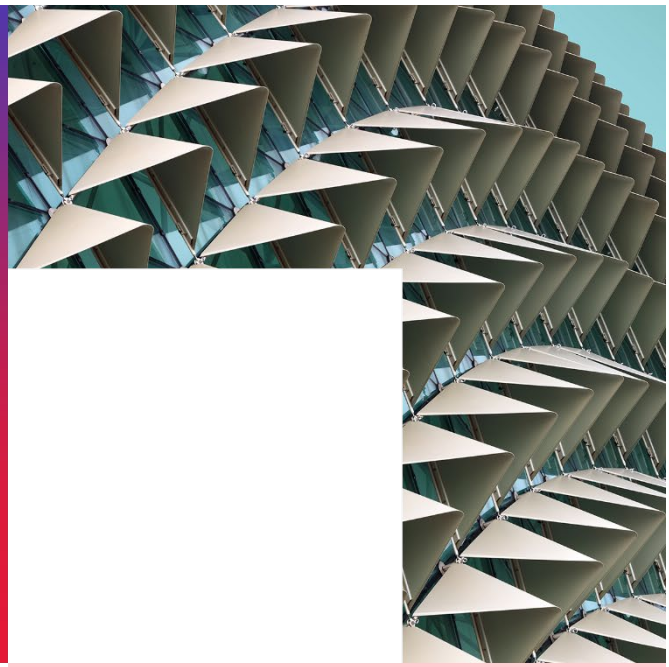


BCR-C – CGI Responsable du Traitement
Annexe G – Norme sur l’analyse d’impact relative à la protection des données

1. OBJET

L'adoption des BCR-C par CGI et l'engagement des Entités CGI à se conformer aux BCR-C démontrent que CGI a l'intention d'offrir un niveau élevé de protection aux Données à Caractère Personnel qu'elle Traite.

Le présent document décrit comment une Entité CGI, en tant que Responsable du Traitement, mettra en œuvre une procédure d'analyse de l'impact sur la protection des Données à Caractère Personnel, principalement à titre préventif, pour s'assurer que son Traitement des Données à Caractère Personnel est conforme à la Législation Applicable en matière de Protection des Données et aux meilleures pratiques en la matière. Le présent document a été élaboré en tenant compte des lignes directrices en vigueur publiées par les Autorités de Contrôle et les organismes internationaux de normalisation.

Cette procédure permettra à CGI de :

- Déterminer quel Traitement est susceptible d'engendrer un risque élevé pour la protection des Données à Caractère Personnel ;
- Evaluer le degré de conformité du Traitement qu'elle met en place avec la Législation Applicable en matière de Protection des Données ;
- Evaluer le niveau de risque pour les droits des personnes physiques associé au Traitement (gravité, probabilité) ;
- Déterminer les mesures correctrices à mettre en œuvre afin que les Données à Caractère Personnel soient Traitées conformément aux lois applicables et de manière à atténuer les risques ;
- Approuver ou de rejeter le Traitement en tenant compte des risques résiduels.

2. DÉFINITIONS

Les termes utilisés aux présentes avec des majuscules ont la même signification que dans les BCR-C.

Analyse d'impact relative à la protection des données (« AIPD ») : processus global d'identification, d'analyse, d'évaluation, de consultation, de communication et de planification du traitement ou de la gestion des impacts potentiels sur la protection des données en ce qui concerne le Traitement des Données à Caractère Personnel.

3. PORTÉE

Lorsque CGI est le Responsable du Traitement, CGI effectuera une AIPD pour les Traitements nouveaux et existants :

a) Lorsque les droits et libertés des personnes physiques sont à risque élevé ;
b) Lorsque le Traitement n'a pas déjà fait l'objet d'une autre AIPD reflétant un ensemble similaire d'instructions de Traitement ;
c) Pour atténuer l'impact d'un produit technologique pour lequel CGI détient la propriété intellectuelle, s'il y a lieu sur le plan commercial ;
d) Lorsque les politiques internes de CGI exigent une AIPD pour atténuer le risque et assurer la conformité à la Législation Applicable en matière de Protection des Données.

Ces critères sont décrits plus en détail à l'Annexe A.

