

G2S

be|ys

Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données

**PR**  
Procédure

Modèle : Procédure (G2S) - V 1.0 du 15/02/2016  
Type : PR - Modèle Procédure  
Réfèrent du modèle : ML Fourès (MLF – marie-laure.foures@almerys.com – 06.31.67.46.43)

## Procédure

# Protection des données à caractère personnel

## Gestion en cas de contrôle des Autorités de protection des données

### Objet / Synthèse \*

Dans le cadre des règles contraignantes d'entreprise (BCR), le Groupe et toutes ses entités s'engagent en cas de contrôle des Autorités de protection des données, à coopérer afin de faciliter leurs démarches.  
Cette procédure permet de définir les étapes à respecter lorsqu'un tel contrôle interviendrait au sein des Groupes.  
Cette procédure intervient aussi dans l'hypothèse où le contrôle n'est pas lié au BCR mais concerne tout de même des données à caractère personnel.

Client  
Projet

### Niveau de diffusion \*

### Liste de Diffusion

### Localisation \*

### (GED ou réseau)

D2 - Interne G2S Group et Be Invest  
Groupes

< permalien GED ou chemin réseau >

Version *	Date *	Modifications *	Rédacteur *
V1	23/11/2016	Création	Aïssatou SARR (ASA)
V2	01/12/2016	Relecture	Frédéric Rustan (FRU)
V2	05/12/2016	Relecture	Sylvain Seramy (SSE)
V3	20/01/2017/	Modifications	Aïssatou SARR (ASA)
Date de péremption			
Responsable d'actualisation			Aïssatou SARR (ASA)
Identifiant du document			<identifiant du document>



G2S Group <b>be ys</b>	Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données	<b>PR</b> Procédure
------------------------	---	------------------------

Modèle :	Procédure (G2S) - V 1.0 du 15/02/2016
Type :	PR - Modèle Procédure
Référent du modèle :	ML Fourès (MLF – marie-laure.foures@almerys.com – 06.31.67.46.43)

## Procédure

# Protection des données à caractère personnel

## Gestion en cas de contrôle des Autorités de protection des données

### Objet / Synthèse \*

Dans le cadre des règles contraignantes d'entreprise (BCR), le Groupe et toutes ses entités s'engagent en cas de contrôle des Autorités de protection des données, à coopérer afin de faciliter leurs démarches.

Cette procédure permet de définir les étapes à respecter lorsqu'un tel contrôle interviendrait au sein des Groupes.

Cette procédure intervient aussi dans l'hypothèse où le contrôle n'est pas lié au BCR mais concerne tout de même des données à caractère personnel.

Client

Projet

<u>Niveau de diffusion</u> *	D2 - Interne G2S Group et Be Invest
<u>Liste de Diffusion</u>	Groupes
<u>Localisation</u> * (GED ou réseau)	< permalien GED ou chemin réseau >

Version *	Date *	Modifications *	Rédacteur *
V1	23/11/2016	Création	Aïssatou SARR (ASA)
V2	01/12/2016	Relecture	Frédéric Rustan (FRU)
V2	05/12/2016	Relecture	Sylvain Seramy (SSE)
V3	20/01/2017/	Modifications	Aïssatou SARR (ASA)
<b>Date de péremption</b>			
<b>Responsable d'actualisation</b>		Aïssatou SARR (ASA)	
<b>Identifiant du document</b>		<identifiant du document>	

10/10/10



G2S Group <b>be ys</b>	Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données	<b>PR</b> Procédure
------------------------	---	------------------------

## Documents de Références

Libellé	Adresse GED ou WIKI ou Chemin réseau ou insertion du document

## Glossaire

Terme / Acronyme	Définition
DPO	Délégué à la Protection des données
RT	Responsable des Traitements
JLD	Juge des Libertés et de la Détention

## Validation

Processus	Sous-processus		
Référentiel(s) concerné(s)	Responsable du ou des référentiel(s)	Date :	Signature :
<input type="checkbox"/> ISO 9001 <input type="checkbox"/> ISO 27001 <input type="checkbox"/> HDS <input checked="" type="checkbox"/> BCR			
Relecteur :	Rôle :	Date :	Signature :
Valideur :	Fonction :	Date :	Signature :
Laurent Caredda (LCA)	Président du Groupe		

## Sommaire

1. Contexte d'application et Objectifs.....	3
2. Description de la Procédure .....	7
3. Moyens et Outils.....	11
4. Acteurs .....	12



G2S Group <b>be ys</b>	Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données	<b>PR</b> Procédure
------------------------	---	------------------------

