

# **Procédure de protection des données personnelles**

**C6.PLC.01**

**Version 1.0**

**Date d'entrée en vigueur : 25/05/2018**

## Notifications juridiques

**EuroChem Group, textes non publiés. Tous droits réservés.**

Ces textes contiennent des informations confidentielles concernant EuroChem et ne pourront être ni copiés ni stockés dans un système de recherche documentaire, ni transférés, utilisés, diffusés, traduits ou retransmis sous quelle que forme ou par quelque moyen que ce soit, électroniquement ou mécaniquement, entièrement ou partiellement, sans le consentement exprès et écrit du titulaire des droits d'auteur.

### **Marques commerciales et de service**

EuroChem, la marque EuroChem, et tout autre mot ou symbole utilisés afin d'identifier les produits et services décrits dans ces textes, sont soit des marques commerciales ou de service appartenant à EuroChem et ses concédants de licence, ou sont alors la propriété de leurs détenteurs respectifs.

Ces marques ne pourront être ni copiées, ni imitées ou utilisées, entièrement ou partiellement, sans l'autorisation expresse et écrite d'EuroChem. De plus, les couvertures, en-têtes de pages, graphismes, icônes ou autres éléments graphiques qui pourraient être des marques commerciales ou de services ou dénominations commerciales d'EuroChem, ne pourront être ni copiées, ni imitées, utilisées, entièrement ou partiellement, sans la permission préalable, expresse et écrite, d'EuroChem.

Une liste complète des marques d'EuroChem peut être consultée sur la page : <http://www.eurochemgroup.com>.

## Sommaire

Nom	Procédure de protection des données personnelles
ID	C6.PLC.01
Superviseur de la procédure	A.A. Ilyin, Chief Financial Officer, EuroChem Group
Propriétaire de la procédure	V.V. Sidnev, General Counsel, EuroChem Group
Développé par	E.V. Kholmanskikh, Chief Compliance Officer, EuroChem Group
Version	1.0
Date d'entrée en vigueur	25/05/2018
Date d'approbation	25/05/2018

## Revision history

Version	Effective date	Purpose	Revision details
1.0	25/05/2018		N/A

**Contents**

<b>Notifications juridiques .....</b>	<b>2</b>
<b>1. Termes et définitions .....</b>	<b>6</b>
<b>2. Champ d'application .....</b>	<b>8</b>
2.1. Objectifs .....	8
2.2. Champs d'application et exigences obligatoires et légales .....	8
<b>3. Dispositions générales .....</b>	<b>9</b>
3.1. Objectifs de la procédure .....	9
3.2. Principes de la procédure .....	9
<b>4. Mesures de protection des données .....</b>	<b>10</b>
4.1. Un traitement juste et en conformité avec la loi .....	10
4.1.1. Données concernant les salarié(e)s .....	11
4.1.2. Données relatives aux tiers .....	12
4.1.3. Consentement .....	14
4.2. Protection des droits de la personne concernée .....	15
4.3. Sécurité des Données Personnelles .....	17
4.4. Violation des Données Personnelles .....	19
4.5. Conservation et suppression de données .....	20
4.6. La formation du personnel .....	21
4.7. Registre des opérations de traitement .....	21
Chaque entreprise du Groupe a identifié les Données Personnelles qu'il traite et contrôle, et les liste dans un registre (annexe 4). .....	21
Ce registre garantit que les entreprises du Groupe sont en conformité avec les obligations requises sous le « RGPD » : .....	21
4.8. Transfert de données .....	22
4.9. Evaluation de l'impact de la Protection des Données .....	23
4.10. Les Responsables de la Protection des Données .....	23
4.10.1. Les responsabilités des Responsables de la Protection des Données .....	24
<b>5. Gouvernance de la procédure .....</b>	<b>26</b>
5.1. Responsabilité .....	26
5.2. Contrôle .....	26

<b>5.3. Confidentialité</b> .....	<b>26</b>
<b>5.4. Révision de la Procédure</b> .....	<b>27</b>
<b>5.5. Réclamations et questions</b> .....	<b>27</b>
<b>Annex 1. Références</b> .....	<b>28</b>
<b>Annexe 2. Registre de violations de Données Personnelles</b> .....	<b>29</b>
<b>Annexe 3. Planning de conservation</b> .....	<b>30</b>
<b>Annexe 4. Registre des données</b> .....	<b>31</b>

## 1. Termes et définitions

Sauf indication contraire, les mots et expressions définies dans cette Procédure de Protection de Données Personnelles sont identiques et ont exactement les mêmes significations que celles définies dans le Code de Conduite de la Procédure de Compliance.

