OBJET : cette procédure décrit les dispositions mises en œuvre pour traiter de façon efficace l'accueil d'un agent CNIL dans le cadre d'un contrôle, en application du Règlement Général sur la Protection des Données à caractère personnel (RGPD), par Total Marketing France (TMF) et ses filiales. Elle complète et précise la procédure d'accueil d'un agent CNIL initiée par le groupe Total et prend en compte les bonnes pratiques de la CNIL.

PERIMETRE D'APPLICATION ET CIBLE : cette procédure s'applique à toutes les activités de la société Total Marketing France et ses filiales. Les exigences qu'elle contient s'adresse à tous les collaborateurs impliqués dans le traitement de données personnelles et en particulier les responsables de traitements, les relais protection des données personnelles ou Data Privacy Liaison (DPL) et les délégués à la protection des données personnelles ou Data Protection Officer (DPO).

DATE D'APPLICATION : 01/07/2020

REVISION		Date d'application	N° version	Objet		
		09/07/2020	0	Création de la procédure		
			ENTITE	NOM	DATE	VISA
Circuit de validation	Métier	Rédacteur	FR/SG	Luc HOBON	09/07/2020	✓
	HSEQ	Vérificateur	FR/HSEQ/MEO	Pascal POTERALA	09/07/2020	✓
	Métier	Approbateur	FR/SG	Emmanuel de FOURNAS	09/07/2020	✓

DOCUMENTS REFERENCES :

- Règlement UE 2016/679 : Le règlement général sur la protection des données – RGPD
- Procédure Groupe : TOTAL RGPD 2018 – Fiche pratique guidelines accueil autorité de contrôle
- Procédure CR-MS-JUR-003 Consignes d'accueil des huissiers de justice et fonctionnaires habilités
- Procédure CR-MS-RH-001 FR Consignes Huissiers Fonctionnaires habilités
- Annexe 9 – CR-MS-RH-001 Lignes de conduite à adopter en cas d'accueil d'un agent de la CNIL
- Règle TMF : CR FR HSEQ 102 : « Actions correctives, Actions préventives (ACP) »

TABLE DES MATIERES

SIGLES ET DEFINITIONS :

Sigle / terme	Définition
Accountability	Principe majeur du RGPD impliquant que le responsable de traitement doit être en mesure à tout moment de démontrer sa conformité au RGPD
Autorité de contrôle de protection des données personnelles	Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du présent règlement, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union (CHAPITRE VI Autorités de contrôle indépendantes- Article 51 Autorité de contrôle)
BDPL	Branch Data Privacy Lead ou Coordinateur Branche Protection des Données Personnelles
CDPL	Corporate Data Privacy Lead ou Responsable Protection des Données Personnelles Groupe
CNIL	Commission Nationale de l'Informatique et des Libertés Il s'agit de l'autorité de contrôle en France. C'est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.
Contrôle	Il s'agit d'une enquête se déroulant chez un responsable de traitement (organisation), menée par une autorité de contrôle de protection des données personnelles de l'Union européenne. L'objectif du contrôle est de vérifier le respect par l'organisation de ses obligations réglementaires, lorsqu'elle met en œuvre des traitements de données personnelles.
Donnée personnelle	Toute information relative à une personne physique, identifiée ou identifiable, que celle-ci agisse à titre personnel ou professionnel
DPL	Data Privacy Liaison ou Relais Protection des Données Personnelles dans une entité
DPO	Data Protection Officer ou Délégué à la protection des données personnelles
Entité	Structure qui dispose d'une connaissance métier lui permettant d'opérer et de maitriser le traitement de données personnelles
Responsable de Traitement (RT)	Personne qui définit, seule ou conjointement avec d'autres, les finalités et les moyens du traitement de données personnelles. Il donne des instructions et contrôle le sous-traitant. Il est garant de la conformité RGPD de ses traitements et en particulier de la bonne exécution de cette procédure au sein de son entité.
RGPD	Règlement Général sur la Protection des Données à caractère personnel Le règlement n° 2016/679, dit Règlement Général sur la Protection des Données à caractère personnel (RGPD, ou encore GDPR, de l'anglais General Data Protection Regulation), est un règlement de l'Union européenne, directement applicable dans les Etats de l'UE, qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.
Registre de Traitement	Le registre des activités de traitement permet de recenser les traitements de données et de disposer d'une vue d'ensemble de ce que le responsable de traitement fait avec les données personnelles. Il permet notamment d'identifier : les parties prenantes ; les catégories, ...
Sous-traitant (ST)	Traite les données pour le compte et sous l'instruction du Responsable de Traitement
Traitement de données personnelles	Il s'agit de toute opération (ou tout ensemble d'opérations) effectuée à l'aide de procédés automatisés ou non et appliquée à des données personnelles. Tout traitement doit avoir une base juridique et une finalité déterminée préalablement au recueil des données et à leur exploitation.
Violation de données personnelles	Incident de sécurité entraînant (de manière accidentelle ou illicite) la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles (transmises, conservées ou traitées d'une autre manière), ou l'accès non autorisé à de telles données

