DIRECTION JURIDIQUE

Groupe Verallia

Notification des violations de données à caractère personnel

Cette procédure est susceptible d'être mise à jour pour tenir compte, si besoin, des évolutions de la règlementation européenne.

Il est confidentiel et appartient au Groupe Verallia. Il ne peut être communiqué en tout ou partie à l'extérieur du Groupe Verallia - sauf pour répondre à une exigence légale ou réglementaire (communication dans le cadre d'un contrôle d'une Autorité de contrôle par exemple) ou après autorisation du Comité Conformité Groupe.

Suivi des modifications :

Version	Date	Auteur	Vérification	Approbation	Objet
V1.0	15/02/2021	Idea	Idea	Idea	Création

Table des matières

Introduction

Le Règlement général sur la protection des données (RGPD) fait obligation aux responsables de traitements de notifier à l'autorité de protection des données (ex. : CNIL pour la France), et selon le degré de gravité, aux personnes concernées, certains incidents de sécurité constituant des violations de données à caractère personnel.

Le respect de cette obligation impose la mise en place au sein de Verallia d'une organisation destinée à assurer la détection de telles violations, d'en évaluer la gravité et de mettre en œuvre les mesures appropriées afin de minimiser les risques, réduire les impacts pour les personnes concernées et identifier toute action utile permettant de prévenir la survenance de nouvelles violations.

1. Objet de cette procédure

La présente procédure vise à définir la conduite à tenir en cas de survenance d'une violation de donnée à caractère personnel et identifier les responsabilités afin de permettre la réalisation des notifications prévues par le RGPD et organiser la traçabilité des violations de données à caractère personnel.

La présente procédure s'adresse tant à l'ensemble du personnel de Verallia (salariés, intérimaires, stagiaires…), qu'au personnel des prestataires de Verallia ayant la qualité de sous-traitant au sens de l'article 28 du RGPD et appelés à ce titre à traiter des données à caractère personnel pour le compte de Verallia ainsi que d'une manière générale à toute personne traitant/détenant des données à caractère personnel pour le compte de Verallia (ci-après le « **Personnel** »).

2. Définitions /types de violations concernées

La notion de violation de données à caractère personnel est définie à l'article 4, 12° du RGPD comme : « *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* ».

Une violation de données est donc un incident de sécurité portant sur des données à caractère personnel (en revanche, tout incident de sécurité ne constitue pas nécessairement une violation de données à caractère personnel).

Il existe trois grandes catégories de violations de données à caractère personnel :

- **Les violations portant sur la confidentialité** : accès potentiel ou avéré aux données à caractère personnel par des personnes autres que celles autorisées à y accéder pour une finalité particulière (accès non autorisé).
- **Les violations portant sur la disponibilité des données** : destruction, perte ou altération accidentelle ou non autorisée de données à caractère personnel rendant les données inaccessibles (perte de contrôle de l'accès aux données),
- **Les violations portant sur l'intégrité des données** : altération non autorisée ou accidentelle des données à caractère personnel (modifications indésirées).

Une violation de données à caractère personnel peut survenir notamment pour les raisons suivantes :

- La perte/le vol d'un moyen de communication ;

- Des processus opérationnels erronés/ des erreurs/négligences humaines dans le traitement des données/ des actes intentionnels malveillants par des acteurs internes ou externes ;
- Une sécurité insuffisante/ une défaillance technique.

Exemples :

- Perte d'un ordinateur portable, d'une clé USB
- Vol/destruction d'équipements
- Accès au système donné par erreur à une mauvaise personne
- Envoi d'un courriel à la mauvaise personne
- Utilisation d'un canal de communication non sécurisé pour échanger des données à caractère personnel sensibles
- Accès à des données à caractère personnel par des collaborateurs en dehors du cadre de leur autorisation professionnelle
- Divulgation non autorisée de données à caractère personnel
- Utilisation non autorisée/contraire aux finalités du système d'information
- Documents papiers non rangés laissé à la portée de tiers
- Attaque informatique (hameçonnage, rançongiciel)
- Défaillance système
- Absence de mot de passe sécurisé sur les ordinateurs, les appareils ou les applications contenant des données à caractère personnel.

Important : Pour les besoins de la présente procédure, la notion de violation de données à caractère personnel renvoie tant aux **violations avérées qu'aux suspicions**.

3. Responsabilités générales

Au sein de chaque entité Verallia, le Personnel de Verallia apporte, sous l'impulsion et le contrôle du Coordinateur à la Protection des Données Société (« **CPD Société** »), tout son concours aux investigations et actions nécessaires pour détecter, traiter et contenir toute violation.