## 1. Contexte d'application et Objectifs

L'un des critères les plus importants servant à évaluer le niveau de protection adéquat d'un système d'autoréglementation est le degré de soutien et d'assistance offert aux personnes concernées:

«Une exigence essentielle à laquelle doit répondre un système de protection des données approprié et efficace est qu'une personne physique confrontée à un problème touchant aux données personnelles la concernant ne soit pas laissée à elle-même, mais puisse bénéficier d'un soutien institutionnel pour la solution de ses problèmes»

Il s'agit là en effet de l'un des éléments les plus importants des règles d'entreprise contraignantes applicables aux transferts internationaux de données: les règles doivent clairement faire état du devoir de coopération avec les autorités de protection des données, de façon à ce que les particuliers puissent bénéficier du soutien institutionnel nécessaire.

Il faut qu'il soit clairement entendu que le groupe dans son ensemble et chacune de ses filiales, séparément, acceptent les conditions des contrôles établies par les Autorités de protection des données. Il faut qu'il soit également clairement entendu que le groupe dans son ensemble et chacune de ses filiales, séparément, respectent les conseils de l'autorité compétente chargée de la protection des données pour tout ce qui touche à l'interprétation et à l'application de ces règles d'entreprise contraignantes.

Les conseils de l'autorité compétente chargée de la protection des données prendront la forme de recommandations adressées au groupe, soit en réponse à un questionnaire, à une plainte introduite par une personne concernée ou à la propre initiative de l'autorité chargée de la protection des données.

Avant de formuler tout conseil, l'autorité compétente de protection des données peut solliciter l'avis du groupe, des personnes concernées ainsi que des autorités de protection des données susceptibles d'être associées au processus du fait de la procédure de coopération prévue dans les règles contraignantes d'entreprise (BCR).

Les conseils de l'autorité peuvent être rendus publics.

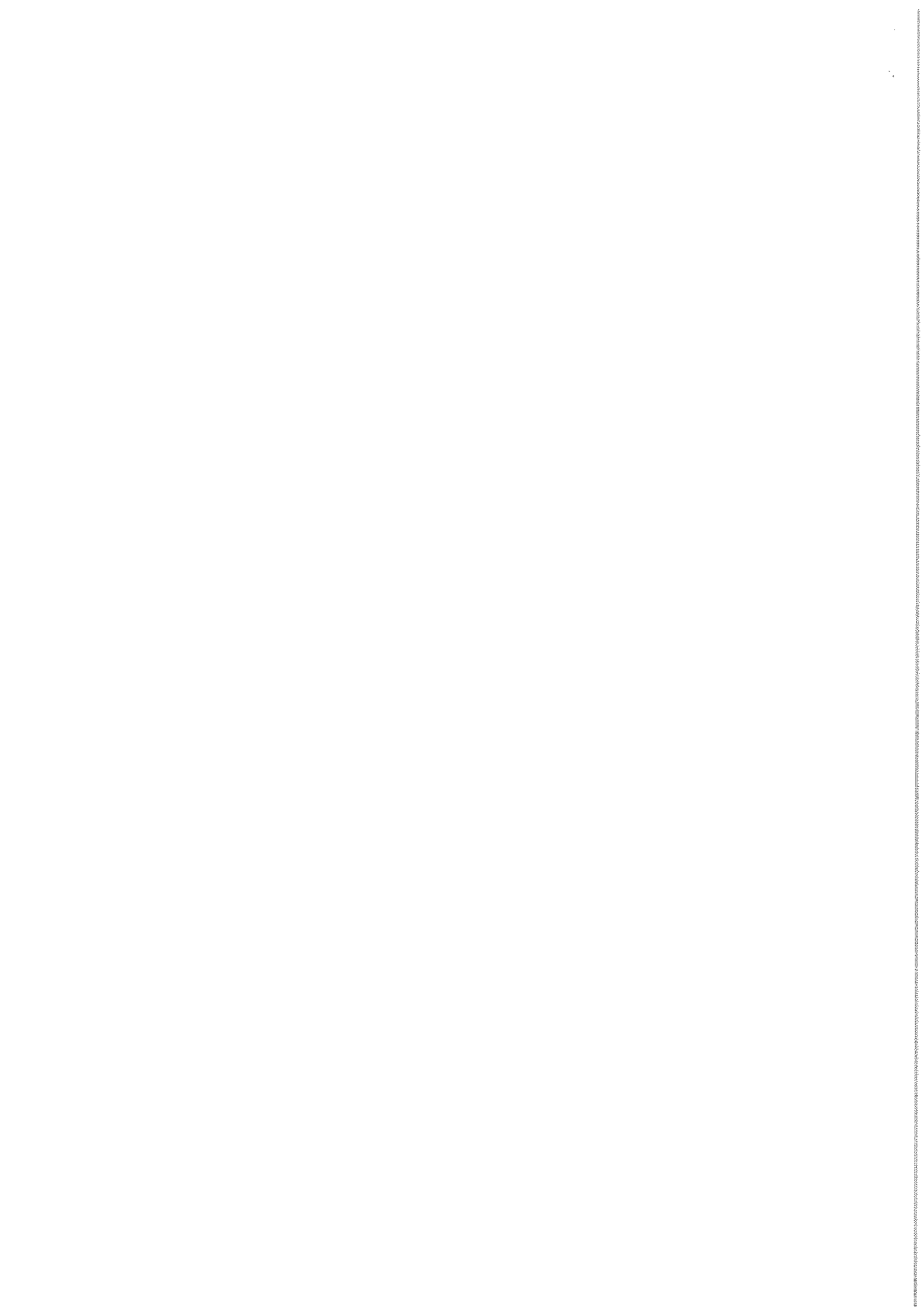
Outre toute disposition pertinente au niveau national, si le groupe refuse fermement et persiste à refuser de coopérer ou de se conformer aux conseils de l'autorité compétente de protection des données, l'autorisation octroyée par cette dernière ou par l'instance compétente dûment habilitée à le faire en vertu de la législation nationale pourra être suspendue ou lui être retirée.