Lorsqu'elle agit en qualité de Sous-Traitant, CGI peut être tenue par ses clients de coopérer et de fournir des renseignements pertinents pour leur permettre de mener une AIPD. CGI doit fournir à ses clients toute l'information pertinente dont elle dispose **tout en s'assurant qu'elle ne fournit pas de conseils juridiques dans le cadre de l'analyse d'impact qui demeure l'entière responsabilité du client**. Les lignes directrices de la présente procédure peuvent également être appliquées lorsque CGI contribue à une AIPD axée sur le client lorsque CGI est ou sera un Sous-Traitant. Dans ce cas, il est important de garder à l'esprit que l'exécution d'une AIPD est un projet en soi et nécessite du temps et des ressources. Par conséquent, son coût doit être discuté avec le client.

4. MÉTHODOLOGIE

❖ À QUELLE ÉTAPE DU CYCLE DE VIE DU PROJET CGI RÉALISERA-T-ELLE UNE AIPD ?

L'AIPD est l'un des éléments essentiels des principes de la protection des Données à Caractère Personnel dès la conception et par défaut. Elle englobe le développement du système, les activités et les processus manuels de soutien.

Les risques et les mesures d'atténuation doivent être déterminés et abordés avant le début du Traitement.

Toutefois :

a) l'industrie reconnaît par principe que plus les exigences sont déterminées tôt dans le cycle de vie, plus leur mise en œuvre est rentable ;

b) pour établir plus précisément le coût d'un projet, les mesures d'atténuation doivent être prises en compte avant que des engagements financiers importants soient pris à l'égard du projet, de sorte que l'AIPD initiale doit être effectuée le plus tôt possible dans le cycle de vie du projet et examinée à des étapes clés, p. ex. au moment de la proposition ou du démarrage du projet, dans le cadre de la conception du système, avant l'approbation et la mise en œuvre de la solution ;

c) une AIPD doit évoluer avec le système et les processus. Il ne s'agit pas d'un exercice ponctuel ; il faut donc le reproduire en cas de changement du profil de risque en matière de protection des Données à Caractère Personnel, p. ex. un changement aux données recueillies, l'introduction de différentes technologies, un changement d'utilisation des données, la divulgation à différentes personnes, etc.

❖ QUI SERA RESPONSABLE DE L'AIPD ET QUI Y PARTICIPERA?

Le chargé de projet doit désigner et nommer une personne dûment qualifiée qui sera responsable de l'exécution de l'AIPD. Les compétences appropriées comprennent des compétences organisationnelles, la gestion des risques, la compréhension de la protection des Données à Caractère Personnel et la sécurité de l'information.

La personne responsable de l'approbation de l'AIPD sera :

- pour les projets locaux et régionaux – le dirigeant de l'Unité d'Affaires avec l'approbation finale du président de l'UAS ;
- pour les projets régionaux – le président de l'UAS ;
- pour les projets corporatifs – le dirigeant des Services Corporatifs.

Les intervenants participeront à l'AIPD au besoin, en fonction de leur contribution potentielle, de leur influence et de l'impact du système. Ils peuvent comprendre :

- les équipes opérationnelles touchées (RH, Affaires juridiques, sécurité de l'information, Finances, communications et audit interne) ;
- la direction informatique ;
- les sous-traitants internes et externes et les partenaires commerciaux ;
- les spécialistes des systèmes, y compris les architectes et les concepteurs, les administrateurs de bases de données, les spécialistes de la sécurité physique et technique, les administrateurs d'ordinateurs ou de réseau, les exploitants d'applications et les exploitants d'ordinateurs ou de réseau ;
- l'équipe protection des données personnelles de CGI

Les responsabilités sont décrites plus en détail à l'Annexe B – Matrice RACI de l'AIPD.

5. EXTENSIBILITÉ

- Les droits des personnes physiques s'appliquent intégralement, quel que soit le niveau de risque du Traitement. Les organisations doivent adapter leur conformité en matière de protection des données (p. ex. exécution d'une AIPD) en fonction du niveau de risque que leurs opérations de Traitement des Données à Caractère Personnel posent pour les droits et libertés fondamentaux des personnes physiques.

