

G2S Group <b>be ys</b>	Protection des données à caractère personnel – Audit des traitements de données à caractère personnel	<b>PR</b> Procédure
------------------------	---	------------------------

Modèle :	Procédure (G2S et Be Invest) - 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	
Audit des traitements de données à caractère personnel	
<b>Objet / Synthèse *</b>	<p>Cette procédure permet de définir les éléments nécessaires aux audits à effectuer dans le cadre du respect de notre Politique de Protection des données, ainsi que dans le respect des engagements pris dans le cadre des Binding Corporate Rules (BCR).</p> <p>Il découle de l'obtention des BCR, l'obligation de se soumettre à tout audit effectué par les Autorités de protection des données et de se conformer à leur avis sur toute question ayant trait aux règles.</p> <p>La procédure d'Audit des traitements de données à caractère personnel est effectuée annuellement, au sein de chacune des entités du Groupe.</p>
<b>Client</b>	Groupe
<b>Projet</b>	

<b>Niveau de diffusion *</b>	D2 - Interne G2S Group
<b>Liste de Diffusion</b>	Groupe
<b>Localisation * (GED ou réseau)</b>	< 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 (FRU)
<b>Date de péremption</b>			
<b>Responsable d'actualisation</b>		Aïssatou SARR (ASA)	
<b>Identifiant du document</b>		<identifiant du document>	



G2S Group <b>be ys</b>	Protection des données à caractère personnel – Audit des traitements de données à caractère personnel	<b>PR</b> Procédure
------------------------	---	------------------------


## Documents de Références

Libellé	Adresse GED ou WIKI ou Chemin réseau ou insertion du document
Règlement Général sur la protection des données (RGPD)	Q:\Conformité\CNIL\Règlement Européen
Norme ISO 19011 de décembre 2002 ; Ligne directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental	Q:\Conformité\CNIL\Normes ISO

## Glossaire

Terme / Acronyme	Définition
RGPD	Règlement Général sur la protection des données
DPO	Délégué à la Protection des Données

## 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	Président du Groupe	13/01/17	

## Sommaire

1. Contexte d'application et Objectifs.....	3
2. Description de la Procédure .....	5
3. Moyens et Outils.....	8
4. Acteurs .....	9





G2S Group <b>be ys</b>	Protection des données à caractère personnel – Audit des traitements de données à caractère personnel	<b>PR</b> Procédure
------------------------	---	------------------------

## 1. Contexte d'application et Objectifs

Les BCR imposent au Groupe la réalisation d'audits en matière de protection des données à intervalles réguliers ou sur demande expresse du Délégué à la Protection des données (DPO), ou de toute autre instance compétente au sein de l'organisation.

Ces audits pourront être effectués par des contrôleurs internes ou externes agréés.

Le programme d'audit couvre tous les aspects des BCR, y compris les méthodes visant à garantir la mise en œuvre des mesures correctives. Les résultats seront communiqués au Délégué à la Protection des données (DPO) (si l'audit n'est pas effectué par lui) ainsi qu'au conseil d'administration de la maison mère du Groupe.

Les Autorités de protection des données peuvent, sur demande, avoir accès aux résultats de l'audit. Elles peuvent mener elles-mêmes des audits sur la protection des données, si nécessaire.

Les Autorités de protection des données pourront mener des audits :

- si celles effectuées par le Groupe ne sont pas disponibles pour l'une ou l'autre raison,
- lorsqu'ils ne contiennent pas les informations pertinentes nécessaires à un suivi normal de l'autorisation octroyée,
- lorsque l'urgence de la situation plaide en faveur d'une participation directe de l'autorité compétente de protection des données ou de contrôleurs indépendants en son nom.

Ces audits seraient menés conformément à la législation et aux réglementations régissant les pouvoirs d'investigation des autorités chargées de la protection des données, sans préjuger en aucune façon des pouvoirs d'inspection de chaque autorité de protection des données ;

Le Groupe sera averti en temps opportun par l'autorité compétente de protection des données de ces audits.

Ils seront effectués dans le respect total de la confidentialité et du secret des affaires et devront être ciblés uniquement sur la vérification du respect des règles d'entreprise contraignantes.

### 1.1. Quelle entité (service au sein du groupe) décide du plan/programme d'audit ?

Le plan et le programme d'audit est décidé par le Délégué à la Protection des Données (DPO).