En complément, les définitions suivantes s'appliqueront :

Term	Definition
“Données personnelles”	Signifie toute information relative à un sujet identifié ou identifiable ; il peut s’agir d’une grande diversité d’identifiants personnels, comprenant le nom d’une personne naturelle, son numéro de téléphone (professionnel), une adresse e-mail (professionnelle), un numéro d’identification, une donnée de localisation, une identification internet, etc....
“Donnée sensible”	Signifie donnée personnelle concernant l’origine raciale ou ethnique, opinions politiques, religieuses ou philosophiques, l’appartenance à un syndicat professionnel ; traitement de données génétiques ou biométriques dans le but d’identifier une personne naturelle, données relatives à sa santé ou sa vie ou orientation sexuelles.
“Contrôleur des données” ou “Contrôleur”	Signifie la personne naturelle ou légale, autorité publique, agence ou tout autre organisme qui, seul ou ensemble avec des tiers, détermine le but et les moyens mis en place pour le traitement des données personnelles.
“Processeur de données” ou “Processeur”	Signifie la personne naturelle ou légale qui traite les données personnelles pour le compte du contrôleur.
“Personne concernée”	Signifie toute personne vivante concernée par les données personnelles détenues par le Groupe.
“Traitement”	Signifie toute opération ou ensemble d’opérations effectuées à partir des données personnelles, que ce soit par des moyens automatisés ou non, tels que collection, enregistrement, organisation, structuration, stockage, adaptation ou modification, recherche, consultation, utilisation, diffusion, transmission ou autre mise à disposition, combinaison, restriction, suppression ou destruction.
“Violation des données personnelles”	Signifie violation de la sécurité des données personnelles transmises, stockées ou autrement traitées, entraînant ainsi leur destruction, perte, altération accidentelle ou illégale, leur publication ou mise à disposition non autorisée.
“Consentement de la personne concernée”	Signifie toute indication donnée librement, spécifiquement et clairement par la personne concernée, par laquelle elle donne son

	consentement au traitement des données personnelles, soit expressément, soit par une autre action claire et affirmative.	
“Responsable UE de la Protection des Personnelles”	Signifie ‘employé du Groupe’ responsable du déploiement de la procédure au sein des territoires du Groupe appartenant à l’UE .	
“Responsable Global de la Protection des Personnelles”	Signifie employé du Groupe responsable du déploiement de la procédure au sein des territoires du Groupe.	
“Responsable Local de la Protection des Personnelles”	Signifie employé du Groupe responsable du traitement des données au sein d’une des sociétés membres du Groupe.	
“Accord sur le traitement des Données Personnelles”	Signifie tout accord conclu entre le Groupe et toute autre partie concernant le déploiement de la procédure au sein du Groupe.	
“Délai de conservation”	Signifie le délai exact à respecter pour la conservation des données (ou documents).	

## **2. Champ d'application**

### **2.1. Objectifs**

Cette procédure a pour objectif de fixer le cadre et les principes de base pour la protection et le traitement des données personnelles au sein du Groupe.

En tant qu'employeur, client et fournisseur, chaque membre du Groupe collecte et utilise des données personnelles concernant ses employés, ses contacts d'affaires, ses clients, prospects, etc. Le traitement des données personnelles étant indispensable à nos activités, le Groupe considère que la protection des droits personnels et de la sphère privé de chaque individu est la base de toute relation de confiance. C'est pourquoi le Groupe souhaite être exemplaire dans la Protection et le traitement des Données Personnelles.