- Les mesures de conformité et de responsabilité requises doivent tenir compte de **la nature, de la portée, du contexte et des objectifs du Traitement**, c.-à-d. une approche fondée sur le risque où les mesures d'atténuation sont liées aux particularités d'une opération de Traitement particulière.

- À cette fin, l'outil d'inventaire de traitement des données aide le responsable du projet à analyser les risques et détermine l'exigence d'effectuer une AIPD complète et, dans le cadre de cette dernière, l'évaluateur ou le coordonnateur de l'AIPD doit harmoniser les mesures de conformité au niveau de risque.

6. LE PROCESSUS D'AIPD

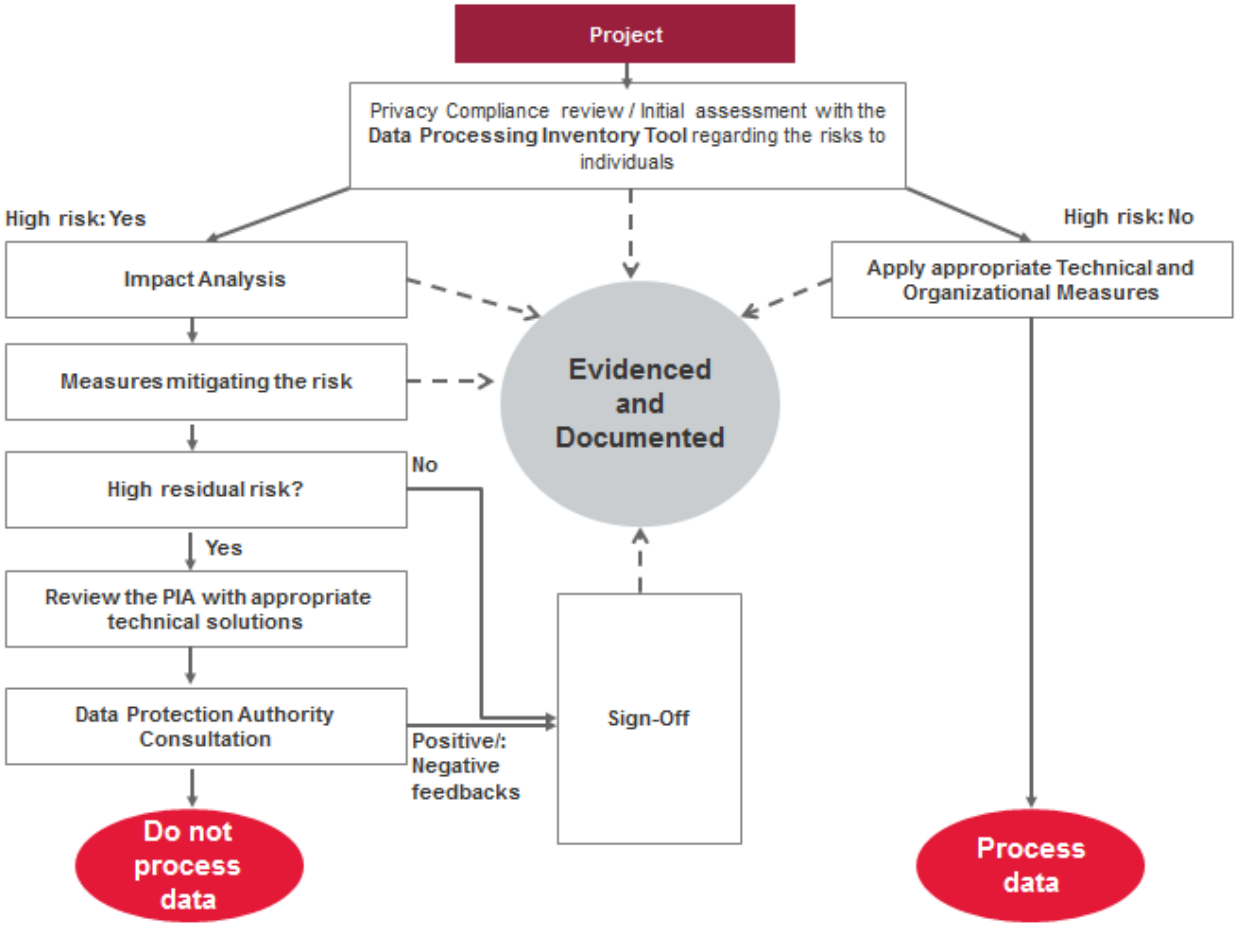


Figure 1 : Vue d'ensemble du processus d'AIPD

L'AIPD et les documents associés comprendront :

