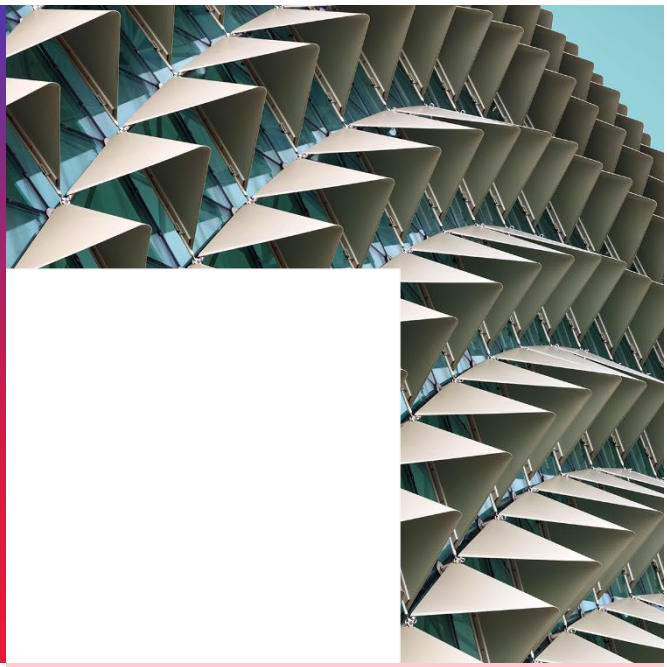


BCR-C – CGI Responsable du Traitement
Annexe C – Processus d'audit interne de la protection des données personnelles

1. INTRODUCTION

Les BCR-C de CGI et l'engagement des Entités CGI à se conformer aux BCR-C démontrent que CGI entend offrir un niveau élevé de protection des Données à Caractère Personnel qu'elle Traite.

Les BCR-C définissent un ensemble de principes et d'exigences qui s'appliquent au Traitement des Données à Caractère Personnel par CGI. Il incombe à CGI de veiller à ce que ces principes et exigences soient respectés au sein de l'organisation et, en particulier, de vérifier que les Entités CGI s'engagent à se conformer aux exigences et respectent cet engagement.

Dans ce contexte, le présent document définit la façon dont CGI vérifie ses Traitements de Données à Caractère Personnel afin d'évaluer la conformité aux BCR-C. Veuillez noter que les définitions des termes utilisés dans le présent document se trouvent dans les BCR-C.

2. OBJET

Le présent document couvre les audits effectués par CGI pour les Entités CGI concernant leur Traitement des Données à Caractère Personnel. Il ne s'applique pas aux audits que CGI peut effectuer pour des tiers ni aux audits effectués par des tiers pour CGI.

Les audits sur la protection des Données à Caractère Personnel visent à permettre à CGI de comprendre les pratiques utilisées par les Entités CGI lors du Traitement des Données à Caractère Personnel et leur conformité aux BCR-C de CGI.

Lorsqu'un audit sur la protection des Données à Caractère Personnel démontre qu'une ou plusieurs entités ne se conforment pas aux BCR-C, des mesures correctives seront déterminées et un plan d'action sera adopté.

3. PORTÉE

A. QUE PEUT-ON VÉRIFIER ?

CGI vérifie le Traitement des Données à Caractère Personnel des Associés de CGI, de son personnel, de ses sous-traitants, de ses fournisseurs et de ses clients.

Les secteurs suivants peuvent être pris en compte dans la portée d'un audit sur la protection des Données à Caractère Personnel :

i. Structure de gouvernance

- Rôles et responsabilités
- Politiques et normes
- Dérogations/exceptions aux BCR-C, conformément aux lois locales en vigueur
- Évaluations des risques liés à la sécurité d'entreprise et à la protection des Données à Caractère Personnel
- Formation et sensibilisation
- Conformité aux accords contractuels avec les clients et les tiers
- Surveillance des nouvelles lois et réglementations sur la protection des Données à Caractère Personnel

ii. Gestion des Données à Caractère Personnel

- Fonds de Données à Caractère Personnel (Traitées, consultées, transférées, hébergées) et dossiers d'inventaire
- Registres du mécanisme de transfert utilisé pour les flux transfrontaliers de données
- Mécanismes juridiques et matériels de transfert de données
- Légalité des finalités de Traitement
- Bases légales des Traitements (y compris l'harmonisation avec toutes les finalités du Traitement)
- Analyse d'impact relative à la protection des données
- Exigences en matière de conservation de données

iii. Intégration de la protection des Données à Caractère Personnel dans les opérations

