personne agissant sous l'autorité du responsable du traitement (Directeur Administratif) ou sous celle du sous-traitant, qui a accès à des données à caractère personnel ne peut les traiter que sur instruction du responsable du traitement (Directeur Administratif), ou s'il y est obligé par la législation en vigueur.

Lorsque la Commission de la Protection de la Vie Privée (CPVP) exerce les pouvoirs qui lui sont conférés, le responsable du traitement (Directeur Administratif) et le sous-traitant répondent à la CPVP dans un délai raisonnable au travers d'une procédure clairement établie au sein du BIA (via le RSI le coordinateur qualité). La réponse comprend une description des mesures prises et des résultats obtenus, compte tenu des observations formulées par la CPVP.

Le responsable du traitement (Directeur Administratif) ou le sous-traitant veille à ce que le RSI (le coordinateur qualité) soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel. Il veille également à ce qu'il soit doté des moyens d'accomplir les missions et obligations qui lui incombent de manière effective et en toute indépendance, et ne reçoive aucune instruction en ce qui concerne l'exercice de sa fonction.

3. Appréciation et Traitement des risques sur la vie privée

L'appréciation des risques qui s'applique sur le domaine d'application de la PSSI [article 1.3] s'appuie sur :

- Une **identification et une analyse des risques** consistant à :
  1. évaluer **l'impact** sur la vie privée qui pourrait découler d'une défaillance de la sécurité, en tenant compte des conséquences d'une perte de confidentialité, intégrité ou disponibilité des données à caractère personnel;
  2. évaluer la **probabilité** réaliste d'une défaillance de sécurité de cette nature au vu des menaces et des vulnérabilités prédominantes, des impacts associés à ces données et des mesures actuellement mises en œuvre;
  3. estimer les **niveaux de gravité des risques** encourus sur les données à caractères personnels;
- Une **identification des non-conformités** aux **exigences légales** et réglementaires auxquelles est soumises le BIA, en particulier toutes celles liées à la protection des données à caractère personnel.

Cette démarche est conforme aux recommandations de la CPVP et se traduit par :

- une **appréciation systématique des événements redoutés** concernant la vie privée,
- une **appréciation des menaces** qui peuvent conduire à ces événements redoutés uniquement dans les cas où leur gravité est jugée comme importante,
- un **choix de mesures** en fonction de chaque risque,
- cette réflexion fait l'objet d'une **grille d'analyse crée lors de la création de nouveaux traitements**.

L'annexe IV décrit les référentiels et les métriques retenus par le BIA pour l'appréciation des risques liés à la protection de l'information.

Tout risque identifié au travers de cette démarche est évaluée par la Direction du BIA qui procèdent aux arbitrages utiles et aux **choix de traitement des risques** en décidant d'appliquer des mesures appropriées et proportionnées au niveau de sensibilité des données (cf. point 4).

Toutes les non-conformités aux principes de la protection des données à caractère personnel énoncés à l'article 5 devront obligatoirement être refusées et traitées selon la PROCBIA9.

4. Niveau de sensibilité des données à caractère personnel

Les traitements de données à caractère personnel effectués par le BIA sont décrits dans une fiche signalétique individuelle, appelée **Fiche de Renseignement des Traitement (FRT**) maintenue à jour dans un registre public, qui **précise**, en autre, **le niveau de sensibilité des données** à caractère personnel traitées.

La classification de cette sensibilité est découpée en 4 niveaux :

- Niveau 1 - **Données publiques** : des données personnelles dont l'abus ne semble pas, en règle générale, avoir de conséquence particulière pour la personne concernée. Il s'agit par exemple du nom, du prénom, de l'adresse et de la date de naissance, pour autant qu'ils ne soient pas dans une relation sensible, ou alors d'informations qui apparaissent dans les médias.
- Niveau 2 - **Données privées** : des données personnelles dont l'abus peut affecter la situation économique ou la place dans la société de la personne concernée. Il s'agit par exemple de données relatives à la situation d'un salarié ou client, ou aux relations professionnelles.
- Niveau 3 - **Données personnelles confidentielles** : des données personnelles dont l'abus peut gravement affecter la situation économique ou la place dans la société de la personne concernée. Il s'agit par exemple de données relatives à la santé, de données sensibles ou de profils de la personnalité.
- Niveau 4 - **Données très sensibles** : des données dont l'abus peut mettre en danger l'intégrité physique ou la vie de la personne concernée. Il s'agit par exemple d'adresses d'hommes de liaison de la police, d'adresses de témoins dans certaines poursuites pénales ou d'adresses de personnes qui sont menacées suite à l'expression de leur opinion ou de leur appartenance religieuse ou politique.