Cette décision peut être prise conjointement avec l'auditeur interne de l'entreprise, le service chargé de la Sécurité et le Responsable des Traitements.

### 1.2. Quelle est l'entité qui mènera l'audit ?

Les audits peuvent être menés par le Délégué à la Protection des Données (DPO) ou une entreprise externe.

### 1.3. Quelle est la fréquence de l'audit ?

Les audits seront effectués dans chacune des entités du Groupe avec une périodicité annuelle.



G2S Group <b>be ys</b>	Protection des données à caractère personnel – Audit des traitements de données à caractère personnel	<b>PR</b> Procédure
------------------------	---	------------------------

Toutefois, le DPO peut demander à ce que des audits supplémentaires soient effectués, notamment s'il pense que certaines obligations liées aux règles contraignantes d'entreprise ne sont pas appliquées.

#### 1.4. Champ couvert par l'audit ?

Le programme d'audit couvre adéquatement les différents aspects des règles d'entreprise contraignantes, notamment les méthodes visant à garantir que des mesures correctives ont été mises en œuvre.

Les audits couvrent la gestion de toutes les données à caractère personnel, le respect des principes de protection des données, ainsi que le respect des obligations liées au BCR.

Et ce quel que soit le système applicatif ou la base de données dans laquelle des données à caractère personnel seraient présentes.

Les audits couvrent aussi tous les transferts de données à caractère personnel effectués au sein des entités du Groupe, ainsi que tous les transferts ultérieurs à la mise en place des BCR.

Si des données à caractère personnel sont transférées vers des entités en dehors de l'Union Européenne autres que les filiales soumises au respect des BCR, les audits doivent vérifier le bon respect des Clauses Contractuelles Types signées entre les entités du Groupe et le prestataire (sous-traitant ou Responsable de Traitement).

Lorsque la législation locale applicable à une Entreprise du Groupe, exige un degré de protection des données personnelles supérieur à celui exigé par les BCR, ladite législation locale prime sur les BCR.  
Dans tous les cas, les données seront traitées conformément au droit applicable visé à l'article 4 de la directive 95/46/CE, ainsi qu'à la législation locale.

Les audits permettent de vérifier s'il y a ou non conflit entre les BCR et les législations locales de protection des données.

#### 1.5. Quelle est l'entité qui recevra les résultats des audits ?

Les résultats des audits devront être présentés aux membres de la Direction du Groupe.

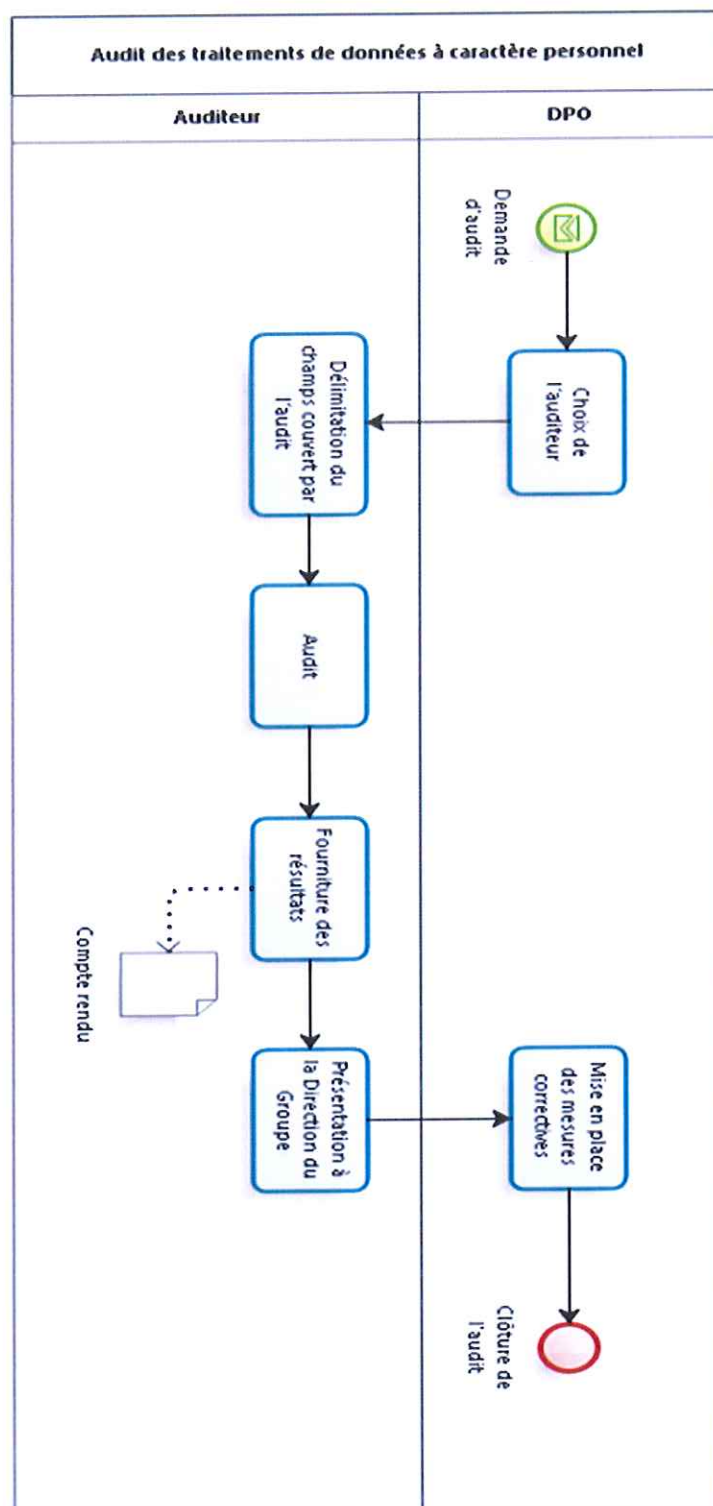
Dans l'hypothèse où les audits seraient effectués par une entreprise externe, les résultats devront être fournis au Délégué à la Protection des données.