i. une description technique et fonctionnelle du Traitement et des flux de données ;
ii. la détermination des avantages que le Traitement apportera ;
iii. une comparaison du Traitement par rapport aux exigences en matière de protection des données du RGPD ;
iv. une analyse du risque lié à la protection des Données à Caractère Personnel ;
v. le plan d'atténuation des risques ;
vi. l'approbation de l'AIPD par le dirigeant de l'Unité d'Affaires ou des Services Corporatifs responsable ;
vii. un registre de l'exécution et des résultats de l'AIPD.

Le résultat de l'AIPD indiquera si le Traitement peut avoir lieu compte tenu des risques résiduels. Si les risques résiduels sont élevés, même une fois que les mesures d'atténuation sont appliquées, le Chef de la Protection des Données (CPO) doit être consulté, puis CGI peut choisir a) de refuser d'autoriser le Traitement ou b) de consulter l'Autorité de Contrôle pour obtenir son avis.

Dans de telles circonstances, le Traitement ne peut avoir lieu qu'après réception d'un avis positif de l'Autorité de Contrôle.

❖ SURVEILLANCE DE LA CONFORMITÉ AVEC L'AIPD

La conformité fait partie des trois lignes de défense de CGI (voir le processus d'audit de la protection des données personnelles de CGI). En plus des contrôles de l'Unité d'Affaires, ce régime de conformité permet de déterminer les domaines visés par un audit sur la protection des Données à Caractère Personnel, notamment :

a) « Planification de la gestion des Données à Caractère Personnel », qui comprend la conformité à la présente procédure d'AIPD;
b) « Intégration de la protection des Données à Caractère Personnel aux activités » pour garantir la mise en œuvre et l'efficacité des mesures d'atténuation définies dans l'AIPD.

❖ DIFFUSION DES RÉSULTATS

Lorsque CGI agit en qualité de Responsable du Traitement, elle met à la disposition des Personnes Concernées les informations précisées dans la section Transparence des BCR-C.

CGI protégera la confidentialité des documents de l'AIPD, mais l'Autorité de Contrôle pourra les obtenir sur demande.

❖ MODÈLE D'AIPD

Afin d'assurer l'uniformité de l'approche en matière d'AIPD, CGI fournit un modèle pour soutenir l'exécution de l'AIPD. Ce modèle doit être utilisé avec une adaptation minimale et seulement avec l'approbation préalable de l'équipe protection des données personnelles de CGI.

ANNEXE A : CRITÈRES DE DECLENCHEMENT D'UNE AIPD

Des AIPD sont requises lorsqu'il existe un « risque élevé » pour les droits et libertés des personnes physiques, c.-à-d. lorsque le Traitement des Données à Caractère Personnel est susceptible d'entraîner des « dommages physiques, matériels ou un préjudice moral ».

Voici une liste non exhaustive d'exemples de « dommages physiques, matériels ou préjudice moral » et d'opérations de Traitement qui pourraient entraîner de tels dommages et donc introduire un risque :

- Discrimination ou stigmatisation ;
- Atteinte à la réputation ;
- Préjudice corporel ;
- Dommages à la capacité de gain et pertes financières ;
- Vol ou usurpation d'identité ;
- Perte de liberté ou de liberté de mouvement ;
- Perte de confidentialité de Données à Caractère Personnel ;
- Effet dissuasif sur la liberté d'expression, d'association, etc. ;
- Peur, embarras, appréhension ou anxiété personnelle, familiale, professionnelle ou sociale ;
- Réduction des choix personnels ou intrusion dans la vie privée ;
- Renversement non autorisé de la pseudonymisation ;
- Personnes physiques privées de droits et libertés ou empêchées d'exercer le contrôle sur leurs données ;
- Tout autre désavantage économique ou social important.