Plus le niveau de sensibilité des données à caractère personnel est élevé, plus le niveau de protection assuré par des mesures spécifiques de sécurité est important.

En référence au cadre général de classification des informations (cf. matrice de classification en annexe II), les données à caractère personnel sont classifiées selon le schéma de classification :

- « Confidentiel » pour les niveaux de sensibilité 1 & 2,
- « Secret » pour les niveaux de sensibilité 3 & 4.

Cela signifie que les données à caractère personnel confidentielles et très sensibles (interne ou externe) sont considérées comme secrètes au BIA.

5. Principes relatifs aux respects des obligations légales

Les principes énoncés respectent la directive Européenne de 1995 modifiée en 2012

5.1 Principes relatifs aux modalités de traitement des données à caractère personnel

P1. Principe de Finalité

P1.1 : Spécification/Modification de la finalité

Le responsable du traitement (Directeur Administratif) ou son sous-traitant doit consigner le **but du 'traitement'** dans la **fiche signalétique du traitement** (cf. Annexe I) renseignée par le RSI (le coordinateur qualité) et maintenu à jour dans le registre des traitements de données à caractère personnel placé sous la responsabilité du RSI (le coordinateur qualité). Cette fiche signalétique est datée et signée par le responsable du traitement (Directeur Administratif).

La finalité du traitement est décrite dans un langage clair et facilement compréhensible par les personnes concernées.

Toute modification subséquente de la finalité initiale doit pouvoir être reconstituée, tout comme les actions informationnelles (publication officielle, nouveaux consentements, etc.) entreprises vis-à-vis des personnes concernées dans le respect des principes énoncés au chapitre 5.2.

P1.2 : Limitation d'utilisation

Le responsable du traitement (Directeur Administratif) ou son sous-traitant doit s'assurer que le traitement de données à caractère personnel reste dans le cadre du but (finalité) défini. Tout traitement de données qui va au-delà des buts spécifiés initialement représente un détournement de finalité.

Le RSI (le coordinateur qualité) procédera régulièrement à un contrôle de la finalité des traitements effectués par le BIA. Dans le cas ou un détournement de finalité est constaté, il en informera immédiatement le responsable du traitement (Directeur Administratif) ou son sous-traitant qui procédera, sans délai, aux corrections nécessaires.

Selon la gravité de détournement de finalité constatée, le RSI (le coordinateur qualité) avisera le Directeur Administratif du BIA et le Comité de Sécurité des Données (CSD) qui prendront les décisions qui s'imposent pour rétablir le traitement dans le but initialement annoncé. En outre, une information à destination des personnes concernées pourra également être réalisée dans le respect des principes énoncés à l'article 5.2.

P2. Principe de Proportionnalité

P2.1 : Pertinence des données collectées

Ne peuvent être traitées que les données absolument utiles et nécessaires (évitement et/ou minimisation de données) à l'accomplissement de la tâche ou à l'atteinte du but. Les données personnelles confidentielles et très sensibles (cf. article 4) doivent à cet égard faire l'objet d'une attention toute particulière et ne peuvent être collectées que si la finalité du traitement le justifie.

Les formulaires papiers ou informatisés de collecte des données à caractère personnel sont conçus pour ne collecter que les données strictement nécessaire à la finalité du traitement.

Les données à caractère personnel collectées inutilement au regard de la finalité du traitement doivent être détruites, à moins qu'il existe des obligations d'archivage ou de conservation. Le responsable du traitement (Directeur Administratif) s'assure que ce principe est respecté par tous ses sous-traitants.

P2.2 : Exactitude des données

Le responsable du traitement (Directeur Administratif) ou son sous-traitant doit s'assurer que les données à caractère personnel traitées sont correctes et doit prendre toute mesure appropriée permettant d'effacer ou de rectifier les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées.

Lorsque des données à caractère personnel sont collectées, des mesures raisonnables et des procédures sont mises en œuvre pour authentifier la personne concernée et valider la plausibilité des informations reçues.

Dans le cas de collecte de données au travers de formulaires informatisés, des contraintes adéquates (formats prédéfinis, etc.) dans les masques de saisie permettent d'éviter de nombreuses fautes de frappe ou autres mauvaises saisies.

Une donnée personnelle dont l'exactitude ne peut être assurée par des mesures raisonnables ne doit pas être collectée ou sera nécessairement révisée ou détruite après un certain laps de temps.