Cette décision prendra la forme d'un acte administratif que le destinataire pourra contester en introduisant une action auprès du tribunal compétent, conformément à la législation nationale en vigueur. Elle sera notifiée à la Commission européenne ainsi qu'aux autres autorités de protection des données concernées et pourra également être rendue publique.



### 1.1. Quelles sont les mesures à mettre en œuvre à l'arrivée de la délégation ?

Lors de l'arrivée de la délégation de contrôle de l'Autorités de protection des données, certaines mesures doivent être mises en œuvre par le DPO.

Pour commencer, il faut les accueillir dans une pièce calme, où l'on pourra discuter sans être dérangé, si la délégation est accueillie par l'accueil, ils devront joindre le DPO au plus vite.





G2S Group 	Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données	
---	---	---

Le DPO préviendra ensuite le Responsable des traitements du contrôle en cours.

Celui-ci désignera un Responsable des lieux qui sera l'image de l'entreprise face à l'Autorités de protection des données. Il est désigné par le Responsable des traitements, et cela peut être le DPO ou toutes autres personnes que le RT considérera comme étant apte à cela.

Lorsque le responsable des lieux a été choisi, il faudra vérifier l'identité des agents de contrôle. Pour cela, il faudra demander à voir leurs cartes d'identité ainsi que leurs cartes professionnelles pour vérifier s'ils sont bien habilités à faire des contrôles.

Il faudra demander à voir l'ordre de mission et la décision de contrôle du président de l'Autorités de protection des données.

## 1.2. Quel est le rôle du responsable des lieux ?

Le rôle du responsable des lieux est d'être la « vitrine » de l'entreprise lors du contrôle, il se doit de faciliter celui-ci en fournissant les informations et les documents demandés, il peut décider d'accepter ou pas le contrôle. Et à la fin de celui-ci, il signe le Procès-Verbal.

Il est préférable que le responsable des lieux soit le DPO étant donné qu'il est plus à même de fournir les informations nécessaires au déroulement du contrôle.

Toutefois, le Responsable de Traitement est libre de désigner une autre personne.

## 1.3. Quels sont les horaires légaux pour effectuer un contrôle ?

Selon l'article 44 de la loi « Informatique et Libertés » les horaires durant lesquels les contrôles peuvent s'effectuer sont de 06h00 à 21h00. Toutefois, un contrôle peut être plus long et finir après 21h00.

Il faut donc s'assurer que le responsable des lieux reste disponible jusque tard dans la soirée, étant donné qu'il doit signer le PV à la fin du contrôle.

Il faut savoir que c'est l'heure du début du contrôle qui est important.

## 1.4. Quelles sont les conséquences en cas d'opposition au contrôle de la CNIL ?

Le responsable des lieux peut s'opposer à tout moment à la visite de la délégation de l'Autorités de protection des données.

Il ne peut toutefois pas s'opposer au contrôle.

En cas d'opposition, les agents de l'Autorité de protection des données pourront saisir le juge des libertés et de la détention (JLD) en vue d'obtenir une ordonnance autorisant la visite avec l'aide, le cas échéant, de la force publique. Cette ordonnance peut faire l'objet d'un recours devant le premier président de la cour d'appel.



G2S Group <b>be ys</b>	Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données	<b>PR</b> Procédure
------------------------	---	------------------------

En pratique, celle-ci a toujours été accordée aux agents de la Commission.