1. PRINCIPES GENERAUX SUR LE CONTROLE CNIL

1.1. Rappel de l'article 58-1 du Règlement Général sur la Protection des Données (RGPD)

Chaque autorité de contrôle dispose de tous les pouvoirs d'enquête suivants :

a) Ordonner au responsable du traitement et au sous-traitant, et, le cas échéant, au représentant du responsable du traitement ou du sous-traitant, de lui communiquer toute information dont elle a besoin pour l'accomplissement de ses missions ;
b) Mener des enquêtes sous la forme d'audits sur la protection des données ;
c) Procéder à un examen des certifications délivrées en application de l'article 42, paragraphe 7[1] ;
d) Notifier au responsable du traitement ou au sous-traitant une violation alléguée du présent règlement ;
e) Obtenir du responsable du traitement et du sous-traitant l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'accomplissement de ses missions ;
f) Obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation et à tout moyen de traitement, conformément au droit de l'Union ou au droit procédural des États membres.

1.2. Qu'est-ce qu'un contrôle ?

Il s'agit d'une enquête se déroulant au sein d'une organisation (responsable de traitement ou sous-traitant), menée par une autorité de contrôle de protection des données personnelles de l'Union européenne, ci-après « autorité de contrôle ».
L'objectif du contrôle est de vérifier le respect par l'organisation de ses obligations légales et réglementaires, lorsqu'elle traite des données personnelles.

1.3. Origine d'un contrôle

L'autorité de contrôle peut déclencher un contrôle sans préavis et sans justification notamment à la suite de :

- une plainte ou une alerte d'un tiers même par lettre simple sur un sujet relatif aux données personnelles ;
- une mise en œuvre du programme annuel thématique des contrôles prévus par l'autorité de contrôle ;
- une mise en demeure de remédier à un manquement précédemment constaté ;
- une demande d'une autre autorité de contrôle de l'Union européenne ou dans le cadre d'une démarche conjointe ;
- toutes autres demandes.

1.4. Lieux des contrôles

Les contrôles physiques peuvent être réalisés dans les locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données personnelles à usage professionnel, à l'exclusion des parties affectées au domicile privé.

Des contrôles en ligne (sites internet, applications mobiles, etc.) peuvent également être réalisés à distance par les agents de l'autorité de contrôle.

1.5. Moment des contrôles

La réglementation nationale peut définir des horaires durant lesquels un contrôle est effectué. Il convient donc de vérifier les dispositions en vigueur dans le pays en question.

À titre d'exemple, en France, la CNIL doit commencer entre 6h et 21h, sans limite de durée légale (c'est-à-dire que le contrôle peut durer au-delà de 21h).

[1]Article 42-Certification du Responsable du traitement et sous-traitant

1.6. Les enquêteurs

Les enquêteurs sont des membres et / ou des agents d'une autorité de contrôle, accompagnés le cas échéant d'experts.

Le Règlement Général sur la Protection des Données prévoit notamment la possibilité de réalisation d'opérations de contrôle conjointes par plusieurs autorités européennes de protection des données. Une autorité de contrôle est en droit de participer à ce type d'opérations si un responsable du traitement dispose d'un établissement sur le territoire de l'Etat membre dont elle relève, ou si un nombre important de personnes concernées sont susceptibles d'être sensiblement affectées.

1.7. Opposition au contrôle

Les enquêteurs doivent informer, dès leur arrivée, le représentant des locaux (c'est-à-dire le chef d'établissement) ou son représentant de son droit d'opposition. L'usage abusif de ce droit peut être sanctionné pénalement, c'est le délit d'entrave. À titre d'exemple, en France, les sanctions encourues sont une peine d'un an d'emprisonnement et une amende de 15 000€ d'amende.

Le représentant des locaux ne peut s'opposer au contrôle déclenché à la suite d'une décision judiciaire. Elle est adoptée lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie. En fonction des pays, il est possible d'interjeter l'appel de cette ordonnance.

1.8. Pouvoirs des enquêteurs

Les enquêteurs n'ont pas le droit de fouille, sauf si une décision judiciaire les y autorise.

Ils peuvent copier tout document en relation avec l'objet de l'enquête, quel qu'en soit le support (papier, électronique), à l'exception des correspondances avocat-client et certains traitements intéressant la sûreté de l'Etat. Les données médicales[2] et documents classifiés « secret défense » font, quant à eux, l'objet de procédures spécifiques.

Les documents confidentiels peuvent-être copiés mais l'organisation doit néanmoins mentionner sur le procès-verbal le caractère confidentiel des documents en indiquant le fondement légal, la nature des données couvertes ou des fichiers concernés ainsi qu'une liste précise des documents concernés.

Les enquêteurs peuvent accéder aux programmes informatiques et aux données. Ils peuvent également en demander la transcription, par tout traitement approprié, dans des documents directement utilisables pour les besoins du contrôle.