P2.3 : Durée de conservation des données

Dans les archives courantes et intermédiaires (informatisées ou papiers), les données ne sont conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées.

Avant la mise en œuvre du traitement, le responsable de traitement ou son sous-traitant précise, dans le cadre des dossiers de formalités préalables et dans la fiche signalétique du traitement, la durée de conservation des données.

Le responsable de traitement ou son sous-traitant établisse, dans le cadre de ses moyens d'archivage, et après validation de la Direction, des procédures aptes à gérer des durées de conservation distinctes selon les catégories de données qu'il collecte et soit en mesure d'effectuer, le cas échéant, toute purge ou destruction sélective de données.

P3. Principe de Licéité :

P3.1 : Motifs Justificatifs

Le responsable du traitement (Directeur Administratif) ou son sous-traitant qui traite des données à caractère personnel a besoin d'un motif justificatif, en d'autres termes, du consentement de la personne concernée, d'un intérêt prépondérant privé ou public ou d'une loi. Le motif justificatif ne vaut que pour le but indiqué par la loi.

Le consentement par la personne concernée n'est valable, que si elle exprime librement sa volonté, après avoir été dûment informée. En d'autres termes, le consentement doit être accordé en l'absence de toute contrainte directe ou indirecte, et sur la base d'une information objective et pertinente.

Lorsqu'il s'agit de données personnelles confidentielles ou très sensibles (cf. article 4), son consentement doit au surplus être explicite et le responsable de traitement doit vérifier l'absence de toutes contraintes directes ou indirectes, ainsi que la pertinence de l'information délivrée.

Le consentement est explicite, si la personne concernée a signé de manière autographe ou électronique le document informatif reçu.

P3.2 : Base légale

Le responsable du traitement (Directeur Administratif) ou son sous-traitant n'est en droit de traiter des données à caractère personnel que s'il existe une base légale. Lors du traitement de données très sensibles (cf. article 4), celui-ci doit être expressément prévu dans une base légale au sens formel.

Dans le cas où des données à caractère personnel sont rendues accessibles en ligne, le responsable du traitement (Directeur Administratif) ou son sous-traitant doit s'assurer qu'une base légale est prévu expressément. S'agissant de données très sensibles, un accès en ligne n'est autorisé que si une loi au sens formel le prévoit expressément.

P3.3 : Traitement des données par un tiers

Le traitement de données à caractère personnel peut être confié à un tiers, pour autant qu'une convention écrite ou la loi le prévoie, et que le mandant ait pris les mesures nécessaires pour que seuls les traitements que lui-même serait en droit d'effectuer, sont effectués. En plus, aucune obligation légale ou contractuelle de garder le secret ne doit l'interdire.

Le responsable du traitement (Directeur Administratif) ou son sous-traitant doit s'assurer que le tiers respecte strictement les obligations contractuelles sur lesquelles il s'est engagé et doit signaler sans délai au RSI (le coordinateur qualité) toute dérive constatée.

Pour s'assurer du respect des obligations contractuel, le responsable du traitement (Directeur Administratif) ou son sous-traitant peut demander au RSI (le coordinateur qualité) ou à un auditeur spécialisé d'effectuer un contrôle sur pièce et sur place ou un avis sur la situation constatée.

P4. Principe d'Enregistrement des fichiers

Le responsable des traitements est tenu de déclarer tous les traitements de données à caractère personnel et tous les fichiers associés au traitement au RSI (le coordinateur qualité) du BIA.

Le RSI (le coordinateur qualité) établi et gère un inventaire des traitements et des fichiers de données à caractère personnel relevant des régimes de la déclaration et de l'autorisation ainsi que les traitements de données à caractère personnel dispensés de déclaration par la CPVP.

Cet inventaire contient à minima les informations suivantes :

- les nom et adresse du responsable du traitement (Directeur Administratif) ou de son sous-traitant ;
- le nom et la dénomination complète du traitement ;
- la personne auprès de laquelle peut être exercé le droit d'accès ;
- la finalité du traitement et la durée de conservation des données collectées ;
- les niveaux de sensibilités de données à caractère personnel traitées ; les catégories de destinataires des données ;
- les catégories de participants au traitement, c'est-à-dire les tiers qui sont en droit d'introduire des données dans le fichier ou d'y procéder à des mutations ;
- Les principes de sécurité mis en œuvre pour assurer la sécurité des données.