Les résultats des audits doivent être tenus à la disposition des Autorités de protection des données, qui pourront donc y accéder à leurs demandes.





## 2. Description de la Procédure

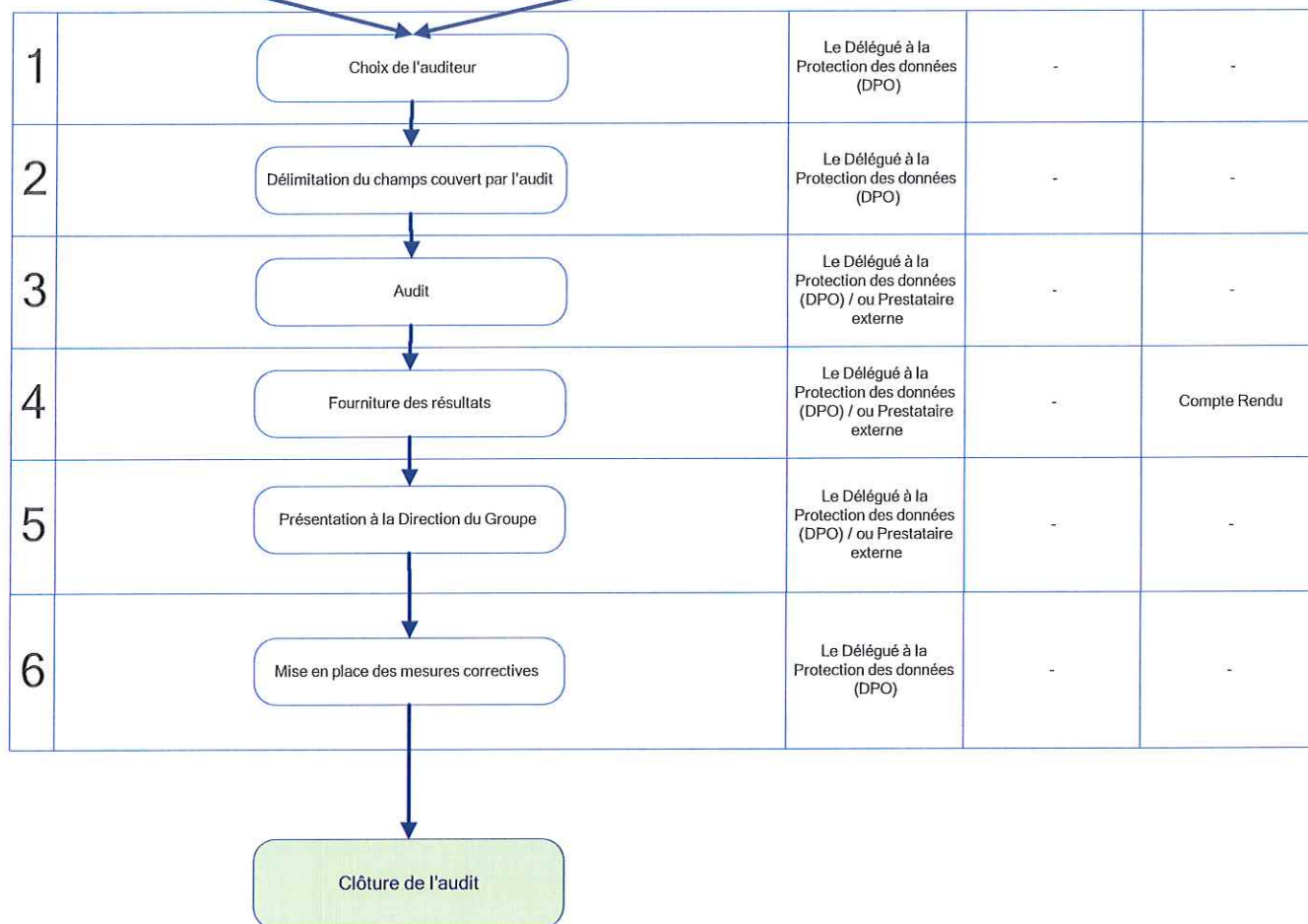


Logigramme détaillée des activités portées par la procédure :



G2S Group <b>be ys</b>	Protection des données à caractère personnel – Audit des traitements de données à caractère personnel	<b>PR</b> Procédure
------------------------	---	------------------------

Nom procédure	Responsable	Outils	Documents
---------------	-------------	--------	-----------



[illegible]

G2S Group

be

ys

Protection des données à caractère personnel – Audit des traitements de données à caractère personnel

PR

Procédure

N° étape	Acteur	Entrée ou déclencheur	Action (objectif et description)	Sortie ou livrable	Outil(s)
1. Choix de l'auditeur	Le Délégué à la Protection des données (DPO)	Lorsque l'audit annuel doit être effectué ou si le DPO décide d'un audit exceptionnel	Soit c'est le DPO lui-même qui effectue l'audit, soit il décide de passer par un prestataire externe.		
2. Délimitation des champs couverts par l'audit	Le Délégué à la Protection des données (DPO)	Lorsque le choix de l'auditeur a été fait	Le DPO défini ce qui doit être auditer, selon si on est dans le cadre de l'audit annuel (qui est complet) ou si c'est un audit exceptionnel.		
3. Audit	Le Délégué à la Protection des données (DPO) / ou Prestataire externe	Lorsque le champ couvert par l'audit a été défini	Audit des traitements de données à caractère personnel.		
4. Fourniture des résultats	Le Délégué à la Protection des données (DPO) / ou Prestataire externe	Fin de l'audit	L'auditeur rédige un compte rendu d'audit avec les manquements relevés, les points positifs et les préconisations.	Compte rendu	