Par exception, une ordonnance du JLD peut être demandée avant toute opposition, lorsque l'urgence, la gravité des faits ou encore le risque de destruction des preuves le justifient (article 44-II de la LIL).

L'ordonnance permettra à l'Autorité de protection des données d'effectuer un nouveau contrôle, avec l'aide des forces de police si l'entreprise reste réfractaire.

## 1.5. Dans quels cas le contrôleur doit-il disposer d'une habilitation spécifique ?

Il est énoncé à l'article 44 de la loi que lors d'un contrôle sur place, le contrôleur doit disposer d'une habilitation spécifique dans le cadre de l'application de l'article 26 de la loi 78-17 du 6 janvier 1978.

Il est énoncé dans cet article que celle-ci est nécessaire pour tous les traitements de données à caractère personnel :

- Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique,
- Qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté,
- Qui portent sur les données dites sensibles du I de l'article 8 (origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle),

Toutefois, il ne faut pas confondre les données issues du secret professionnel et celle dont il est nécessaire d'obtenir une habilitation spécifique.

De plus, pour les traitements de données de santé, il n'est pas nécessaire d'avoir une habilitation spécifique, mais il faut un médecin spécialement habilité qui pourra relever des secrets professionnels dont les membres de la délégation ne peuvent prendre connaissance.

## 1.6. Que va regarder la délégation lors du contrôle ?

La délégation va effectuer un contrôle complet des obligations dont l'entreprise est tenue selon la loi « Informatique et Libertés », le Règlement Général sur la Protection des Données (RGPD), ou tous autres textes de Protection des données auxquels le Groupe serait soumis.



Elle va donc vérifier si tous les traitements de données à caractère personnel ont été déclarés auprès des Autorités de protection des données et si toutes les formalités ont été effectué afin d'être en conformité avec la loi.

Si le contrôle a été initié suite à une plainte, elle va vérifier si la plainte du client est fondée et si l'entreprise est susceptible d'avoir d'autres manquements.

Elle vérifiera aussi que tous les engagements pris dans le cadre des règles contraignantes d'entreprise sont bien respectés.





G2S Group 	Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données	
---	---	---

### 1.7. Qui peut être sollicité lors d'un contrôle ?

Pour répondre aux questions, le DPO peut demander au Responsable de traitement, au responsable des lieux (dans le cas où le responsable des traitements aurait choisi une personne autre que le DPO) des informations essentielles à la coopération avec les Autorités de protection des données.

Le DPO peut aussi solliciter les informaticiens ou les chefs de projet ayant travaillé sur les traitements contrôlés.