Il est crucial pour le Groupe d'être en conformité avec les obligations pour la Protection des Données Personnelles dans les pays où ses affaires sont conduites et où les personnes concernées résident. Tous les membres du Groupe doivent se conformer aux règles en vigueur localement et relatifs au contrôle et au traitement des données personnelles.

La priorité du Groupe est de mettre en place des standards universels et mondialement applicables pour le traitement des données personnelles. Cette Procédure de Protection des Données sert de cadre général et est applicable à travers le Groupe. Etant donné les différents règlements en vigueur, et la diversité des activités du Groupe, l'implémentation de ces principes de Protection des Données varie légèrement entre les différents membres du Groupe.

Cette Procédure doit être portée à la connaissance de tous les employés du Groupe devant se conformer avec la Procédure et ses exigences. D'autre part, la procédure s'applique également aux tiers ayant à faire aux membres du Groupe et qui ont ou pourraient avoir accès aux Données Personnelles. Ces tiers sont censés avoir lu et compris la présente procédure et doivent être en conformité avec elle.

### **2.2. Champs d'application et exigences obligatoires et légales**

Les pays dans lesquels le Groupe intervient peuvent être divisés en 3 grands groupes en fonction de leur situation : UE, Russie et autres pays.

A l'exception des sièges en Suisse et en Russie, certains membres du Groupe sont situés dans l'UE. Le Règlement sur la Protection de Données (Règlement EU 2016/679, General Data Protection Regulation ou « RGPD ») sont obligatoires et s'appliquent de façon identique à tous les pays membres de l'UE.



Le champ d'application du RGPD dépasse les frontières de l'UE, puisqu'il s'applique également aux membres du Groupe établis en dehors de l'UE, si la personne concernée réside dans un des pays de l'UE.

Par la présente Procédure de Protection des Données Personnelles, le Groupe s'engage par lui-même à appliquer à la ligne les principes et obligations relevant du RGPD. Cependant, les membres individuels du groupe doivent également être en conformité avec les règles locales. La présente Procédure de Protection complète simplement les règles applicables localement. D'autre part, les règles localement en vigueur l'emportent sur la présente Procédure de Protection des Données au cas où les deux entreraient en conflit ou au cas où les règles locales présenteraient des exigences plus strictes. Quelques exemples de règles applicables aux membres du Groupe sont :

- Loi fédérale № 152-FZ sur les données personnelles datant de 2006 (applicable pour la Russie);
- Loi fédérale sur les données personnelles (FADP) datant du 19 juin 1992 (applicable pour la Suisse);
- Législation locale relative au Code de Gouvernance d'Entreprise et au délai de conservation des données.

### **3. Dispositions générales**

#### **3.1. Objectifs de la procédure**

Les principaux objectifs de la procédure sont les suivants :

- Protéger la liberté et les droits de toutes les personnes concernées et de les en informer ;
- Traiter les données personnelles correctement ;
- Eviter toute violation des Données Personnelles et de leur sécurité de manière générale ;
- Améliorer la prise de conscience relative à la protection des données personnelles de façon générale.

#### **3.2. Principes de la procédure**

Tout traitement de Données Personnelles doit être effectué en conformité avec les principes de protection des données comme indiqué dans le RGPD.

La Procédure du Groupe est établie afin d'assurer la conformité avec ces principes.

En somme, en tant que Groupe nous nous engageons à être en phase avec les principes suivants :

**Le principe d'équité : nous nous engageons à traiter les Données Personnelles uniquement après en avoir informé la personne concernée et à condition que le traitement se fasse en conformité avec la loi.**

**Le principe de la limitation de la finalité : nous nous engageons à traiter les données personnelles uniquement dans un but spécifique, et pour des raisons explicites et légitimes, et ne procéderons à aucun traitement incompatible avec ces objectifs.**

**Le principe de minimisation : nous traitons uniquement les données personnelles adéquates, importantes et en nous limitant à celles qui sont nécessaires pour atteindre la finalité que nous nous sommes fixée.**

**Le principe d'exactitude : nous ne traitons que des données exactes, et, si nécessaire, actualisées. Nous prendrons toutes les mesures nécessaires et raisonnables afin de garantir que les données personnelles incorrectes soient supprimées ou alors rectifiées sans attendre.**