Les enquêteurs peuvent demander à toute personne susceptible de leur fournir, dans les limites de l'objet du contrôle, des informations ou explications leur permettant de réaliser l'enquête sur place (disposition des locaux, organisation du système informatique, etc.).

Toutefois, les enquêteurs ne disposent pas du pouvoir d'apposer des scellés.

[2] S'agissant des données médicales, seul un médecin désigné par l'autorité de contrôle, peut consulter et copier ces données.

1.9. Droits de l'entreprise

- Se faire assister par un avocat, mais il ne s'agit pas d'une condition de validité de la visite.
- Faire consigner dans un procès-verbal tout élément important et toute réserve éventuelle.
- Ne pas s'auto-incriminer : l'entreprise peut refuser de répondre à une question qui l'amènerait à avouer directement sa participation à une infraction mais elle ne peut pas refuser de fournir des documents saisissables qui seraient incriminants.
- Si la visite a été autorisée par un juge : il est possible de le saisir à tout moment d'une demande de suspension ou d'arrêt.

1.10. Les décisions de l'autorité de contrôle

À l'issue du contrôle, l'autorité examine les copies des documents récupérées pour apprécier la conformité de l'entité à la réglementation sur la protection des données personnelles.

Elle peut alors prendre trois décisions.
- Envoyer un courrier de clôture du contrôle incluant d'éventuelles observations.
- Demander que soient prises des mesures de mise en conformité (sous forme de mise en demeure, d'avertissement, ou d'injonction).
- Prononcer des sanctions, après délibérations[3] (limitation, suspension ou interdiction du traitement, retrait d'une certification, amende administrative pouvant aller jusqu'à 10 ou 20 millions d'euros, ou jusqu'à 2 ou 4% du chiffre d'affaire mondial de l'entreprise en fonction du type de manquement constaté).

Remarque : En cas de manquement sérieux, l'autorité de contrôle peut également effectuer une dénonciation aux juridictions pénales si l'Etat membre dont elle relève a mis en place des sanctions pénales complémentaires.
De plus, les personnes concernées, victimes d'un dommage matériel ou moral, peuvent également demander des dommages et intérêts devant les juridictions de leur pays.

Il appartient donc aux entités de vérifier la législation applicable dans leur pays.

1.11. Les voies de recours contre ces décisions

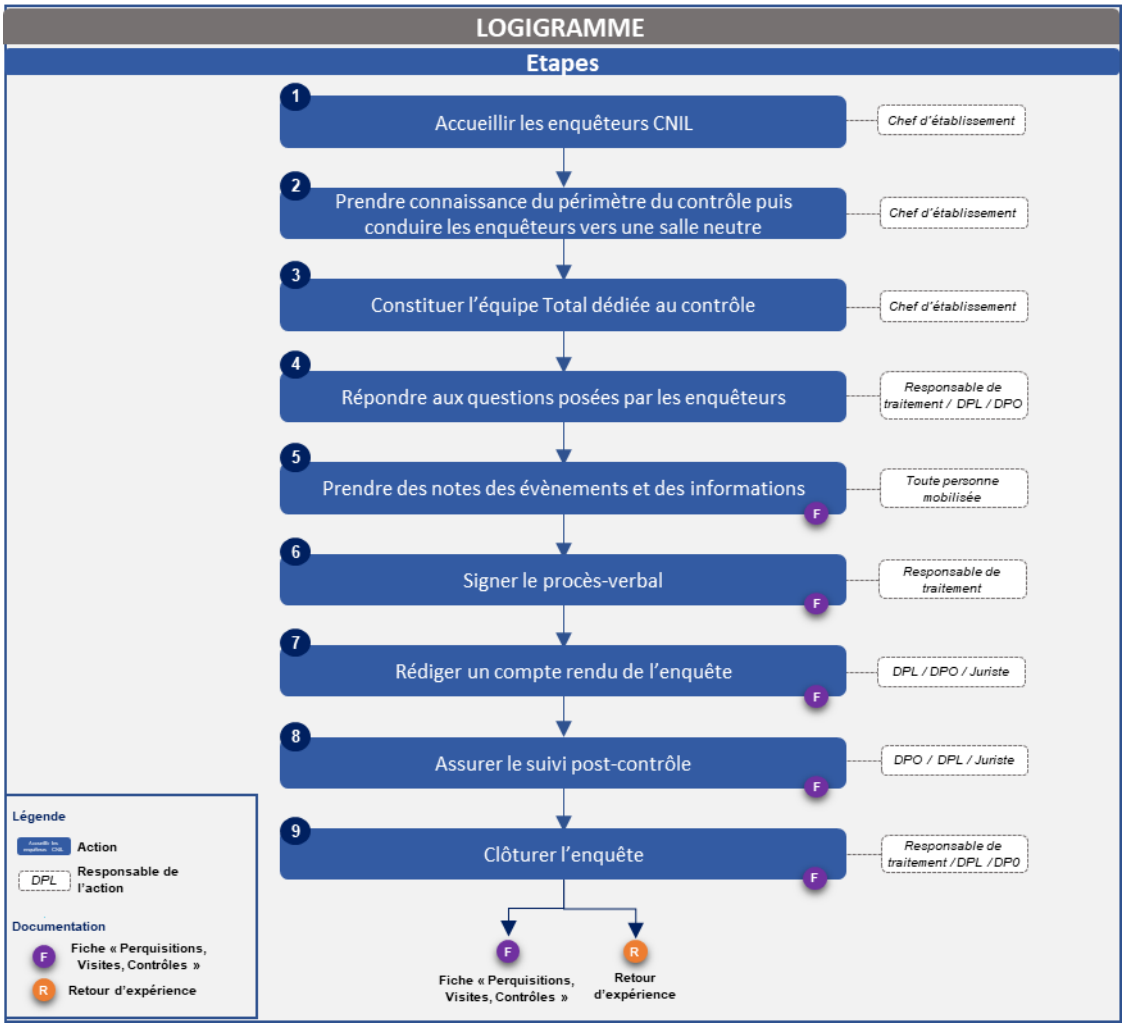
Il est possible de contester la décision d'une autorité de contrôle en formant un recours. Ce recours ne peut-être intenté que devant les juridictions du pays de l'autorité.
En France, par exemple, les décisions de la CNIL peuvent faire l'objet d'un recours devant le Conseil d'Etat en premier et dernier ressort.