5.2 Principes relatifs à la sécurité des données à caractère personnel

P5. Principe de Sécurité des données

Le responsable des traitements de données à caractère personnel (le Directeur Administratif) et ses sous-traitants mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir, compte étant tenu des techniques les plus récentes et des coûts liés à leur mise en œuvre, un niveau de sécurité adapté aux risques présentés par le traitement et à la sensibilité des données à caractère personnel à protéger.

En ce qui concerne le traitement automatisé de données, le responsable des traitements de données à caractère personnel (le Directeur Administratif) et ses sous-traitants mettent en œuvre, à la suite d'une évaluation des risques (cf. article 3), des mesures destinées à:

- empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle de l'accès aux installations);
- empêcher que des supports de données ne puissent être lus, copiés, modifiés ou enlevés par une personne non autorisée (contrôle des supports de données);
- empêcher l'introduction non autorisée de données dans le fichier, ainsi que toute inspection, modification ou effacement non autorisé de données à caractère personnel enregistrées (contrôle du stockage);
- empêcher que les systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle des utilisateurs);
- garantir que les personnes autorisées à utiliser un système de traitement automatisé de données ne puissent accéder qu'aux données sur lesquelles porte leur autorisation (contrôle de l'accès aux données);
- garantir qu'il puisse être vérifié et constaté à quelles instances des données à caractère personnel ont été ou peuvent être transmises ou mises à disposition par des installations de transmission de données (contrôle de la transmission);
- garantir qu'il puisse être vérifié et constaté a posteriori quelles données à caractère personnel ont été introduites dans les systèmes de traitement automatisé de données, et à quel moment et par quelle personne elles y ont été introduites (contrôle de l'introduction);
- empêcher que, lors de la transmission de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);
- garantir que les systèmes installés puissent être rétablis en cas d'interruption (restauration);
- garantir que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité).

Les mesures suivantes sont appliquées au traitement de données à caractère personnel en fonction de la sensibilité des données traitées et de l'appréciation des risques sur la vie privés qui aura été menée :

(Pour plus de détails voir le FOR47 « mesures concernant la sécurité de l'information »)

- **Organisation et aspects humains de la sécurité :**

Formation des utilisateurs	Contrat de confidentialité	Connaissance de la PSSI
Sensibilisation sur la sécurité	Engagement personnel	Veille et suivi juridique
Diffusion d'une charte	Formalisation de consignes	

- **Protection physique et de l'environnement**

Accès sécurisés des bureaux	Broyeurs de documents	Système de détection d'intrusion
Politique du bureau propre	Mise au rebus sécurisée des unités de stockages informatiques	Locaux techniques sécurisés : salles serveurs.
Identification des ordinateurs	Registre des accès aux locaux techniques sécurisés : salles serveurs.	Sécurisation des moyens de paiements
Vidéosurveillance	Sécurisation des impressions	

- **Sécurité des systèmes et applications**

Détection d'intrusion	Chiffrement des supports amovibles	Renforcement sécurité système
Segmentation physique du LAN	Chiffrement des disques durs	Renforcement sécurité PC
DMZ Internet	Chiffrement de la base de données	Contrôle d'intégrité des données
Lutte anti-virale	Redondance du réseau	Protection des fichiers bureautiques
Filtrage des flux (firewall)	Systèmes de secours	Suppression des résidus mémoires

- **Sécurisation logique des accès**

Authentification forte des utilisateurs	Authentification forte des partenaires	Registre à jour des droits d'accès
Authentification forte des informaticiens	Contrôle d'accès réseau	Authentification lors des échanges

- **Journalisation, traçage et analyse des accès**

Journalisation des accès internet	Traçabilité des accès de télémaintenance	Journalisation des accès aux systèmes
Traçabilité des opérations informatiques (administrateur)	Traçabilité des accès aux données	

- **Surveillance, revue et maintenance**

Audit technique systèmes et réseaux	Rapport annuel informatique
Tests intrusifs	Rapport annuel des métiers

- **Gestion des incidents et de la continuité**

Procédures d'alerte de la direction	Plan de gestion de crise	Tests de reprise d'activité
Sauvegarde des données	Plan de continuité d'activité	Tableau de bord des incidents
Systèmes de secours informatiques		

- **Sécurité des échanges de données**

Mise en place de VPN	Chiffrement des supports transmis
Chiffrement des fichiers émis	Envoi sécurisé des dossiers papiers

P6. Principe de journalisation et de traçabilité des opérations de traitement

Le responsable du traitement (Directeur Administratif) et chaque sous-traitant remplissent et actualisent les fiches de renseignements des traitements (FRT) qui comportent au moins les informations suivantes:

- le nom et les coordonnées du responsable du traitement (Directeur Administratif), ou de tout responsable conjoint du traitement ou de tout sous-traitant;
- les finalités du traitement;
- les destinataires ou les catégories de destinataires des données à caractère personnel;
- les transferts de données vers un pays tiers ou à une organisation internationale, y compris leur identification respective.