- Obligations en matière de protection des Données à Caractère Personnel (p. ex. protection des Données à Caractère Personnel dès la conception) et droits (p. ex. réponse aux demandes et aux plaintes en matière de protection des Données à Caractère Personnel)
- Proportionnalité des Données à Caractère Personnel Traitées
- Respect des exigences de conservation des données
- Transparence et information fournie aux Personnes Concernées
- Gestion du consentement des Personnes Concernées
- Mesures de sécurité logique et physique en place pour protéger les données inactives/en transit
- Gestion et signalement des atteintes à la vie privée
- Autoévaluations de la conformité de la protection des Données à Caractère Personnel

Les audits sur la protection des Données à Caractère Personnel peuvent être ciblés localement, à l'échelle de l'entreprise ou par fonction. La cible appropriée doit être déterminée avant le début de l'audit et doit être expressément définie dans la note de service sur la portée, comme décrit ci-dessous.

Les audits sur la protection des Données à Caractère Personnel seront effectués par des auditeurs qualifiés de CGI qui seront appuyés par des experts, au besoin.

Les audits sur la protection des Données à Caractère Personnel peuvent être effectués des façons suivantes :

- **Audits non planifiés** : Couvrent certains points de conformité et pour une portée géographique limitée

- **Audits planifiés** : Couvrent la conformité générale aux BCR-C en fonction des critères suivants :

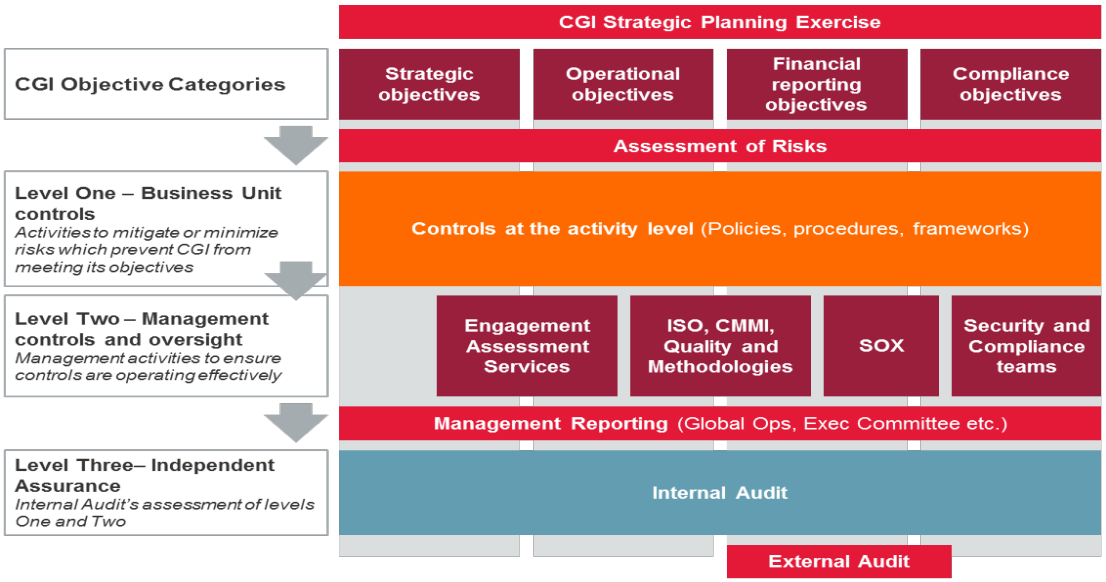
    - régions, entités ou fonctions limitées ;
    - contrats avec les clients.

B. QUI PEUT LANCER L'AUDIT ?

Les audits sur la protection des Données à Caractère Personnel peuvent être amorcés comme suit :

- En tant qu'audits non planifiés par l'équipe protection des données personnelles de CGI pour un Traitement particulier ou pour le déploiement du programme de protection des Données à Caractère Personnel ;
- Par l'équipe Audit interne et risques d'entreprise à des fins de gouvernance et de conformité aux BCR-C et au programme de protection des données personnelles ;
- Dans le cadre de la gestion du système qualité et du Cadre de gestion du partenariat client (CPMF) de CGI ;
- À la demande de la haute direction (p. ex. à la suite d'un incident préoccupant) ;
- Pour qu'un client ou une Autorité de Contrôle satisfasse aux exigences d'un organisme externe.

Le diagramme suivant définit les trois lignes de défense de CGI :



Le dirigeant de l'Unité d'Affaires ou des Services Corporatifs doit assumer un rôle de direction pour faciliter l'audit et s'assurer que les problèmes sont réglés en temps opportun.