[3] En France, le dossier est transmis à une formation spécifique, composée de six membres, appelée « formation restreinte », qui pourra décider de prononcer des sanctions.

2. GESTION DU CONTROLE CNIL

Le responsable de traitement est la personne qui définit les finalités et les moyens du traitement des données personnelles. Dans le cas de Total Marketing France, chaque membre du comité directeur est en charge du bon respect de la réglementation pour les activités de son périmètre de responsabilité.
Pour une filiale TMF, le directeur / la directrice de la filiale est en charge du bon respect de la réglementation pour les activités de son périmètre de responsabilité.

Le responsable de traitement désigne au sein de son entité la / les personnes en charge de répondre aux questions des enquêteurs dans le cadre d'un contrôle CNIL.
Chaque entité doit s'appuyer en interne sur un relais protection des données personnelles ou Data Privacy Liaison (DPL). Il est également important de solliciter le délégué à la protection des données ou Data Protection Officer (DPO) lorsque le responsable de traitement en a nommé un.



2.1. Etape 1 : Accueillir les enquêteurs CNIL

Le personnel de l'accueil de l'établissement doit être formé et connaître la possibilité d'un contrôle physique de la CNIL. Les enquêteurs peuvent aussi être accompagnés d'experts.

Extrait de la règle interne : CR-MS-RH-001 FR - Accueil des huissiers et des fonctionnaires habilités

Les Chefs d'Etablissements doivent s'assurer que l'accueil dans leurs Etablissements de tout huissier ou fonctionnaire habilité (dont l'enquêteur de la CNIL) *se fait dans des conditions permettant à ceux-ci d'accomplir la mission pour laquelle ils se présentent, le tout dans le respect des intérêts du M&S.*
A cette fin, les Chefs d'Etablissement doivent :

1. *connaître et maîtriser le contenu des annexes 1 à 10 de la règle interne CR-MS-RH-001 FR ;*
2. *assurer les rôles et fonctions qui leurs sont confiés à l'égard des personnels d'accueil présents au sein de leurs Etablissements.*
3. *assurer la mise à jour des informations fournies dans les listes des personnes à contacter en interne en cas de changement ;*
4. *connaître l'interlocuteur SI qui pourra intervenir ou être contacté en cas de besoin.*

Les Chefs d'Etablissements doivent s'assurer de la communication et de la parfaite connaissance des dix (10) recommandations de base par tout personnel d'accueil présent au sein de leurs Etablissements. En particulier, ils doivent veiller à ce que le prestataire-employeur des personnels d'accueil a bien été informé des consignes d'accueil en vigueur dans chaque Etablissement. Ledit Prestataire devra s'engager à remettre au personnel d'accueil, sur un support imprimé, lesdites consignes d'accueil.

1. *Les enquêteurs doivent être accueillis avec courtoisie.*
2. *Chaque enquêteur doit être prié de s'identifier par la présentation de son ordre de mission, pièces d'identité ou cartes professionnelles, ou tout autre titre justifiant de sa qualité.*
3. *Les nom, prénom, fonction, organisme / administration d'appartenance et pièces d'identité ou carte professionnelle présentée par tout enquêteur doivent être minutieusement reportés sur le registre d'accueil prévu à cet effet.*
4. *Il faut informer immédiatement la personne devant les recevoir selon la « Liste des personnes à contacter en interne »* (se reporter à l'annexe 1 de cette procédure). Appeler sur le téléphone fixe et le téléphone mobile.
5. *Si la première personne contactée en interne ne répond pas, ne pas laisser de message mais appeler sans délai la personne suivante dans la liste, et ainsi de suite jusqu'à établissement d'un contact.*
6. *Ne pas céder à la panique et garder son calme en toutes circonstances.*
7. *Après avoir eu le contact interne en ligne, il convient d'en informer les enquêteurs en leur précisant que cette personne arrive.*
8. *En attendant l'arrivée du contact interne, les enquêteurs doivent impérativement patienter à l'accueil.*
9. *Ne jamais communiquer d'information de quelque nature que ce soit aux enquêteurs, sans y avoir été préalablement autorisé par le contact interne.*
10. *Ne jamais signer un document, quel qu'il soit, qui serait présenté par les enquêteurs.*