**Le principe de limitation des traitements : nous conservons l'ensemble des données personnelles sous une forme permettant l'identification des personnes concernées uniquement pour la durée nécessaire afin d'atteindre les objectifs pour lesquels les données sont traitées.**

**Le principe de sécurité : nous traitons les données de façon à ce que la sécurité de celles-ci soient respectées : protection contre tout traitement non autorisé ou enfreignant la loi, perte accidentelle, destruction ou endommagement, en utilisant toutes les mesures techniques et organisationnelles possibles.**

**Le principe de la traçabilité : nous serons responsables à tout moment et capables de faire preuve de conformité avec les principes de Protection des Données susmentionnées, aussi bien vis-à-vis des autorités compétentes que vis-à-vis des personnes concernées.**

## **4. Mesures de protection des données**

**L'engagement du Groupe concernant l'implémentation des principes de Protection des Données Personnelles est illustrée par les mesures suivantes que nous avons prises :**

### **4.1. Un traitement juste et en conformité avec la loi**

**Le Groupe garantit que les données sont collectées et traitées de façon juste et en conformité avec la loi. Nous prenons toutes les mesures nécessaires afin de tenir les données à jour et exactes et les conserverons uniquement pour une durée définie au préalable.**

Le Groupe garantit que les données ne seront utilisées que sur la base décrite ci-après, en conformité avec la loi, et en fonction de la catégorie à laquelle la personne concernée appartient.

#### **4.1.1. Données concernant les salarié(e)s**

« Données concernant les salariés » signifie toute donnée traitée par les membres du Groupe, relative aux employés et, si nécessaire, leurs conjoint(e)s et enfants. Toutefois, les données concernant les salarié(e)s ne se limitent pas uniquement aux données personnelles des employés actuellement sous contrat. Le Groupe traite d'autres catégories de données relatives aux ressources humaines, comme par exemple celles concernant les retraités et les candidats.

Toutes les données concernant les salariés sont collectées par le Groupe dans lequel le salarié est embauché. L'employeur est considéré comme étant le Contrôleur des données, ce qui signifie que le Groupe détermine les objectifs et les mesures de traitement de ces données.

##### **1. Traitement des données en conformité avec la loi**

Dans la relation avec l'employeur, la grande majorité des activités de traitement est justifiée par la nécessité de la mise en place d'un contrat de travail : les membres du Groupe ne seraient pas en mesure d'exécuter correctement leurs obligations liées aux contrats de travail sans traiter les données de leurs salariés.

Quelques-unes de ces données sont justifiées par une obligation légale : dans tous les pays dans lesquels les membres du Groupe font leurs affaires, il y a une obligation légale de traiter certaines données personnelles des salariés, telles que les informations relatives à la Sécurité Sociale, les assurances, le paiement des salaires etc.

Certaines activités de traitement des données peuvent également être justifiées par des accords collectifs. Les accords collectifs sont des accords conclus pour définir la grille des rémunérations, ou d'autres accords entre l'employeur et les représentants du personnel, respectant le cadre imposé par la Loi du Travail. Les accords doivent couvrir les objectifs spécifiques de l'opération de traitement prévue, et doivent être établis en respectant les paramètres de la loi sur la Protection des données.

Chaque membre du Groupe peut dans pratiquement tous les cas s'appuyer sur les intérêts légitimes du traitement des données, puisque celui-ci est nécessaire au bon fonctionnement de ses affaires. Un exemple : lors de la réception d'une candidature, les membres du Groupe n'ont pas conclu de contrat avec les candidats, mais doivent procéder à l'évaluation des candidats potentiels (en particulier lorsque le candidat initie la procédure en contactant l'un des membres du Groupe).

Dans un nombre limité de cas, les opérations de traitement pourront être justifiées par un consentement exprès donné par l'employé (p.ex. publication d'une interview ou d'une photographie dans un journal interne etc...)

Chaque membre du Groupe est seul responsable de l'identification des opérations de traitement.