C. FRÉQUENCE

Les audits sur la protection des Données à Caractère Personnel seront lancés comme suit :

- Au moins une fois par année pour les audits planifiés qui couvrent la conformité générale pour des régions, des entités ou des fonctions limitées ;
- Au moins tous les deux ans pour les audits mondiaux planifiés sur la protection des Données à Caractère Personnel qui couvrent la conformité générale aux BCR-C ;
- En tant qu'audits planifiés de conformité aux engagements en fonction des exigences d'échantillonnage précisées dans le manuel de gestion du système qualité.

Des audits sur la protection des Données à Caractère Personnel peuvent également être lancés comme suit :

- En tant qu'audits non planifiés dont l'objectif est déterminé par le Chef de la Protection des Données (CPO) ;
- Lorsqu'une Personne Concernée soumet une plainte ;
- Lors du lancement d'un nouveau projet.

Dans la mesure du possible, les audits sur la protection des Données à Caractère Personnel seront combinés aux audits sur la sécurité et la qualité. Les équipes d'audit feront part de leurs plans annuels pour optimiser la couverture et la valeur.

D. QUELS RENSEIGNEMENTS ET PROCESSUS PEUVENT ÊTRE VÉRIFIÉS ?

Les auditeurs doivent avoir accès à l'ensemble des documents et systèmes nécessaires pour effectuer l'audit. Ils doivent également être en mesure de mener des entrevues avec les entités auditées, au besoin, et peuvent effectuer des inspections des lieux non planifiées.

Les éléments de preuve suivants peuvent notamment faire l'objet d'un audit :

- Politiques, normes et procédures relatives à la protection des données ;
- Dérogations et exceptions aux BCR-C ;
- Avis de confidentialité ;
- Accords de collaboration inter-UA ;
- Inventaire de données ;

- Accords de transfert de données ;
- Accords/exigences contractuelles des clients ;
- Mesures de sécurité physique et logique en place pour protéger les Données à Caractère Personnel.

L'équipe d'audit peut visiter des services et des sites clés pertinents pour la portée de l'audit sur la protection des Données à Caractère Personnel.

E. MÉTHODOLOGIE

Lorsque des audits sur la protection des Données à Caractère Personnel sont effectués par des équipes établies de CGI, comme la fonction d'audit interne, la méthodologie de l'équipe s'applique. Toutefois, dans ces cas, l'équipe protection des données personnelles doit :

- Recevoir un avis d'audit sur la protection des Données à Caractère Personnel imminent ;
- Recevoir des rapports préliminaires avec la possibilité d'apporter des révisions et des commentaires ;
- Recevoir des copies des rapports d'audit définitifs ;
- Surveiller et valider la clôture des défaillances relevées lors des audits sur la conformité aux BCR-C.

Les sous-sections suivantes décrivent l'approche recommandée pour effectuer un audit sur la protection des Données à Caractère Personnel.

F. AVIS D'AUDIT

Lorsque CGI décide de lancer un audit sur la protection des Données à Caractère Personnel, les renseignements suivants doivent être documentés et communiqués avant le lancement de l'audit. Cet avis doit contenir, entre autres :

- Portée et objectifs de l'audit (matériel et géographique) ;
- Fonctions et rôles à interroger ;
- Quand, où et par qui ;
- Durée de l'audit ;
- Documentation, systèmes informatiques ou processus à examiner.

À moins que l'équipe protection des données personnelles de CGI n'en décide autrement pour un Traitement particulier, la note de service sur la portée doit être communiquée aux entités auditées et à la direction appropriée avant le début de l'audit sur la protection des Données à Caractère Personnel et, au plus tard, au début de la première entrevue. Aucune période de préavis minimale n'est exigée.

G. TRAVAIL D'AUDIT SUR LE TERRAIN

Pendant le travail d'audit sur le terrain, l'équipe d'audit doit recueillir suffisamment d'information pour tirer des conclusions pertinentes conformément aux processus appliqués par la fonction de l'équipe d'audit et, entre autres, par le biais d'échantillonnage d'éléments probants et d'entrevues. Aucune taille minimale/maximale d'échantillon n'est exigée. Toutefois, les exigences d'échantillonnage précisées à l'Annexe A du manuel de gestion du système qualité peuvent servir de guide. L'équipe doit s'efforcer de réduire au minimum les répercussions sur les activités quotidiennes.

L'audit peut prendre les formes suivantes :

- Questionnaire ;
- Examen de la documentation et des systèmes informatisés ;
- Inspection des lieux ;
- Entrevue ;
- Une combinaison de ce qui précède.