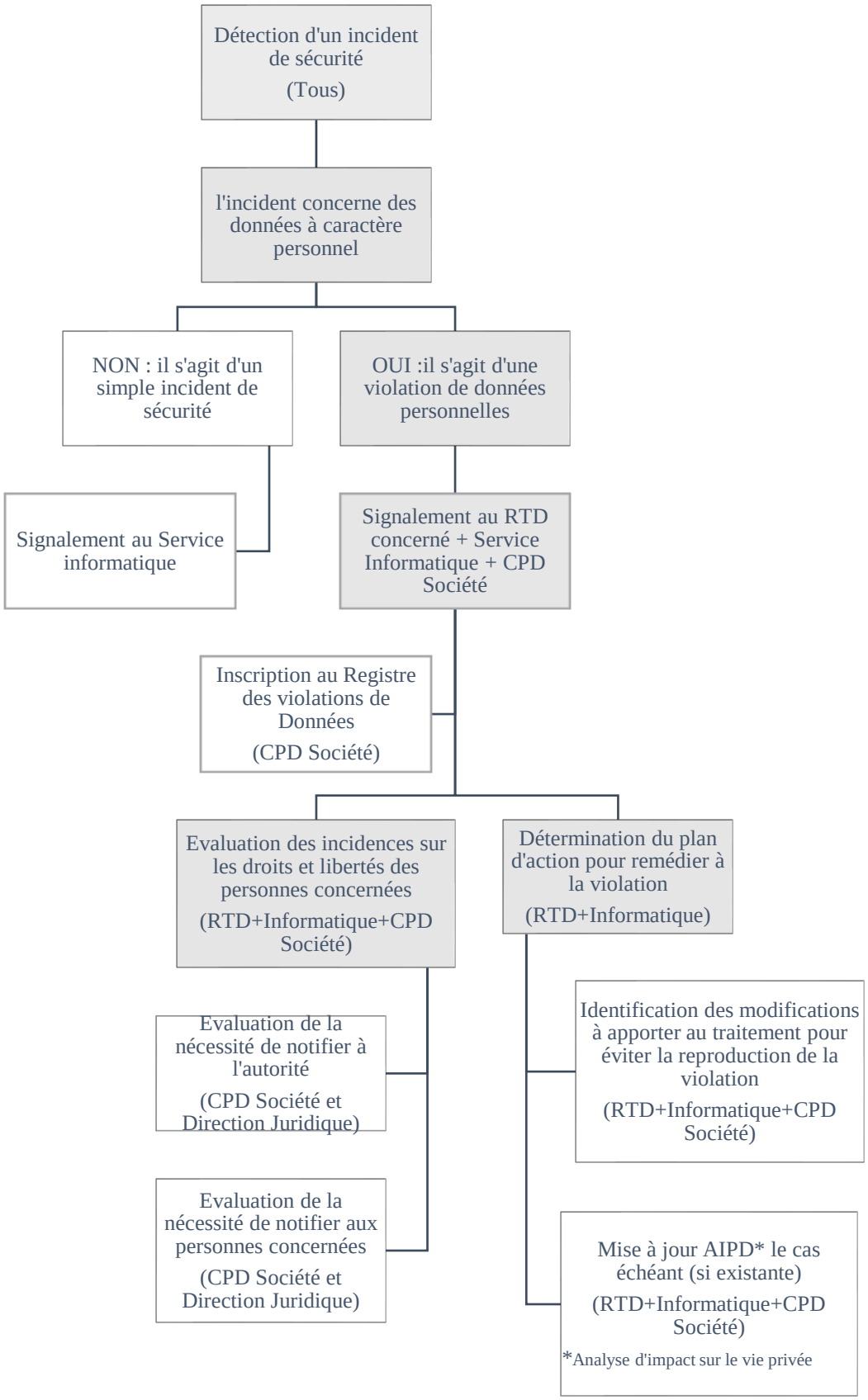
Les Responsables de Traitement des Données (« **RTD** ») et CPD Société de chaque entité Verallia s'assurent de la diffusion appropriée ainsi que du respect de la présente procédure par le Personnel. Ils s'assurent que le Personnel apporte son concours aux investigations et actions nécessaires pour traiter et contenir la violation.