2.2. Etape 2 : Prendre connaissance du périmètre du contrôle puis conduire les enquêteurs vers une salle neutre

À l'arrivée des enquêteurs sur site pour un contrôle, le chef d'établissement (ou par défaut le contact interne) est prévenu par l'accueil.
Le chef d'établissement (ou par défaut le contact interne), obligatoirement accompagné par un juriste ainsi que par le DPO, le cas échéant, doivent recevoir les enquêteurs.
En l'absence du chef d'établissement ou de son représentant, l'enquête peut avoir lieu en présence de deux témoins.

Bien qu'une première vérification ait été faite par l'accueil, le contact interne doit lui aussi vérifier avec l'aide du juriste les éléments suivants (essayer d'obtenir une copie ou si possible d'en faire une photocopie).

- L'ordre de mission des membres et / ou agents de l'autorité de contrôle.

Prendre le temps de lire attentivement le document afin de prendre connaissance de la mission.
Vérifiez que l'adresse indiquée dans les documents présentés est bien celle de l'établissement visité.

- La carte de service des membres et / ou agents de l'autorité de contrôle (noter les coordonnées des personnes).

Cette vérification est primordiale car elle permet de connaître les limites des pouvoirs des enquêteurs ainsi que les droits et obligations de l'entreprise.

Après cette vérification, le chef d'établissement (ou par défaut le contact interne) dirige les enquêteurs vers une salle, la plus neutre possible pour entamer le contrôle.

2.3. Etape 3 : Constituer l'équipe Total dédiée au contrôle

Le chef d'établissement (ou par défaut le contact interne) doit alors constituer l'équipe dédiée au bon déroulement du contrôle, à savoir notamment :
- le ou les responsable(s) de traitement concerné(s) par le contrôle ou à défaut leur(s) représentant(s) ;
- le Data Privacy Liaison (DPL) du périmètre concerné ;
- le Data Protection Officer (DPO) du périmètre concerné le cas échéant ;
- un (ou plusieurs) juriste de l'entité ou de la filiale concernée afin d'apporter son assistance dans la vérification les documents présentés par les enquêteurs, pour intervenir en cas de dépassement de leur mission par les enquêteurs, pour faire consigner dans un procès-verbal toute information importante et, d'une manière générale, pour prendre des notes sur les évènements et les informations ;
- un représentant de la DSI pour accéder aux outils informatiques.

L'équipe dédiée :
- doit rester calme et courtoise avec les enquêteurs et conserver une attitude neutre et professionnelle en toute circonstance ;
- ne doit pas laisser les enquêteurs circuler seuls dans l'établissement (il convient de mobiliser autant de personnes qu'il y a d'enquêteurs) ;
- doit rester présente jusqu'à la fin des opérations (contrôle et signature du procès-verbal) ;
- garder confidentielle la survenance d'une enquête (tant au sein de l'entreprise que vis-à-vis de l'extérieur).

L'équipe dédiée doit également informer le Branch Data Privacy Lead (BDPL) de la branche M&S et le Corporate Data Privacy Lead (CDPL) des circonstances du contrôle.

2.4. Etape 4 : Répondre aux questions posées par les enquêteurs

2.4.1. Mobiliser les interlocuteurs-clés

Le responsable de traitement doit trouver rapidement les bons interlocuteurs qui pourront répondre, aux questions principalement opérationnelles et techniques des enquêteurs de l'autorité de contrôle.

Afin de répondre de façon efficace aux questions des enquêteurs, le responsable de traitement doit expliquer en amont la nature et l'objet de l'enquête aux personnes interrogées, et s'assurer de leur coopération.

Les personnes interrogées doivent s'assurer que les questions posées ont un lien avec l'objet de l'enquête : il ne doit pas être répondu aux questions sans lien avec l'objet de l'enquête.

Enfin, le responsable de traitement doit indiquer aux personnes interrogées que leurs réponses doivent être factuelles, se limiter strictement aux questions posées, ne pas employer d'expression ambigüe ou non maîtrisée ; en cas d'incertitude, elles ne doivent pas hésiter à dire qu'elles ne savent pas, elles ne doivent pas formuler d'hypothèses.

2.4.2. Fournir aux enquêteurs les documents RGPD en lien avec l'objet du contrôle

Le responsable de traitement a l'obligation de fournir les informations, renseignements, pièces et documents qui seront demandés par les enquêteurs : registre des traitements, analyse d'impact relative à la protection des données (AIPD ou PIA en anglais), By Design, Binding Corporate Rules (BCR) signées, …). Si les documents demandés ne sont pas disponibles, demander un délai pour adresser ultérieurement lesdits documents.