Le CSI s'assure que les principes de journalisation informatiques soient opérationnels et veille à ce que des relevés soient établis au moins pour les opérations de traitement suivantes: la collecte, l'altération, la consultation, la communication, l'interconnexion ou l'effacement. Ce principe de journalisation concerne à minima les données classifiées de niveau 3 et 4.

Pour la traçabilité, les relevés des opérations de consultation et de communication indiquent en particulier la finalité, la date et l'heure de celles-ci et, dans la mesure du possible, l'identification de la personne qui a consulté ou communiqué les données à caractère personnel. Les relevés sont utilisés uniquement à des fins de vérification de la licéité du traitement des données, d'autocontrôle et de garantie de l'intégrité et de la sécurité des données.

Le responsable du traitement (Directeur Administratif) et le sous-traitant mettent la documentation et les relevés à la disposition de la CPVP, à la demande de celle-ci.

P7. Principe de communication à la CPVP d'une violation de données

En cas de violation de données à caractère personnel, le responsable du traitement (Directeur Administratif) ou son sous- traitant en adresse notification, sans délai, au RSI (le coordinateur qualité) qui, selon le niveau de gravité de la violation, se chargera de la transmettre à la CPVP, si possible, 24 heures au plus tard après en avoir pris connaissance.

Lorsque la notification a lieu après ce délai, le responsable du traitement (Directeur Administratif) ou son sous-traitant fournit une justification (via le RSI, le coordinateur qualité) à CPVP, sur demande.

La notification doit, à tout le moins:

- décrire la nature de la violation de données à caractère personnel, y compris les catégories et le nombre de personnes concernées par la violation et les catégories et le nombre d'enregistrements de données concernés;
- communiquer l'identité et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;
- recommander des mesures à prendre pour atténuer les éventuelles conséquences négatives de la violation de données à caractère personnel;
- décrire les conséquences éventuelles de la violation de données à caractère personnel;
- décrire les mesures proposées ou prises par le responsable du traitement (Directeur Administratif) pour remédier à la violation de données à caractère personnel.

Le RSI (le coordinateur qualité) conserve une trace documentaire de toute violation de données à caractère personnel, en indiquant son contexte, ses effets et les mesures prises pour y remédier. La documentation constituée doit permettre à la CPVP de vérifier le respect des dispositions du présent article. Elle comporte uniquement les informations nécessaires à cette fin.

Les principes relatifs à la communication de la personne concernée par la violation de ses données à caractère personnel sont énoncés à l'article 5.3.

5.3 Principes relatifs au respect des droits de la personne concernée

P8. Principe de Transparence et d'Information de la personne concernée :

P8.1 : Bonne foi

Le responsable du traitement (Directeur Administratif) ou son sous-traitant doit s'assurer que le traitement de données à caractère personnel est accompli conformément au principe de la bonne foi. Il s'assure notamment que le traitement ne se fait pas de manière secrète, sauf, si une loi le prévoit expressément (dans un cadre judiciaire par exemple) et vérifier l'absence de contraintes ou d'éléments trompeurs.

Le responsable du traitement (Directeur Administratif) ou son sous-traitant doit également s'assurer que la personne concernée a été suffisamment informée de la manière et du but du traitement et qu'elle n'a pas été informée de manière fausse.

P8.2 : Reconnaissabilité

Le responsable du traitement (Directeur Administratif) ou son sous-traitant doit s'assurer que la collecte de données à caractère personnel, et en particulier les finalités du traitement, sont reconnaissables pour la personne concernée.

En cas de doute sur les finalités du traitement annoncées, la personne concernée pourra demander au responsable du traitement (Directeur Administratif) ou son sous-traitant des informations complémentaires selon les modalités prévues au principe 8 relatif au droit d'accès de la personne concernée.

P8.3 : Obligation d'informer

Le responsable du traitement (Directeur Administratif) ou son sous-traitant a l'obligation d'informer la personne concernée lorsqu'il collecte des données très sensibles la concernant, que la collecte soit effectuée directement auprès d'elle ou auprès d'un tiers dans le respect des principes énoncés au chapitre 5.2 de la PSSI.