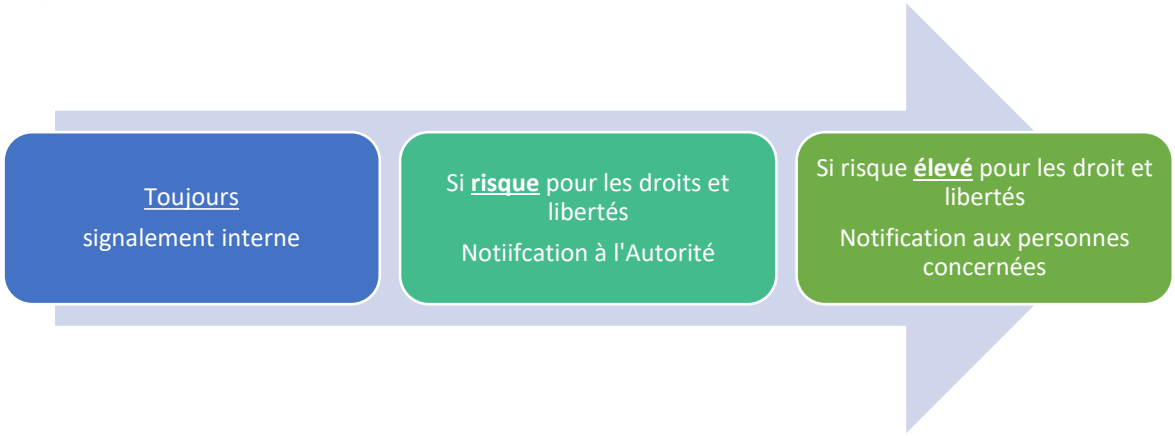
Dans le cadre de ses missions, lorsque le CPD Société n'est pas membre de la Direction Juridique, le CPD Société se fait assister si besoin par la Direction Juridique de la société Verallia concernée (ou à défaut, de la Direction Juridique Groupe).

En outre, le CPD Société intègre dans son rapport annuel au CPD Groupe la liste des violations de données à caractère personnel recensées ayant fait l'objet d'une notification à l'autorité de contrôle et/ou aux personnes concernées. Afin d'aider le CPD Société à faire son rapport au CPD Groupe, un modèle de fichier de rapport est mis à disposition dans le Sharepoint « Personal Data Protection ».

Les RTD concernés par la violation et le Service informatique sont responsables de la mise en œuvre, du point de vue opérationnel, de tout plan de traitement de la violation avec l'assistance, si besoin, du CPD Société (ou Direction juridique).

4. Conduite à tenir





5. Détection et signalement interne

Toute personne (le Personnel, y compris les sous-traitants[1]) doit signaler dans tous les cas et **sans délai** au RTD concerné ainsi qu'au Service Informatique et CPD Société toute violation de données à caractère personnel, ou toute suspicion de violation dont il a connaissance afin de permettre son traitement ainsi que, le cas échéant, la notification à l'autorité de protection des données compétente (ex. CNIL pour la France) dans les délais requis par la réglementation (24h à 72h au plus tard) et/ou aux personnes concernées.

Le signalement doit comporter tous les éléments connus concernant les circonstances de la violation, son importance, le type de données à caractère personnel concernées… Un formulaire, dont un modèle figure **en annexe 1,** peut être utilisé par les entités pour aider au signalement.

Remarque : Si la violation de données à caractère personnel est découverte en dehors des heures de travail, le signalement doit être effectué dès que possible (dès l'ouverture des bureaux ou le 1er jour ouvré suivant).

En cas de sous-traitance :

Tout sous-traitant de Verallia (au sens du RGPD) doit notifier à Verallia toute violation de données dans les meilleurs délais après en avoir pris connaissance.

Il est donc important que le contrat qui lie le sous-traitant à Verallia comporte une obligation en ce sens à la charge du sous-traitant.

6. Évaluation de la violation

6.1. Évaluation initiale de la violation et du risque

Le RTD Société concerné conjointement avec le Service informatique et le CPD Société procèdent à **l'évaluation initiale** de la violation et de sa gravité dans les 24h suivant la violation.

L'objectif de cette évaluation liminaire est de contenir la violation et préserver les preuves.

Leur action , ainsi que celle de toute autre personne disposant d'une expertise en rapport avec la violation (comme le sous-traitant), vise à identifier les mesures appropriées pour déterminer la cause de la violation,

[1] *article 33.2 du RGPD.*

en évaluer l'ampleur et en atténuer les conséquences dommageables potentielles, sans détruire les preuves qui pourraient être nécessaires pour trouver la cause de la violation ou pour y remédier.