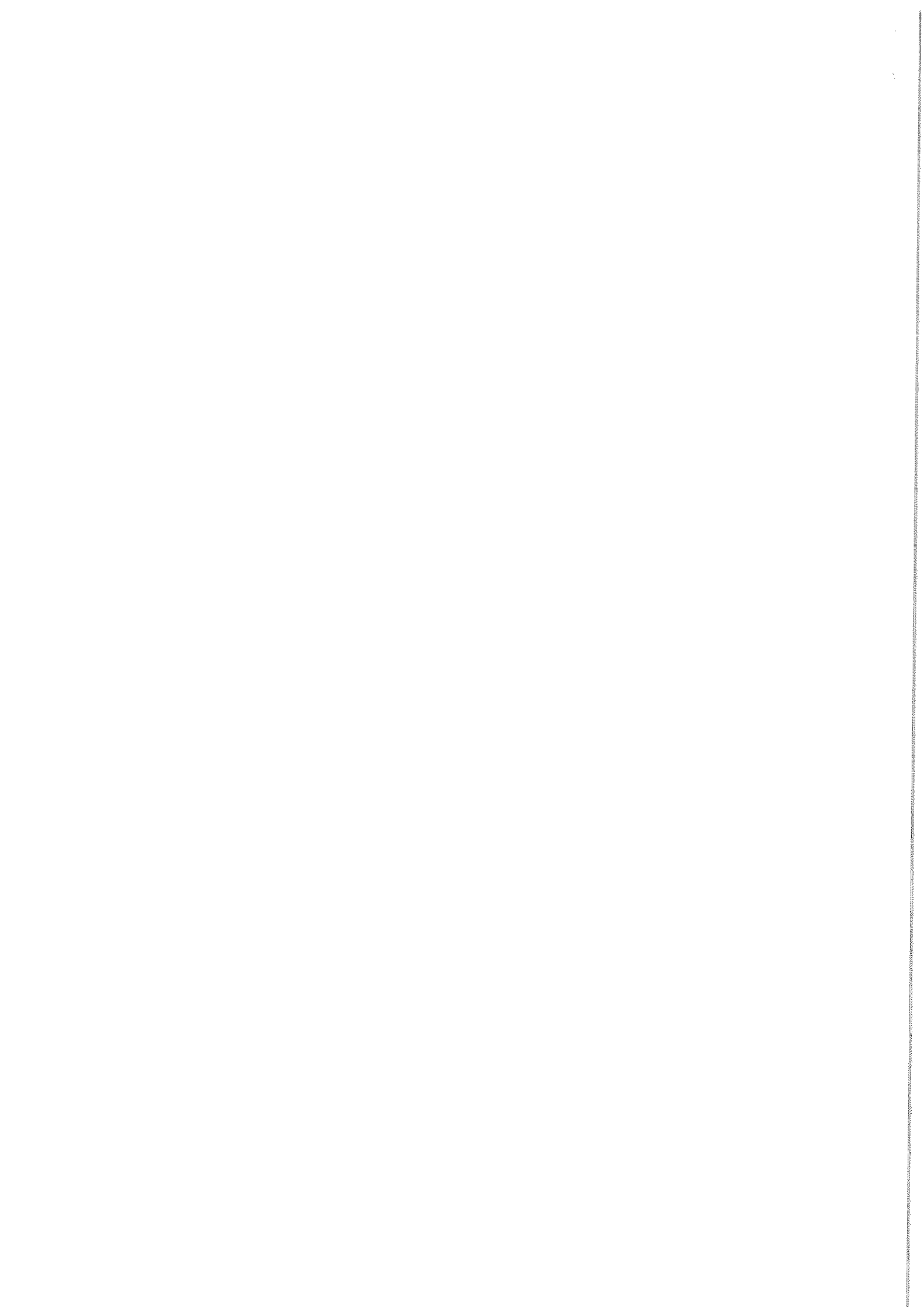
Ainsi que la Sécurité en cas de faille de sécurité des données à caractère personnel.

### 1.8. Quelles sont les actions à mener suite au contrôle ?

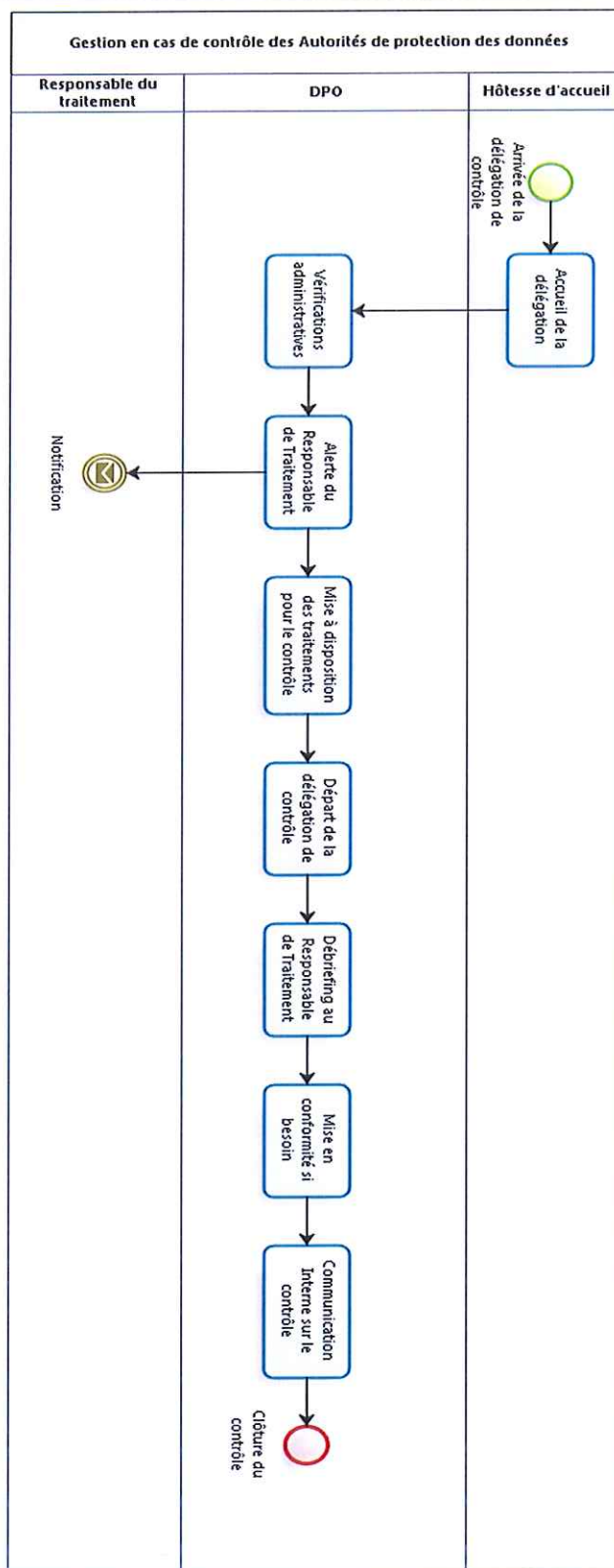
Après le contrôle de la délégation, il est important d'effectuer :