La personne concernée doit au minimum recevoir les informations suivantes:

- l'identité du responsable du traitement (Directeur Administratif) ;
- les finalités du traitement pour lequel les données sont collectées;
- les catégories de destinataires des données si la communication des données est envisagée ;
- l'existence du droit de demander au responsable du traitement (Directeur Administratif) la rectification ou l'effacement de ces données, ou la limitation de leur traitement ;
- le droit d'introduire une réclamation auprès de la CPVP et les coordonnées de ladite CPVP.

Si les données ne sont pas collectées auprès de la personne concernée, le responsable du traitement (Directeur Administratif) ou son sous-traitant doit l'informer au plus tard lors de leur enregistrement ou, en l'absence d'un enregistrement, lors de leur première communication à un tiers.

Les modalités d'information des personnes prévues par le BIA sont les suivantes :

- Affichage dans les zones réservées au public,
- Mentions légales sur les formulaires de collecte de données à caractère personnel,
- Mentions légales dans les espaces d'e-administration du BIA,
- Mise à disposition du registre des traitements de données à caractère personnel sur le site web du BIA,
- Information orale lors de communications téléphoniques visant à collecter des données à caractère personnel

P8.4 : Communication en cas de violation de données

Lorsque la violation de données à caractère personnel est susceptible de porter atteinte à la protection des données à caractère personnel ou à la vie privée de la personne concernée, le responsable du traitement (Directeur Administratif) ou son sous-traitant, après avoir procédé à la notification prévue à l'article 5.2 (article P6), communique la violation sans retard indu à la personne concernée.

La communication à la personne concernée décrit la nature de la violation des données à caractère personnel et contient au moins les informations et recommandations prévues à l'article 5.2 (article P6).

La communication à la personne concernée d'une violation de ses données à caractère personnel n'est pas nécessaire si le responsable du traitement (Directeur Administratif) ou son sous-traitant prouve, à la satisfaction de la CPVP, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données à caractère personnel concernées par ladite violation. De telles mesures de protection technologiques doivent rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

La communication à la personne concernée ne peut être retardée, limitée ou omise que pour des motifs explicitement énoncés par la CPVP ou par une loi.

P9. Principe de Droit d'accès et de procédure

P9.1 : Droit d'accès à ses propres données

Le responsable du traitement (Directeur Administratif) ou son sous-traitant est tenu de répondre à toute personne qui lui demande si des données la concernant sont traitées par le BIA.

Il doit mettre en place des outils de recherche permettant de retrouver toutes les données traitées concernant la personne faisant valoir son droit d'accès.

Le responsable du traitement (Directeur Administratif) ou son sous-traitant doit être en mesure de soumettre les informations à la personne concernée selon une procédure communiquée à la personne concernée.

Il doit enfin communiquer toutes les données concernant le demandeur qui sont contenues dans le traitement de données à caractère personnel et les fichiers associés et notamment :

- les finalités du traitement;
- les catégories de données à caractère personnel concernées;
- les destinataires ou les catégories de destinataires auxquels les données à caractère personnel ont été communiquées, en particulier lorsque les destinataires sont établis dans des pays tiers;
- la durée pendant laquelle les données à caractère personnel seront conservées;
- la communication des données à caractère personnel en cours de traitement, ainsi que toute information disponible sur l'origine de ces données.

P9.2 : Droit d'opposition

S'il y a un traitement illicite ou si les données collectées sont excessives au regard de la finalité du traitement, la personne concernée peut faire valoir droit d'opposition au traitement de ses données à caractère personnel par le BIA.

Après les vérifications requises, le responsable du traitement (Directeur Administratif) ou son sous-traitant est dans l'obligation de répondre à la requête du demandeur sauf si une loi ou réglementation lui permet de conserver en l'état les données et les traitements qui y sont effectués. Dans ce cas, la personne concernée est tenu informé des dispositifs légaux ou réglementaires auxquels est soumis le BIA et les recours possibles que la personne peut engager.

P9.3 : Rectification ou effacement des données

Le responsable du traitement (Directeur Administratif) ou son sous-traitant traite des données personnelles et doit assurer la rectification des données inexactes, notamment sur requête de la personne concernée.

En exerçant son droit d'accès ou en accédant directement (en mode lecture) à ses propres données, la personne concernée peut découvrir que des données inexactes ont été collectées et/ou sont traitées par le responsable de traitement.