Des exemples de questions sont fournis à l'Annexe 1 pour illustrer le type de questions posées dans le cadre d'un audit sur la protection des Données à Caractère Personnel.

H. CONCLUSION DE L'AUDIT

À partir des observations et des informations recueillies, un rapport d'audit doit être rédigé. Le rapport doit inclure, sans s'y limiter, les éléments suivants :

- Objectif et portée de l'audit ;
- Documents, processus, systèmes informatisés examinés ou personnes interrogées ;
- Description du Traitement ou des procédures vérifiés ;
- Résumé du niveau de conformité des processus ou des systèmes informatisés vérifiés ;
- Causes principales de la non-conformité et recommandations ;
- Plans d'action convenus pour remédier aux observations de non-conformité ;
- Responsables du plan d'action et dates cibles de mise en œuvre.

Chaque ébauche de rapport d'audit, peu importe la portée de l'audit, doit être examinée par un Délégué à la Protection des Données qui validera les mesures correctives proposées et les échéanciers.

Une fois que le rapport, les défaillances et les mesures correctives ont été approuvés avec les entités auditées, le rapport d'audit final doit être distribué aux entités suivantes :

- Dirigeants de l'Unité d'Affaires ou des Services Corporatifs ;
- Responsables des processus/systèmes ;
- Chef de la Protection des Données (CPO) ;
- « Responsables des actions » ;
- Délégués à la Protection des Données locaux.

En l'absence d'accord sur les conclusions ou les mesures découlant de l'audit, le Chef de la Protection des Données (CPO) sera l'arbitre final.

I. SUIVI ET ESCALADE DU PLAN D'ACTION

Une fois que les mesures correctives et les délais sont définis, après confirmation par « les responsables des actions » que les mesures ont été prises, la fonction d'audit doit vérifier que les mesures sont effectivement mises en œuvre.

Un rapport d'étape doit être produit au moins à mi-chemin entre le début du plan de redressement et la fin prévue de la mise en œuvre afin de surveiller l'avancement des mesures de redressement. Si les progrès réalisés sont insuffisants ou si des dates cibles sont susceptibles de ne pas être respectées, la haute direction (dirigeant de l'UA) et le Chef de la Protection des Données (CPO) doivent en être avertis et déterminer les mesures à prendre pour résoudre les problèmes.

Au besoin, le Chef de la Protection des Données (CPO) peut transmettre le problème au Président de l'UAS et au « Vice-président exécutif, affaires juridiques et économiques, et secrétaire de l'entreprise ».

J. COMMUNICATION

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

K. RÉFÉRENCES

DOCUMENTS	EMPLACEMENT/RESPONSABLE
BCR-C	Services Corporatifs – Chef de la Protection des Données
Manuel de gestion du système qualité – Annexe A	Audit d'entreprise
Cadre de gestion du partenariat client (CPMF)	Assises de gestion de CGI

L. 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	Révision annuelle – modifications textuelles mineures ; mise à jour de l'email de contact
1.5	Juin 2026	Révision annuelle - Pas de changement

ANNEXE 1 : EXEMPLES DE QUESTIONS

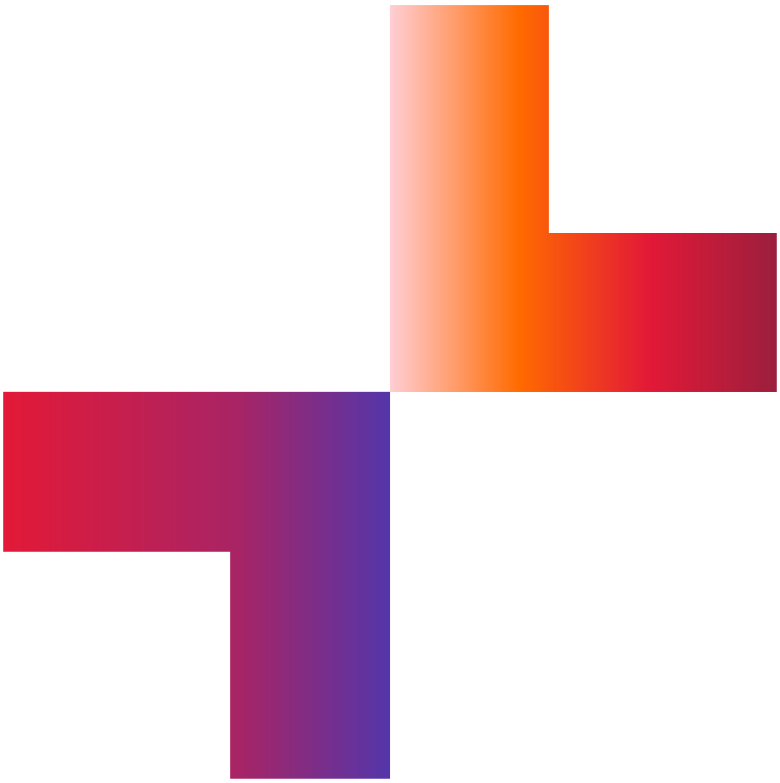
EXEMPLES DE QUESTIONS (série 1 – axée sur un Traitement particulier)