Lorsque l'analyse initiale des risques indique qu'il est probable que l'un ou l'autre de ces risques se concrétise, il doit en être référé à l'équipe protection des données personnelles de CGI qui déterminera, en se fondant sur les lignes directrices, si une AIPD est requise.

- Le Traitement de Données à Caractère Personnel Sensibles, y compris des données sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale ; des données génétiques; des données biométriques, des données concernant la santé; des données concernant la vie sexuelle ; ou des données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes, étant entendu que le Traitement des Données à Caractère Personnel relatives aux condamnations pénales et aux infractions est interdit, sauf si ce Traitement est autorisé par le droit de l'EEE ou par le droit d'un Etat membre ;
- Le profilage au titre duquel les aspects personnels sont évalués pour créer ou utiliser des profils personnels (p. ex. analyser ou prévoir la performance au travail, la situation économique, la santé, les préférences ou intérêts personnels, la fiabilité ou le comportement, l'emplacement ou les mouvements) ou d'autres évaluations systématiques et approfondies des aspects personnels fondées sur un Traitement automatisé sur la base duquel sont prises des décisions produisant des effets juridiques comme l'exclusion ou la discrimination ;
- Le Traitement de Données à Caractère Personnel d'enfants et de personnes vulnérables ;
- Le Traitement de grands volumes de Données à Caractère Personnel concernant un grand nombre de personnes physiques ;
- La surveillance de comportements ou d'activités, particulièrement les activités en ligne et l'assiduité ;

- Le Traitement à l'aide de nouvelles technologies comme l'apprentissage profond et l'IA (p. ex. qui entraînent des conséquences personnelles et sociales inconnues) ;
- La surveillance systématique d'une zone accessible au public.

De plus, un risque peut survenir dans les cas suivants :

- Un nouveau « type » de Traitement des Données à Caractère Personnel est introduit alors qu'aucune AIPD n'a été effectuée (p. ex. « données massives ») ;
- Un délai important (deux ans) s'est écoulé depuis le début du Traitement et l'AIPD initialement réalisée ;
- Les opérations de Traitement ont été initiées avant l'adoption des présentes BCR-C et de la présente procédure ;
- Des risques pour les droits des personnes physiques (et ultimement pour les activités de CGI) découlent des situations suivantes :
    - collecte de Données à Caractère Personnel injustifiable ou excessive ;
    - utilisation ou stockage de données inexactes ou obsolètes ;
    - utilisation inappropriée ou usage abusif des Données à Caractère Personnel, y compris :
        a) l'utilisation des Données à Caractère Personnel au-delà des attentes raisonnables des personnes en faisant coïncider ou en combinant différentes opérations de Traitement ;
        b) l'utilisation inhabituelle des Données à Caractère Personnel au-delà des normes sociétales, lorsqu'une personne raisonnable dans ce contexte s'y opposerait ;
        c) une inférence ou une prise de décision injustifiable que l'organisation ne peut défendre objectivement ;
    - perte, vol, destruction ou altération de Données à Caractère Personnel ;
    - accès, transfert, partage ou publication de Données à Caractère Personnel injustifiables ou non autorisés ;
    - destruction, perte, altération accidentelle ou illicite, divulgation ou accès non autorisé à des Données à Caractère Personnel ;
    - L'opération de Traitement vise à empêcher des personnes physiques d'exercer un droit ou d'utiliser un service ou un contrat.

Toutefois, l'analyse initiale des risques pourrait révéler que la nécessité d'une AIPD doit être remise en question. Voici quelques exemples :

a) À la suite de l'analyse initiale des risques, si le Traitement est manifestement similaire à un ensemble d'opérations pour lesquelles il existe une AIPD récente et à jour, alors le dirigeant de l'Unité d'Affaires ou des Services Corporatifs responsable, en consultation avec le Chef de la Protection des Données (CPO), peut consigner la décision et la justification de ne pas reproduire l'analyse des risques (c.-à-d. l'AIPD).
b) Le Traitement utilise un produit technologique pour lequel une AIPD pertinente a été effectuée et fournie à CGI et couvre entièrement les circonstances de la mise en œuvre des produits au sein de CGI. Dans d'autres cas, une telle AIPD peut constituer, en adoptant les mesures d'atténuation pertinentes, une contribution importante à une AIPD complète effectuée par l'évaluateur.