Par ailleurs, il doit s'assurer que les documents copiés ont un lien avec l'objet de l'enquête : seuls ces documents sont saisissables (original ou copie, selon le type d'enquête). Il est préférable de fournir uniquement des documents photocopiés et non les originaux, si cela ne porte pas préjudice à la tenue de l'enquête.

Le représentant du responsable de traitement doit identifier et isoler :

- les correspondances avocats-clients : elles ne peuvent pas être saisies sauf s'il est avéré qu'elles ne participent pas à l'exercice des droits de la défense ;
- les documents comportant des secrets d'affaires ou des informations confidentielles : la mention de leur confidentialité est apposée sur les documents et dans le procès-verbal de saisie;
- les documents classifiés « secret défense » : le magistrat ou l'officier de police judiciaire doit les placer sous scellés fermés sans qu'aucun enquêteur n'en prenne connaissance ; seuls des personnes spécialement habilitées peuvent prendre connaissance de ces documents classifiés.

Enfin, le responsable de traitement doit conserver une copie des documents saisis ou copiés et s'assurer qu'ils sont bien répertoriés dans le procès-verbal de saisie (cf. 2.6. Etape 6 : Signer le procès-verbal).

Le responsable de traitement doit s'assurer que personne ne fasse obstruction à l'enquête : ne pas détruire, dissimuler aucun document, quel qu'en soit le support (papier / électronique).

Une attention particulière doit être portée à cette étape du contrôle, car elle est déterminante pour les conclusions et décisions de l'autorité de contrôle.

2.4.3. Assurer l'interface avec les enquêteurs CNIL

Le Règlement confère au Data Protection Officer (DPO) la mission de point de contact vis-à-vis de l'autorité de contrôle. En ce sens, il doit, lors d'une visite de contrôle s'assurer que les interlocuteurs nécessaires au déroulement du contrôle soient réunis et que les rôles soient bien répartis entre eux (tenue du chrono, recensement des différents documents copiés, etc.).

Le Data Protection Officer (DPO) peut le cas échéant, faire consigner par écrit tout incident dans le procès-verbal.

Dans le cas où il n'y a pas de Data Protection Officer (DPO), ces missions sont confiées au juriste ou à un avocat.

2.5. Etape 5 : Prendre des notes des évènements et des informations

Les personnes mobilisées doivent prendre des notes de tous les événements et informations relatifs à l'enquête auxquels elles assistent et dont elles ont connaissance : personnes interrogées, questions-réponses, locaux visités, liste des documents demandés, consultés, saisis ou copiés, mots-clés recherchés, incidents, etc. Ces notes doivent être neutres et sans commentaire personnel.

Pour la prise de notes, il est proposé d'utiliser la fiche « Perquisitions, Visites, Contrôles » élaborée par le Groupe (cf. Annexe 2).

2.6. Etape 6 : Signer le procès-verbal

Les enquêteurs dressent un procès-verbal : ils mentionnent la nature, la date, le lieu des investigations, les enquêteurs présents, les personnes concernées et leurs déclarations, les demandes formulées par les enquêteurs, les éventuelles difficultés ou motifs d'opposition rencontrés, les documents et pièces remis.

Le procès-verbal doit être relu avec attention et signé par le responsable du traitement. Pour la relecture, il doit se faire assister d'un juriste (ou d'un avocat, en l'absence de juriste), du Data Privacy Liaison (DPL) et du Data Protection Officer (DPO), le cas échéant.

L'objectif est de s'assurer qu'il est complet et qu'il ne dénature pas les évènements qui ont eu lieu (déclarations, incidents, documents saisis, interrogatoires ; les questions et les réponses doivent être inscrites.
Tenter d'obtenir la copie du procès-verbal. Si ce n'est pas possible, essayer de noter les éléments clés de ce dernier.

Si certains documents n'ont pas pu être fournis à l'issue du contrôle, il est possible de les communiquer par la suite au contact indiqué par l'autorité de contrôle.

2.7. Etape 7 : Rédiger un compte rendu de l'enquête

Après le contrôle, le Data Privacy Liaison (DPL) assisté d'un juriste et le Data Protection Officer (DPO) le cas échéant doivent :
- rédiger un compte-rendu factuel afin de centraliser toutes les informations collectées par les membres de l'équipe mobilisée et rappeler leur obligation de confidentialité quant à l'enquête ;
- transmettre toutes les informations collectées pendant l'enquête aux juristes en charge de suivre, par la suite, le dossier correspondant.

Le compte rendu de l'enquête est également diffusé :
- aux personnes mobilisées de l'équipe dédiée ;
- au(x) directeur(s) de l'entité du périmètre contrôlé ;
- au(x) directeur(s) général(aux) de(s) l'entité(s) juridique(s) ;
- au Branch Data Privacy Lead (BDPL) de la branche M&S et au Corporate Data Privacy Lead (CDPL).