5. Présentation à la Direction du Groupe	Le Délégué à la Protection des données (DPO) / ou Prestataire externe	Dès la réception du compte rendu	Suite à la réception du compte rendu, le DPO en collaboration avec les services concernés définissent des mesures correctives. Puis le compte rendu et les mesures correctives sont présentés à la Direction du Groupe pour validation.		
6. Mise en place des mesures correctives	Le Délégué à la Protection des données (DPO)	Suite à la présentation du compte rendu à la Direction du Groupe	Le DPO collabore avec tous les services concernés afin de mettre en œuvre les mesures correctives.		





G2S Group <b>be ys</b>	Protection des données à caractère personnel – Audit des traitements de données à caractère personnel	<b>PR</b> Procédure
------------------------	---	------------------------

### 3. Moyens et Outils

---

Le Délégué à la Protection des Données bénéficie d'un budget lui permettant de mettre en application les obligations liées au respect des règles contraignantes d'entreprise (BCR).

Ce budget lui permet aussi d'effectuer les audits ou de pouvoir choisir un prestataire externe qui en sera chargé.




G2S Group <b>be ys</b>	Protection des données à caractère personnel – Audit des traitements de données à caractère personnel	<b>PR</b> Procédure
------------------------	---	------------------------

## 4. Acteurs

---

Dans le cadre de cette procédure les acteurs sont :

- Le Délégué à la protection des données (DPO)
- Le Prestataire externe
- La Direction du Groupe

Laurent Caredda		13/01/17
-----------------	---	----------

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