## **2. Traitement juste**

Une vue d'ensemble de la façon dont nous traitons les données de nos employés se trouve dans nos procédures plus détaillées. Ici nous donnons uniquement une vue globale de quelques-uns des aspects de nos opérations de traitement :

**Minimisation** : le Groupe garantit que les données des employées traitées sont limitées à leur stricte minimum.

**Exactitude** : le Groupe garantit que les données de tous ses employés sont régulièrement actualisées au niveau global et que chaque employé peut à tout moment demander la mise à jour ou la modification de ses données.

**Limitation de stockage** : toutes les données des employés seront traitées tout au long de la durée du contrat de travail. A la rupture du contrat de travail, et dès que la durée de conservation requise est écoulée, une large partie de ces données est détruite, sauf si autrement prévu par la loi, ou si la personne concernée a expressément donné son accord pour la conservation de ses données pour d'autres opérations spécifiques de traitement.

**Sécurité** : toutes les données personnelles sont traitées de manière sécurisée. Ex. : Un accès aux données est accordé uniquement si nécessaire ; les données du Groupe sont habituellement transmises de façon anonyme à des tiers ; etc...

**Traitement des données sensibles** : les données sensibles (telles que les données relatives aux origines raciales et ethniques, des croyances politiques religieuses et philosophiques, appartenance aux syndicats, données relatives à la santé et à la vie sexuelle des personnes concernées) seront traitées avec tout le soin nécessaire.

Le Groupe limite le traitement automatique des données personnelles à son stricte minimum.

Si les données personnelles sont traitées automatiquement et font partie du contrat de travail, et si des détails personnels sont évalués (p.ex. évaluation des compétences professionnelles), ce traitement automatique ne pourra servir comme seule base pour d'éventuelles décisions qui pourraient être préjudiciables pour l'employé concerné.

Chaque membre du Groupe est seul responsable du juste traitement des données de ses salariés.

### **4.1.2. Données relatives aux tiers**

Les 'données relatives aux tiers' concernent les clients, sous-traitants, contractants, fournisseurs, partenaires d'affaires, visiteurs des sites web, etc. Il s'agit ici de données professionnelles qui ne 12

comportent aucune donnée sensible ; toutefois, les adresses mail et numéros de téléphones seront considérés comme étant des données personnelles.

A partir du moment où le Groupe collecte les données directement de la personne concernée, il agira en tant que Contrôleur des Données. La nature des affaires du Groupe pourrait nécessiter une collecte des données à partir d'une autre source. Dans ce cas le groupe sera uniquement « Processeur des Données », et non Contrôleur des Données, sauf si un autre accord a été conclu.

## **1. Opérations de traitement en conformité avec la loi.**

Dans la relation contractuelle, la grande majorité des activités de traitement sont justifiées par la nécessité de la mise en place d'un contrat : les membres du Groupe ne seraient pas en mesure d'exécuter correctement leurs obligations du contrat sans être en mesure de traiter les données pertinentes.

Quelques-unes de ces données sont justifiées par une obligation légale : dans certains pays dans lesquels les membres du Groupe font leurs affaires, il y a une obligation légale de traiter certaines données personnelles des fournisseurs.

Le Groupe peut dans pratiquement toutes les instances s'appuyer sur un intérêt légitime de traiter les données personnelles, puisque celles-ci sont nécessaires au bon fonctionnement de ses affaires.

Dans un nombre très limité de cas, le traitement des données pourrait être autorisé par un consentement exprès donné par le tiers (p.ex. pour la réception d'une newsletter du Groupe, etc.).

Dans la mesure où les données des tiers sont contrôlées par le Groupe (c'est-à-dire un membre du Groupe détermine les finalités et les moyens du traitement des données), le Groupe sera responsable de la détermination des principes de traitement en conformité avec la loi.

## **2. Traitement juste**

Une vue d'ensemble détaillée du traitement des données des tiers se trouve dans les procédures plus détaillées. D'une manière générale, les mêmes principes que ceux décrits dans le paragraphe 4.1.1. pour le traitement des données des salariés, s'appliqueront.

Les principes suivants additionnels sont à noter :

Lorsque les données traitées sont collectées via le site Web et/ou d'autres outils internet du Groupe, les personnes concernées en seront informées par une déclaration de confidentialité, et, si applicable, une notification sur les « cookies ». La déclaration de confidentialité et l'information sur les cookies seront intégrées pour être faciles à identifier, directement accessibles et disponibles pour les personnes concernées.