Elle peut alors demander que ces données soient rectifiées ou détruites ou que la transmission de celles-ci soit interrompue. Si ni l'exactitude, ni l'inexactitude des données ne peut être établie, le requérant peut demander leur marquage par mention de leur nature litigieuse. Il incombe au Responsable de Traitement de mettre en place les outils permettant la rectification, la destruction ou le marquage des données, de même que l'interruption de leur transmission s'il y a lieu.

Lorsque l'effacement des données est demandé par la personne concernée, le responsable du traitement (Directeur Administratif) ou son sous-traitant peut procéder au marquage des données à caractère personnel:

- pendant une durée permettant au responsable du traitement (Directeur Administratif) de vérifier l'exactitude des données, lorsque cette dernière est contestée par la personne concernée;
- lorsque les données à caractère personnel doivent être conservées à des fins probatoires;
- lorsque la personne concernée s'oppose à leur effacement et exige, à la place de cela, la limitation de leur utilisation.

Après les vérifications requises, le responsable du traitement (Directeur Administratif) ou son sous-traitant est dans l'obligation de répondre à la requête de la personne concernée sauf si une loi ou réglementation lui permet de conserver en l'état les données et les traitements qui y sont effectués. Dans ce cas, la personne concernée est tenu informé des dispositifs légaux ou réglementaires auxquels est soumis le BIA et les recours possibles que la personne peut engager.

6. Contrôle de conformité

Un **programme annuel d'audits et de contrôle de conformité** est planifié en tenant compte de l'état et de l'importance des processus et des traitements à auditer, ainsi que des résultats des audits précédents. Ce programme est placé sous la responsabilité du RSI (le coordinateur qualité).

Ces audits portent principalement sur :

- Le contrôle de la conformité aux exigences légales et à la PSSI,
- Le contrôle de l'efficacité des dispositifs de protection mis en œuvre pour assurer la protection des données à caractère personnel.

Les auditeurs sont sélectionnés pour leur objectivité et impartialité (notamment ils ne font pas partie des équipes opérationnelles de maitrise d'œuvre).

Les responsabilités et les exigences pour planifier, mener les audits, rendre compte des résultats et conserver des enregistrements sont définies dans une procédure documentée.

L'encadrement responsable du domaine audité doit assurer que des actions sont entreprises sans délai indu pour éliminer les non-conformités détectées et leurs causes.

Les résultats des audits sont signalés au responsable de traitement ou au sous traitant ainsi qu'au CSD qui prendront les décisions qui s'imposent en fonction de la gravité des non-conformités constatées.

7. Revue de direction

La PSSI est revue au moins une fois par an lors de la revue de direction.

Des modifications peuvent également y être apportées en cours d'année notamment en cas d'évolution de la réglementation.

Les éléments d'entrée et de sortie de la revue sont précisés dans le manuel qualité général .

8. Mesures en cas de manquements

Les défauts de conformité à cette politique pourront, selon les circonstances, être considérés comme une faute professionnelle.

Les cas d'infraction à la présente politique commis par un membre du personnel seront traités par son responsable hiérarchique, en conformité avec le règlement intérieur local et les dispositifs prévus par la législation.

Le Directeur Administratif est responsable de l'application des sanctions proportionnées à la faute établie.

9. Modifications

Le CSD valide périodiquement la Politique de Sécurité du Système d'Information (PSSI) du BIA et autorise tout changement dans les objectifs stratégiques.

Dès que les amendements sont approuvés, le manuel électronique « Politique de Sécurité du Système d'Information (PSSI) du BIA » est mis à jour et ces amendements sont mis en évidence.

Date d'approbation : 24/09/2012

Rédaction	Contrôle	Evaluation et Approbation
T.RAMARD (AGERIS) Pour accord, le CQ	CQ	La direction BIA

ANNEXE I : Fiche de Renseignement d'un Traitement (FRT)

Fiche de renseignement des traitements de données à caractère personnel			FRT_01
Identification du traitement			
Traitement	Finalité du traitement	Responsable du traitement	Processus concerné par le traitement
N° Déclaration du traitement			
Nature des données collectées			
Personnes concernées			**Classification des données**
Type de données collectées			**Données Privées**
Destinataire des données (externe)			
Durée de conservation		Durée d'archivage	
Information des personnes et respect du droit d'accès			
Moyens d'information des personnes			
Contact pour exercer son droit d'accès			
Sécurité des données			
Stockage des données (support informatique ou papier)			
Appréciation des risques	Evènements redoutés		Vraisemblance

Annexe II : Schéma de classification des informations du BIA

Le tableau ci-dessous décrit les niveaux de classification des informations par critère de sécurité.