2.8. Etape 8 : Assurer le suivi post-contrôle

Le Data Protection Officer (DPO) et à défaut le Data Privacy Lead (DPL), si aucun DPO n'a été désigné pour l'entité contrôlée doit assurer le suivi post-contrôle de la CNIL.

Il s'appuie sur les juristes en charge de suivre le dossier correspondant.

2.9. Etape 9 : Clôturer l'enquête

2.9.1. Actions correctives et préventives

En fonction des conclusions de l'enquête de la CNIL, le responsable de traitement s'assure que des actions correctives ont été identifiées et sont menées dans le respect du délai imposé par la CNIL.

En fonction des actions menées, il faut vérifier si d'autres traitements doivent également être adaptés (actions préventives) en cohérence avec la procédure « Actions correctives, Actions préventives (ACP) » (CR FR HSEQ 102).

Les personnes en charge de cette analyse sont :
- le responsable de traitement du périmètre contrôlé ;
- le Data Privacy Liaison (DPL) du périmètre contrôlé.

Le Data Privacy Liaison (DPL) est en charge de contrôler la bonne application du plan d'action. Il communique son suivi au Data Protection Officer (DPO).

Le Data Protection Officer (DPO) de Total Marketing France et ses filiales, communique lorsque c'est nécessaire, ces éléments aux autres DPL de son périmètre, pour qu'ils puissent mener à leur tour une analyse de leurs traitements, afin d'identifier et de mener les actions préventives nécessaires.

2.9.2. Retour d'expérience

Dans un objectif d'amélioration continue de la conformité au RGPD, le Data Protection Officer (DPO) assisté du Data Privacy Liaison (DPL) doit initier un retour d'expérience (REX).

Ce REX s'appuie sur les conclusions données par la CNIL et doit inclure :
- les éventuelles observations et bonnes / mauvaises pratiques relevées par l'autorité de contrôle ;
- les éventuels avertissements, injonctions ou mises en demeure ;
- les éventuelles sanctions prononcées ;
- une synthèse des actions correctives menées dans le périmètre concerné ;
- une synthèse des actions préventives menées dans le périmètre concerné ;
- une synthèse des actions préventives menées en dehors du périmètre concerné par le contrôle.

Il a pour objectif :
- d'entretenir la vigilance des collaborateurs à partir d'un exemple concret de contrôle ;
- d'informer les collaborateurs sur les causes immédiates et fondamentales qui ont conduit au contrôle et à ses conséquences ;
- de recommander des actions à mettre en œuvre dans le cadre de traitements de données personnelles similaires ou équivalents ;
- de garder la mémoire des évènements et de leurs enseignements.

Le Data Privacy Liaison (DPL concerné), doit tenir informer son Branch Data Privacy Lead (« BDPL »), ainsi que le Corporate Data Privacy Lead (« CDPL ») de la clôture du contrôle de la CNIL.

ANNEXE 1 : Liste des personnes à contacter en interne en cas de contrôle CNIL

La liste des personnes à contacter permet d'identifier et de contacter les personnes qui doivent participer à l'enquête CNIL.

* Etape 1 : Accueillir les enquêteurs CNIL

Liste par ordre de priorité	**Etablissement xxx**	**Téléphone**	**Mobile**
Chef d'établissement			
Back-Up 1			
Back-Up 2			
Juriste 1			
Juriste 2			
Juriste 3			
Data Protection Officer			

* Etape 3 : Constituer l'équipe Total dédiée au contrôle

Liste par ordre de priorité	**Entité ou Direction**	**Téléphone**	**Mobile**
Responsable de Traitement			
Back-up 1			
Back-up 2			
Back-up 3			
Back-up 4			
Data Privacy Liaison			
Juriste 1			
Juriste 2			
Juriste 3			
Data Protection Officer			

Chaque Data Privacy Liaison (DPL) doit assurer, au fil de l'eau en fonction des mouvements des personnes, la mise à jour de la liste des personnes à contacter dans son entité.

Le DPL réalise un point de contrôle tous les trimestres pour vérifier que cette liste est bien à jour et informe le Data Protection Officer (DPO).