Dans la mesure où nous créons des profils utilisateurs (tracking) sur nos sites internet, les personnes concernées seront systématiquement informées en conformité avec la déclaration de confidentialité. Le tracking personnel sera effectué uniquement s'il est autorisé selon la loi nationale en vigueur ou après consentement exprès de la personne concernée.

Si les sites internet ou applications permettent d'accéder aux données personnelles dans leurs espaces accessibles uniquement pour les utilisateurs enregistrés, l'identification et l'authentification de la personne concernée offriront une protection suffisante pendant l'accès.

**Marketing Digital** : le Groupe réalisera des stratégies de marketing digital dans un contexte 'business to business', et sans nécessité légale d'obtenir un consentement préalable à la conduite des actions de marketing digital vis-à-vis des individus, à condition que ceux-ci aient la possibilité de se désinscrire.

Toutefois, de manière générale, le Groupe s'efforcera d'obtenir systématiquement un consentement avant d'envoyer du matériel promotionnel ou de marketing direct à une tierce personne.

Dans la mesure où le Groupe est le Contrôleur des données des tiers, il sera responsable de la détermination des principes de traitement en conformité avec la loi.

### **4.1.3. Consentement**

Dans la mesure où le Groupe s'appuie sur le principe du consentement comme base de traitement en conformité avec la loi, les conditions suivantes seront applicables :

Les déclarations de consentement seront soumis librement, par écrit et en conformité avec les règles locales. Tout consentement qui ne respecte pas ces conditions, est considéré comme étant 'nul'. La déclaration de consentement doit être obtenu par écrit ou par voie électronique, afin de pouvoir être documenté. Avant de donner son consentement, la personne concernée sera informé de la nature des opérations de traitement. La personne concernée peut retirer son consentement à n'importe quel moment.

Concernant les données sensibles, un consentement écrit des personnes concernées est nécessaire, sauf s'il existe une base légale alternative.

Dans la plupart des cas, le consentement pour le traitement des données personnelles et sensibles est obtenu par le Groupe en utilisant des documents standards.

## 4.2. Protection des droits de la personne concernée

Chaque membre du Groupe garantit que chaque personne concernée dont nous traitons les données au sein du Groupe peut exercer les droits individuels suivants :

**Le droit d'être informé :**

La procédure présente une vue globale des principes générales sous lesquels le Groupe traite les Données Personnelles. Il est partagé avec les personnes concernées au moment où leur données personnelles sont collectées (et dans la mesure où le Groupe est le Contrôleur), et il peut être consulté sous [www.eurochemgroup.ru](http://www.eurochemgroup.ru).

Cependant, au cas où la personne concernée le demande expressément, le membre concerné du Groupe (c'est-à-dire le Contrôleur ou Processeur des Données Personnelles) mettra à la disposition de la personne concernée toutes les informations nécessaires dans une forme concise, transparente et facilement accessible. Le Groupe se réserve le droit de décliner toute demande d'information si la personne concernée dispose déjà de cette information ou si l'effort pour la mettre à disposition serait disproportionné.

**Sur demande, le Groupe fournira les informations suivantes :**

- 1) Nom et coordonnées de l'entité
- 2) La finalité du traitement
- 3) La base de traitement en conformité avec la loi
- 4) Les catégories de Données personnelles obtenues
- 5) Les destinataires ou catégories de destinataires des données personnelles
- 6) Les détails et transferts des données personnelles vers d'autres pays ou organisations internationales (si applicable)
- 7) Les délais de conservation des données personnelles
- 8) Les droits dont disposent les personnes concernées en respectant le traitement
- 9) Le droit de retirer un consentement (si applicable)
- 10) Le droit de porter plainte auprès d'une autorité de surveillance.

**Le droit d'accès :**

Afin d'assurer que les personnes concernées puissent vérifier la conformité avec la loi des moyens de traitement des données, le Groupe leur accorde le droit d'obtenir une confirmation que leurs données sont traitées, ainsi qu'un accès aux données personnelles et toute autre information complémentaire. Les deux parties se mettront d'accord sur le type d'accès accordé.