- Un débriefing auprès du Responsable de Traitement
- Se mettre en conformité en se basant sur les recommandations faites par la délégation
- Communiquer en interne sur le déroulement du contrôle
- Envoyer un courrier à l'Autorité de protection des données pour indiquer toutes les mesures mises en œuvre pour cesser les manquements, et ajouter un plan prévisionnel si les mesures ne peuvent s'appliquer immédiatement.

Dans l'hypothèse où aucunes mesures ne seraient mises en place après le contrôle, sachant qu'il n'y a pas de délai pour leurs applications, l'Autorité de protection des données pourrait envisager une mise en demeure.



## 2. Description de la Procédure

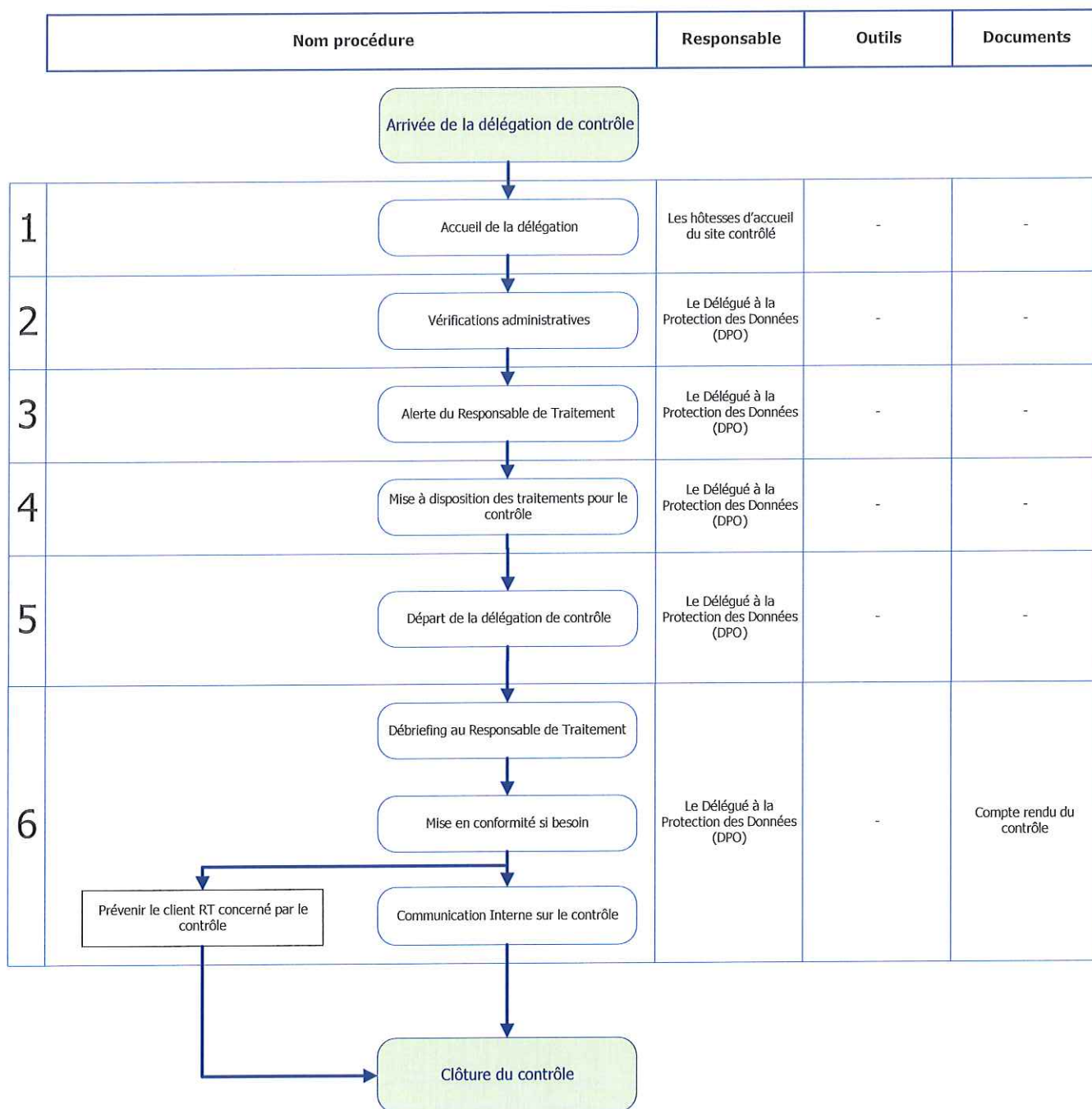


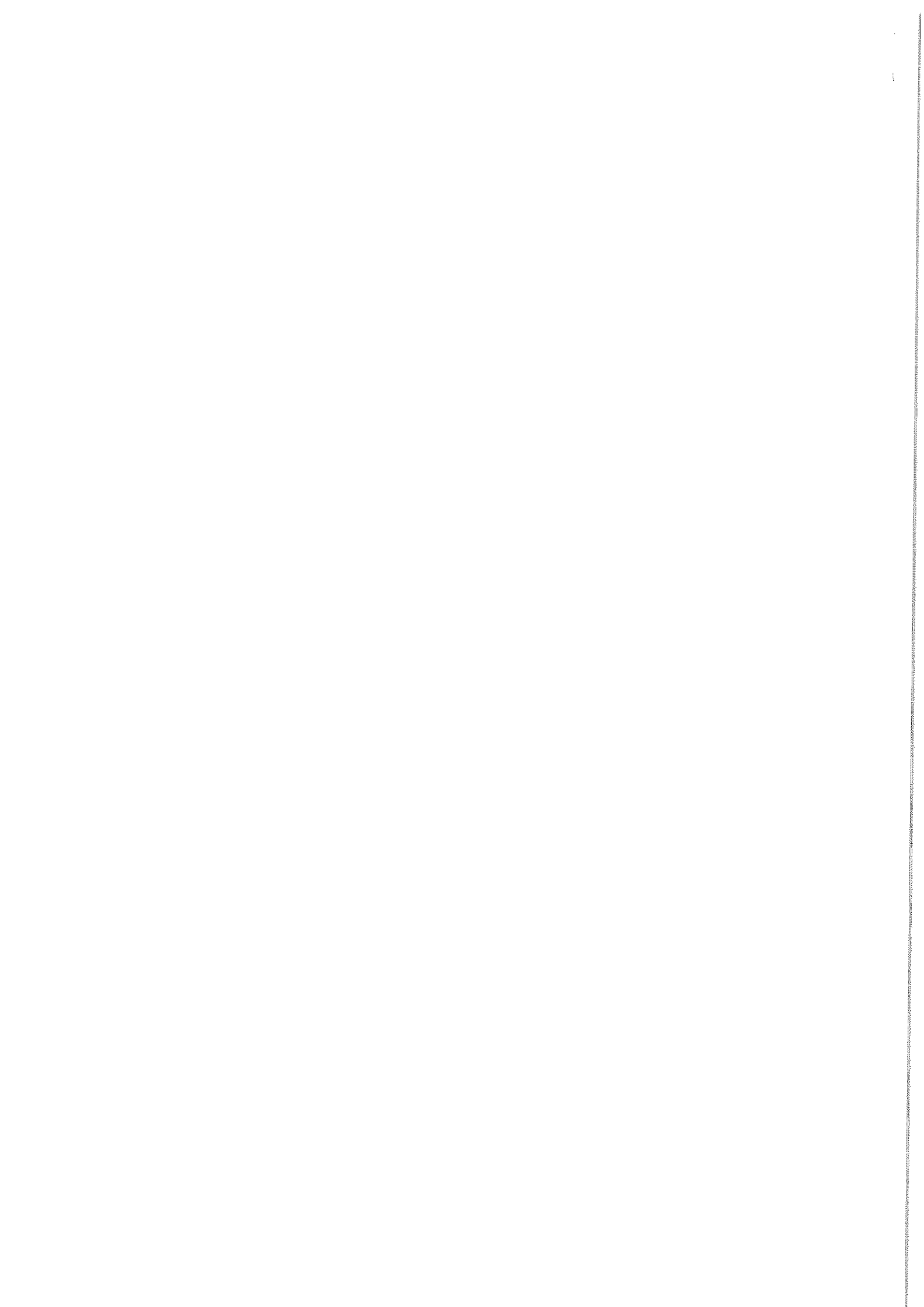




G2S Group <b>be ys</b>	Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données	<b>PR</b> Procédure
------------------------	---	------------------------

Logigramme détaillées des activités portées par la procédure :