- Expliquez à quelles fins les Données à Caractère Personnel sont Traitées.
- Énumérez les Données à Caractère Personnel collectées à cette fin précise.
- De combien de temps votre équipe ou l'entreprise a-t-elle besoin pour Traiter les données ?
- À votre connaissance, pendant combien de temps les Données à Caractère Personnel sont-elles conservées ?
- Les Données à Caractère Personnel sont-elles partagées (soit pour l'hébergement, la maintenance ou la prestation du service) avec des tiers (c.-à-d. d'autres Entités CGI ou des fournisseurs de services externes) ?
- Si oui, les éléments suivants sont requis :
    - Fournir le nom de ces tiers.
    - Préciser les raisons pour lesquelles ils ont accès aux données.
    - Y a-t-il une clause de protection des données dans le contrat ou un accord concernant le Traitement des données avec ces tiers ?
    - Si oui, veuillez préciser et fournir des preuves.
    - Ces tiers sont-ils situés dans un autre pays ? Si oui, énumérez les pays où les données sont transmises ou d'où elles sont consultées.
- Si des Données à Caractère Personnel sont transférées ou consultées depuis des Pays Tiers, veuillez préciser à quelle fin ils ont besoin d'accéder à ces données.
- Avez-vous des accords contractuels avec les tiers? Si oui, veuillez fournir des preuves.
- Les Personnes Concernées ont-elles été informées du Traitement de leurs Données à Caractère Personnel? Si oui, veuillez fournir des preuves.
- Savez-vous si des formalités antérieures relatives à ce Traitement ont été réalisées auprès de l'Autorité de Contrôle compétente ? Si oui, veuillez fournir des preuves.
- Quels sont les engagements en matière de sécurité pris relativement à ce Traitement ? S'appuient-ils sur les politiques et les normes de sécurité des TI et de l'entreprise ? Dans la négative, veuillez préciser si les écarts ont été approuvés et documentés par l'équipe des TI/de sécurité de CGI.

EXEMPLES DE QUESTIONS (série 2 – axée sur la conformité générale)

- Une analyse d'impact relative à la protection des Données à Caractère Personnel a-t-elle été effectuée pour le Traitement des Données à Caractère Personnel ?
- Si oui, dans quelles conditions l'analyse est-elle effectuée ?
- Les Personnes Concernées sont-elles dûment informées du Traitement ? Si oui, comment sont-elles informées ?
- Une politique de conservation des données est-elle en place ?
- Si oui, veuillez fournir les renseignements suivants :
    - Comment surveille-t-on la mise en œuvre de cette politique de conservation ?
    - Des mesures de contrôle sont-elles en place pour assurer la mise en œuvre efficace de la conservation des données ? Si oui, précisez leur nature et fournissez des preuves.
- Comment obtient-on le consentement ?
- Comment surveille-t-on le consentement ?
- Comment surveille-t-on l'accès aux données ?
- Comment les transferts hors de l'Union européenne (UE) sont-ils surveillés ?
- Des clauses contractuelles types de l'UE ont-elles été signées pour les transferts de données ?
- Si oui, est-il facile d'en obtenir copie ?
- Une formation obligatoire sur la protection des données est-elle en place ?
- Si oui, veuillez fournir les renseignements suivants :
    - Quels sujets sont abordés ?
    - Quelle population reçoit cette formation ?
    - Précisez quels contrôles sont en place pour assurer la pleine participation. Fournissez des preuves.
- Des clauses de protection des données sont-elles définies dans les accords conclus avec les tiers ?
- CGI a-t-elle le droit d'empêcher un transfert vers un sous-traitant ultérieur ?
- Le rôle des parties respectives est-il expressément défini dans l'accord conclu avec les tiers (c.-à-d. quelle entité agit comme Responsable du Traitement ou Sous-Traitant ?)

- Lorsque CGI traite des Données à Caractère Personnel au nom de clients, les clients doivent-ils être informés du transfert aux sous-traitants ultérieurs ?



cgi.com