6.2. Investigations et évaluation préliminaire des risques

Le RTD Société concerné conjointement avec le Service informatique et le CPD Société (avec le support de la Direction Juridique) procèdent à la conduite des investigations nécessaires pour évaluer la gravité de la violation et les risques.

Cette évaluation permet de déterminer si l'entité Verallia concernée est tenu de notifier la violation à l'autorité de protection des données compétente et, le cas échéant, aux personnes concernées (v. § 7) et, le cas échéant, de procéder auxdites notifications dans les délais requis étant rappelé que :

- La notification à l'autorité compétente est obligatoire en cas de risque pour les droits et libertés des personnes concernées
- Le signalement aux personnes est obligatoire en cas de risque élevé pour les droits et libertés des personnes concernées

La **gravité** des violations de données à caractère personnel varie en termes d'impact et de risque pour les personnes concernées en **fonction du contenu, de la quantité de données impliquées, ainsi que de la durée d'exposition au risque**. Il est donc important que l'entité Verallia soit en mesure d'identifier rapidement la sensibilité des données et de répondre rapidement à tous les incidents signalés et de manière appropriée.

Les critères à prendre en compte sont les suivants :

- Type de violation
- Nature, caractère sensible et volume des données à caractère personnel
- Nombre de personnes concernées
- Facilité d'identification des personnes concernées
- Gravité des conséquences pour les personnes concernées
- Vulnérabilité/caractéristiques particulières des personnes concernées
- Durée d'exposition des données

En cas de violation avérée, l'évaluation des risques porte uniquement sur l'incidence (réelle et/ou potentielle) de la violation sur les droits et libertés des personnes physiques.

La gravité des violations peut être classée de la manière suivante :

- Criticité très élevée (Violation majeure) : violation entraînant des conséquences significatives ou irréversibles pour les personnes concernées

Exemples :

- perte de contrôle sur leurs données
- limitation de leurs droits
- discrimination
- vol d'identité/ fraude /atteinte à la réputation
- perte financière
- annulation non autorisée de la pseudonymisation
- perte de confidentialité
- tout autre désavantage économique ou social important

• Criticité élevée (violation importante) : conséquences surmontables mais avec de sérieuses difficultés (coût, délai important, aggravation situation) pour les personnes concernées

• Criticité moyenne (violation simple) : gêne pour les personnes concernées

• Non Critique (violation mineure) : simple désagrément que les personnes peuvent dépasser facilement (ex : recommuniquer des données)

Important : Lors de l'évaluation d'un risque, il convient de tenir compte à la fois de la probabilité **et** de la gravité de l'effet négatif pour les droits et libertés des personnes concernées (i.e. incidence pour les personnes).

Cette évaluation peut évoluer dans le temps : une partie de l'incidence peut s'être matérialisée dès la détection de la violation, une autre peut ne se concrétiser qu'ultérieurement (en cas de vol d'identifiants, par exemple, certains d'entre eux peuvent déjà avoir été utilisés, d'autres peuvent être utilisés par la suite).

A l'issue de cette évaluation, le CPD Société, après consultation de la Direction Générale, de la direction juridique (si distincte du CPD Société) et la direction métier concernée, décide des mesures de notification/information appropriées à mettre en œuvre (notification à la l'autorité de protection des données compétente, aux personnes concernées, information des autorités policières…) et le cas échéant, le RTD concerné procède aux notifications avec le support de la Direction Juridique locale.

Lorsque la notification doit être faite auprès de la CNIL (autorité de protection française), tout **projet** de notification à l'autorité de contrôle et/ou aux personnes concernées est envoyée à la Direction Juridique Groupe pour avis.

Lorsque la notification doit être faite auprès d'une autorité de protection des données autre que la CNIL, une copie de la notification est adressée pour information à la Direction Juridique Groupe.

6.3. Évaluation complète

Dès que la violation est suffisamment identifiée et contenue, et si l'évaluation complète n'a pas pu être faite dans les délais de notification, le RTD concerné et le Service informatique conduisent conjointement une évaluation approfondie de la violation, de l'efficacité de la réponse apportée, de l'ensemble des conséquences pour les personnes concernées et des éventuels changements à apporter au système d'information/à l'organisation pour éviter toute nouvelle violation.

7. Exigences en matière de notifications externes

7.1. Notification à l'autorité de protection des données compétente

La notification auprès de l'autorité de protection des données compétente doit être effectuée dans les délais requis par la réglementation applicable. **A cet égard, le RGPD prévoit que la notification doit être effectuée dans les meilleurs délais et si possible 72 heures au plus tard** après la prise de connaissance, de

la constatation de la violation. Passé ce délai, le responsable de traitement (via le RTD avec le support de la Direction Juridique locale) doit justifier des motifs du retard[2].