<b>G2S Group</b> <b>be</b>   <b>ys</b>	<b>Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données</b>	<b>PR</b> <b>Procédure</b>
--	--	-------------------------------

N° étape	Acteur	Entrée ou déclencheur	Action (objectif et description)	Sortie ou livrable	Outil(s)
1. Accueil de la délégation de contrôle	Les hôtes d'accueil du site contrôlé	Arrivée de la délégation de contrôle	accueillir dans une pièce calme, où l'on pourra discuter sans être dérangé, si la délégation est accueillie par l'accueil, ils devront joindre le DPO au plus vite.		
2. Vérifications administratives	Le Délégué à la Protection des Données (DPO)	Après avoir installé la délégation dans une salle au calme	Le DPO doit vérifier l'identité des agents de contrôle. Il demandera à voir leurs cartes d'identité et leurs cartes professionnelles pour vérifier s'ils sont bien habilités à faire des contrôles. Il faudra demander à voir l'ordre de mission et la décision de contrôle du président de l'Autorités de protection des données.		
3. Alerte du Responsable de Traitement	Le Délégué à la Protection des Données (DPO)	Après les vérifications administratives	Le DPO préviendra ensuite le Responsable des traitements du contrôle en cours. Celui-ci désignera un Responsable des lieux qui sera l'image de l'entreprise face à l'Autorités de protection des données.		
4. Mise à disposition des traitements pour le contrôle	Le Délégué à la Protection des Données (DPO)	Après avoir défini un responsable des lieux	Le DPO donnera accès à la délégation aux traitements de données à caractère personnel, tout en n'omettant pas de demander la présence d'un médecin en cas d'accès à des données de santé.		
5. Départ de la délégation de contrôle	Le Délégué à la Protection des Données (DPO)	Lorsque le contrôle de la délégation a pris fin	La délégation fournit un Procès-Verbal (PV) de contrôle dans lequel elle note les manquements relevés lors du contrôle. Le DPO doit signer le PV et accompagner la délégation hors du site. Après le contrôle de la délégation, il est important d'effectuer : <ul style="list-style-type: none"> <li>➢ Un débriefing auprès du Responsable de Traitement,</li> <li>➢ Se mettre en conformité en se basant sur les recommandations faites par la délégation,</li> <li>➢ Communiquer en interne sur le déroulement du contrôle.</li> <li>➢ Si le contrôle est lié à un traitement dont on est sous-traitant, il faudra prévenir le client RT concerné par le contrôle.</li> </ul>	Compte rendu du contrôle	
6. Mise au point interne	Le Délégué à la Protection des Données (DPO)	Suite au départ de la délégation de contrôle			







G2S Group <b>be</b>   <b>ys</b>	Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données	<b>PR</b> Procédure
---------------------------------	---	------------------------

N° étape	Acteur	Entrée ou déclencheur	Action (objectif et description)	Sortie ou livrable	Outil(s)
Clôture du contrôle	Le Délégué à la Protection des Données (DPO)	Après avoir effectué les mises au point interne	Envoyer un courrier à l’Autorité de protection des données pour indiquer toutes les mesures mises en œuvre pour cesser les manquements, et ajouter un plan prévisionnel si les mesures ne peuvent s’appliquer immédiatement.	Courrier pour l’Autorité de protection des données	Lettre Recommandé avec Accusé de Réception



G2S Group 	Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données	
---	---	---

### 3. Moyens et Outils

---

Il n'y a pas d'outils particuliers à utiliser.

Toutefois, le DPO peut être joint sur son téléphone fixe, son mobile ou par mail :

- Fixe : 04 73 74 71 06
- Mobile : 06 86 42 88 59
- Mail : [aissatou.sarr@almerys.com](mailto:aissatou.sarr@almerys.com)  
[dpo@almerys.com](mailto:dpo@almerys.com)  
[dpo@g2s-group.com](mailto:dpo@g2s-group.com)



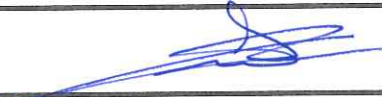


G2S Group <b>be ys</b>	Protection des données à caractère personnel – Gestion en cas de contrôle des Autorités de protection des données	<b>PR</b> Procédure
------------------------	---	------------------------

## 4. Acteurs

Les acteurs de cette procédure sont :

- Le Responsable des Traitements
- Le Délégué à la Protection des données
- Le Responsable des lieux (s'il diffère du DPO)
- Les hôtes d'accueil
- Toutes les personnes nécessaires au bon déroulement du contrôle

Laurent Caredda (LCA)		
-----------------------	--	--

\*\*\*\*\*Fin du Document\*\*\*\*\*