	Disponibilité	Intégrité	Confidentialité	Traçabilité / Preuve
	NON CRITIQUE Une indisponibilité temporaire est acceptable, ou une indisponibilité momentanée est tolérée, mais doit être signalée. Elle est sans conséquence sur le service fourni.	**NEGLIGEABLE** Toute perte d'intégrité doit être signalée et corrigée.	**PUBLIC : 1** Les informations peuvent être consultées en externe. **INTERNE : 2** Les informations peuvent être lues par tous en interne.	**PREUVE NON NECESSAIRE** Les traces sont faibles et non immédiatement disponibles.
	CRITIQUE Les informations doivent toujours être fournies pour remplir le service attendu. Leur indisponibilité peut entrainer des dysfonctionnements important des activités du BIA.	**IMPORTANT** L'information doit rester intègre durant la période d'utilisation. Toute perte en dehors de cette période doit être signalée et corrigée.	**CONFIDENTIEL : 3** Les informations sont protégées par le devoir de réserve et l'obligation de discrétion. Seuls des personnels et destinataires externes clairement identifiés et habilités peuvent accéder aux informations.	**PREUVE AUDITABLE** Fourniture d'une preuve opposable (mais contestable). Les traces sont complètes et sont immédiatement disponibles. Elles permettent de remonter à l'origine des incidents.
	TRES CRITIQUE Les informations doivent être accessibles en permanence et utilisables par tous les services concernés. Les conséquences d'une indisponibilité peuvent être très grave pour le BIA tant en terme de services rendus, qu'en terme d'image voire financier.	**ESSENTIEL** Les informations sont certifiées intègres pendant toute leur durée de vie ou période de validité. Une perte d'intégrité n'est pas acceptable.	**SECRET :4** Les informations sont protégées pendant toute leur durée de vie ou leur période de validité et sont protégées par le secret professionnel.	**PREUVE EXTERNE** Fourniture d'une preuve incontestable. Les traces sont complètes, immédiatement disponibles et protégées pour conserver leur intégrité et sécurité. Elles peuvent être utilisées dans le cadre d'investigations judiciaires.

ANNEXE III : Liste des obligations légales et règlementaires

- Directive 95/46/CE du Parlement Européen et du Conseil du 24/10/1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractères personnel et à la libre circulation de ces données.
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).
- Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité, adoptées sous la forme d'une Recommandation du Conseil de l'OCDE lors de sa 1037ème session, le 25 juillet 2002.
- Projet de Directive du Parlement Européen et du Conseil du 25/01/2012 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.
- Loi du 08/12/1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (M.B., 18 mars 1993) - Version consolidée (01/08/2007).
- Loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins
- Loi du 13 juin 2005 relative aux communications électroniques
- CCT N° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électronique en réseaux.
- Convention Vie Privée signée entre le BIA et le GOCA le 24/05/2006.

ANNEXE IV : Référentiels et métriques d'appréciation des risques

Liste des évènements redoutés :

Fuite de données sur internet
Perte ou vol de support amovible
Perte de données lors d'un échange électronique
Perte ou vol des données chez le partenaire
Vol de matériel informatique dans les locaux
Perte ou vol de documents écrits
Intrusion informatique
Cyber-attaque
Altération ou destruction par un virus informatique
Fishing (récupération de données par abus de confiance)
Erreur utilisateur
Erreur de l'informaticien
Accès illicite aux données (usurpation d'identité)
Acte de malveillance interne
Acte de malveillance par un prestataire
Modification accidentelle des données
Destruction accidentelle des matériels

Seuils de vraisemblance :

Faible
Moyenne
Elevée
Très élevée

Métrique d'appréciation des risques (issue de la norme ISO 27005 – annexe E) :

Métrique de calcul de la vraisemblance d'un scénario d'incident :

Vraisemblance de la menace	Faible			Moyenne			Élevée		
Niveaux de vulnérabilité	F	M	E	F	M	E	F	M	E
Valeur de la vraisemblance d'un scénario d'incident	0	1	2	1	2	3	2	3	4

Vraisemblance de la menace : Déterminé dans les fiches FRT

Métrique de calcul du niveau de risques encourus :

Valeur de l'actif	0	1	2	3	4
Valeur de la vraisemblance					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Valeur de l'actif : C'est la classification générale de toutes les informations du BIA. Voir annexe 2.

Valeur de la vraisemblance : résultat du tableau précédent.

Risque faible : 0-2	
Risque moyen : 3-5	
Risque élevé : 6-8	