Lorsque la violation concerne un sous-traitant :

Il est rappelé que seule Verallia (en qualité de responsable de traitement) peut effectuer une déclaration de violation de données à l'autorité de protection des données : en aucun cas un sous-traitant de Verallia n'est habilité à effectuer une telle déclaration à la place de Verallia.

Chaque entité doit respecter le formalisme demandé pour la notification. En France, la notification s'effectue par le biais d'un téléservice sécurisé dédié accessible sur le site de la CNIL: https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles.

Contenu de la notification (article 33.3 du RGPD)[3] :

- La nature de la violation, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés
- Les coordonnées du DPO ou à défaut d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues (Il est recommandé de communiquer le nom du RSSI ou du CPD Société)
- Les conséquences probables de la violation des données
- Les mesures prises ou proposées pour remédier à la violation, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives

7.2. Notification aux personnes concernées

Les personnes concernées sont informées, individuellement et **dans les meilleurs délais[4]** , lorsque le risque pour leur vie privée est élevé (possibilité de moduler ce délai s'il est prioritaire de limiter les risques de propagation).

Contenu de la notification (article 34.2 du RGPD), a minima et en termes clairs et simples :

- La nature de la violation de données
- Les coordonnées du DPO ou à défaut d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues (Il est recommandé de communiquer le nom du RSSI ou du CPD Société)
- Les conséquences probables de la violation des données
- Les mesures prises ou proposées pour remédier à la violation, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives

Exceptions à l'obligation de notification aux personnes concernées :

- Lorsque la violation en question n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques
- Lorsque le responsable du traitement a pris des mesures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser

[2] Article 33.1 du RGPD. Pour rappel, les congés et/ou weekends ne sont pas des motifs pouvant justifier le retard de notification.
[3] Lorsqu'il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.
[4] Article 34.1 du RGPD

- Lorsque le responsable de traitement a mis en œuvre des mesures organisationnelles et techniques appropriées aux données à caractère personnel affectées par la violation (exemple : chiffrement des données)
- Lorsque l'information aux personnes entraînerait des efforts disproportionnés (dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace).

8. Documentation à tenir

8.1. Registre des violations de données

Le CPD Société tient à jour un Registre des violations de données (article 33.5 du RGPD) décrivant pour chaque violation :

- la nature de la violation ;
- les catégories et le nombre approximatif des personnes concernées ;
- les catégories et le nombre approximatif de fichiers concernés ;
- les conséquences probables de la violation ;
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- le cas échéant, la justification de l'absence de notification auprès de l'autorité de protection des données compétente ou d'information aux personnes concernées.

Toute violation de données doit être inscrite au Registre des violations de données, qu'elle ait donné lieu à une notification à l'autorité de protection des données compétente ou non.

Un modèle de fiche de registre figure dans le Sharepoint « Personal Data Protection ».

8.2. Autres éléments probatoires

Pour chaque violation, la documentation à tenir inclut :

- La copie de la fiche du Registre des violations
- Le plan d'action mis en œuvre pour contenir/traiter la violation
- L'analyse des risques conduite postérieurement à la mise en œuvre des mesures de remédiation

Le cas échéant :

- La copie de la notification à l'autorité de protection des données compétente et de l'accusé réception
- La copie des notifications effectuées aux personnes concernées

Annexe 1 : Exemple de formulaire de signalement

Signalisation d'une violation de données à caractère personnel	
La violation est	☐ suspectée ☐ avérée ☐ en cours ☐ terminée
Description de la violation	
Date et heure à laquelle la violation a été découverte	
Date/période concernée par la violation	
Nom et qualité (salarié , prestataire, résident…) de la personne ayant identifié la violation	
Nom et coordonnées de contact de la personne signalant la violation (tél. + courriel)	
Catégories de personnes susceptibles d'être impactées par la violation	
Catégories de données personnelles concernées	
Catégories de données sensibles	
Volume de données concernées	
Cause/origine de la violation	
Prestataire sous-traitant impliqué/concerné le cas échéant	
Si la violation est en cours, quelles actions sont entreprises pour y mettre fin ?	
Evaluation liminaire de la gravité de l'incident (impact pour Verallia/conséquences possibles pour les personnes concernées)	
Toute autre information pertinente	

Réservé au CPD Société	
Date et heure de réception	