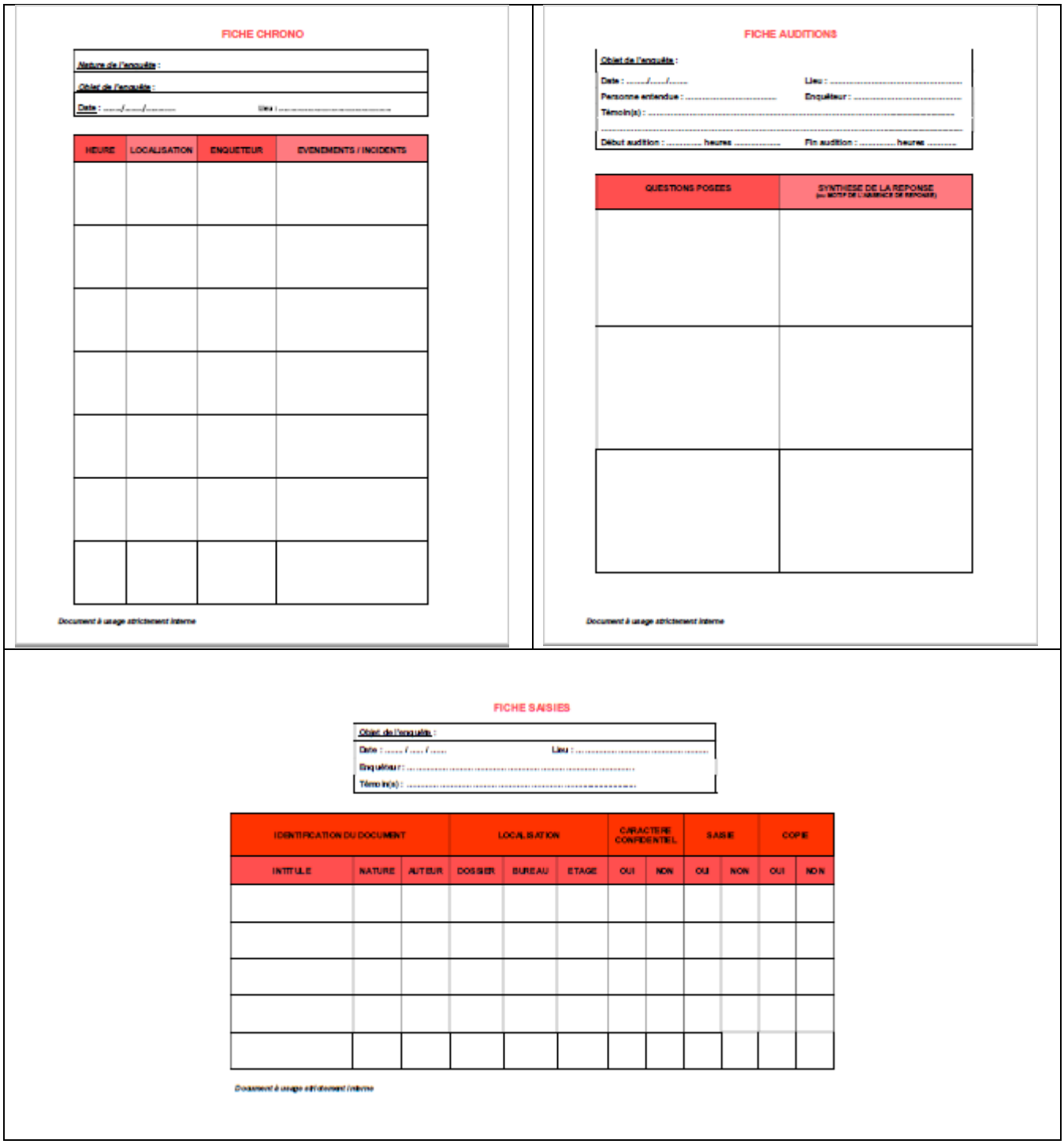
Chaque chef d'établissement doit transmettre, régulièrement et au minimum tous les trimestres, la dernière version à jour de « la liste des personnes à contacter en interne en cas de contrôle CNIL » à l'accueil de l'établissement.

Pour Total Marketing France, cette liste est référencée sous le sigle : « CR FR GOUV PDP 003 Annexe 1 ».
Ce document est disponible dans l'outil de gestion documentaire « NORMA » ou son successeur.

Pour les autres entités, il revient au Data Privacy Liaison (DPL) et au chef d'établissement de définir le processus de mise à jour et de transmission à l'accueil de l'établissement.

ANNEXE 2 : Fiche « Perquisitions, Visites, Contrôles »

Pour la prise de notes, il est proposé d'utiliser la fiche « Perquisitions, Visites, Contrôles » élaborée par le Groupe.



FICHE CHRONO

Nature de l'enquête :

Objet de l'enquête :

Date : ...../...../..... Lieu : .....

HEURE	LOCALISATION	ENQUETEUR	EVENEMENTS / INCIDENTS

Document à usage strictement interne

FICHE AUDITIONS

Objet de l'enquête :

Date : ...../...../..... Lieu : .....

Personne entendue : ..... Enquêteur : .....

Témoin(s) : .....

.....

Début audition : ..... heures ..... Fin audition : ..... heures .....

QUESTIONS POSEES	SYNTHESE DE LA REPONSE (ou MOTIF DE L'ABSENCE DE REPONSE)

Document à usage strictement interne

FICHE SAISIES

Objet de l'enquête :

Date : ...../...../..... Lieu : .....

Enquêteur : .....

Témoin(s) : .....

IDENTIFICATION DU DOCUMENT			LOCALISATION			CARACTERE CONFIDENTIEL		SAISIE		COPIE	
INTITULE	NATURE	AUTEUR	DOSSIER	BUREAU	ETAGE	OUI	NON	OUI	NON	OUI	NON

Document à usage strictement interne