Annexe B – Matrice RACI (responsabilité, approbation, consultation et information) de l'AIPD

Matrice RACI du processus d'AIPD							
R = responsabilité A = approbation C = consultation I = information	Chargé de projet	Évaluateur/ coordonnateur de l'AIPD	Propriétaire de contenu*	Equipe Protection des données personnelles de CGI	Chef de la direction informatique	Autres intervenants (veuillez préciser)	Remarque : * Il peut s'agir du dirigeant de l'UAS, de l'UA ou des Services Corporatifs détenant une responsabilité juridique
Examen préalable de la nécessité d'une AIPD	A/R		I	I			
Évaluation des résultats de l'examen préalable	A/R		C	C			
Nomination de l'évaluateur	A/R	C	I				
Gestion et documentation de l'AIPD	A	R					
Participation à l'AIPD	A/C	R	C	C	C	C	
Approbation des résultats de l'AIPD	C	C	A/R	C	C	I	* D'autres lois locales peuvent nécessiter une approbation officielle.

COMMUNICATION

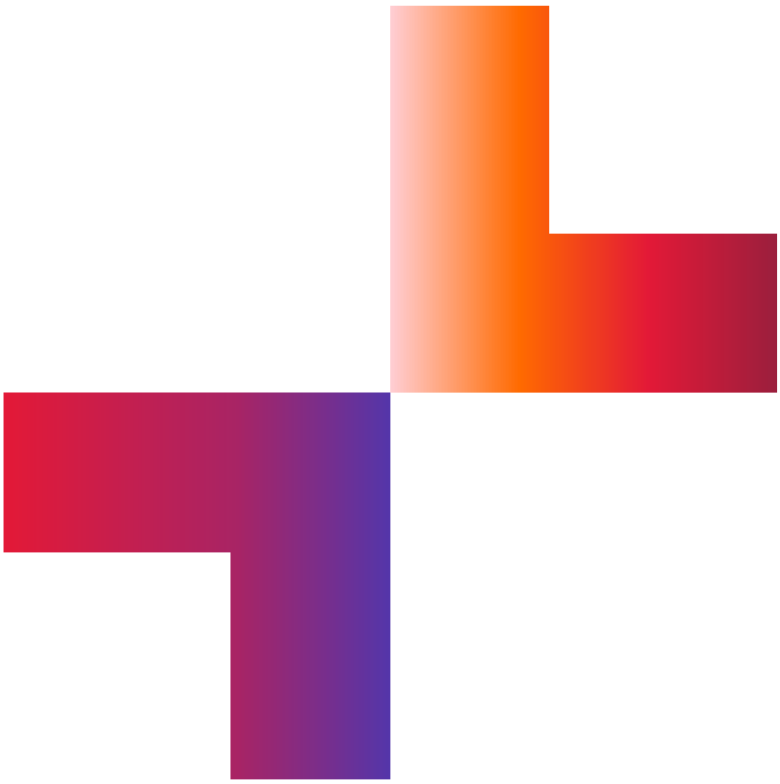
Toutes les demandes concernant ce processus doivent être adressées à privacy@cgi.com.

RÉFÉRENCES

RESPONSABLE DE LA POLITIQUE	AUTORITÉ APPROBATRICE
Chef de la Protection des Données(CPO)	Chef de la Protection des Données (CPO)

HISTORIQUE DES RÉVISIONS

VERSION	DATE	DESCRIPTION
1.0		Version initiale
1.1	Janvier 2020	Révision – Aucune modification
1.2	Mars 2021	Changement de titre de chef de la protection des données à chef de la protection des données personnelles
1.3	Novembre 2022	Révision annuelle - Pas de changement
1.4	Mars 2025	Revue annuelle – modifications textuelles ; mise à jour de l'email de contact
1.5	Juin 2026	Révision annuelle - Pas de changement



cgi.com