#### **Le droit de modification :**

Lorsqu'un membre du Groupe traite des données personnelles non exactes ou incomplètes, la personne concernée peut demander que ses données soient rectifiées ou complétées. Toutefois, le Groupe se réserve le droit de refuser une demande de rectification si une règle applicable l'y autorise.

#### **Le droit de suppression et le droit de limiter les traitements**

**Les personnes concernées ont le droit de suppression des données personnelles des registres du Groupe, si**

- 1) Les données personnelles ne sont plus nécessaires pour la finalité pour laquelle elles ont été collectées à l'origine ;**
- 2) Un consentement est la base légale de détention de ces informations pour un membre du Groupe, et lorsque la personne concernée retire son consentement ;**
- 3) Un membre du Groupe s'appuie uniquement sur son intérêt légitime comme base pour le traitement des données, et lorsque la personne concernée s'oppose au traitement de ces données ; et lorsque l'intérêt légitime n'est pas primordial pour la continuité du traitement ;**
- 4) Un membre du Groupe traite les données personnelles dans un but de marketing direct ;**
- 5) Un membre du groupe a traité les Données Personnelles sans se conformer à la loi.**

**Comme alternative à une suppression des données personnelles, la personne concernée peut demander au membre du Groupe concerné de restreindre le traitement de ses données personnelles à un simple stockage de données, sans s'en servir. Une telle restriction peut être demandée si :**

- 1) La personne concernée conteste l'exactitude de ses Données Personnelles et un membre du Groupe vérifie l'exactitude des données ;**
- 2) Les données ont été traitées en non-conformité avec la loi, et la personne concernée ne souhaite pas la suppression mais la restriction de traitement ;**
- 3) Un membre du Groupe n'a plus besoin des Données Personnelles, mais la personne concernée souhaite que les données soient conservées afin d'exercer une action judiciaire.**
- 4) La personne concernée a exprimé son objection à un membre du Groupe au traitement de ses données, mais le Groupe considère que ses finalités légitimes sont prépondérantes à celles de la personne concernée.**

#### **Le droit de portabilité des données :**



Sous certaines conditions très strictes, la personne concernée pourrait demander à un membre du Groupe de lui fournir l'ensemble des données personnelles sous une forme structurée, communément utilisées et lisible par une machine.

Cela devrait permettre à la personne concernée de transmettre ses données à un autre organisme. Si cela est techniquement faisable, la personne concernée pourra demander un transfert direct à un autre organisme.

Le droit de portabilité s'applique uniquement :

- 1) Aux Données Personnelles qu'un individu a fourni au Contrôleur ;
- 2) Lorsque le traitement est basé sur le consentement ou pour la performance d'un contrat ;
- 3) Lorsque le traitement est effectué de façon automatisée.

Le droit à l'opposition :

Lorsqu'une personne concernée s'oppose au traitement de ses données personnelles pour des motifs « relatifs à leur situation particulière », la personne concernée a le droit de s'opposer à :

- 1) Un traitement basé sur ses intérêts légitimes
- 2) Actions de marketing direct (y compris profiling)

Dans ce cas, le membre du Groupe stoppera le traitement des données personnelles, sauf si :

- 1) Il a des raisons légitimes pour le traitement qui passent avant les intérêts, droits et libertés de la personne concernée.
- 2) Le traitement est fait pour exercer ou défendre d'éventuelles actions en justice.

Toute demande d'exécution des droits susmentionnées, doit être adressée au Responsable de la Protection des Données. Sauf si stipulé autrement sous une loi applicable, chaque demande doit être faite par écrit.

Sauf si autrement stipulé par une règle applicable, la réponse à chaque demande doit être fournie sous 30 jours suite à la réception de la demande écrite par la personne concernée.

Une vérification appropriée doit confirmer que le demandeur est bien la personne concernée ou son représentant légal officiel.

Sauf si autrement stipulé par une règle applicable, chaque demande est traitée de manière gratuite, sauf si la demande est jugée inutile ou excessive.

### **4.3. Sécurité des Données Personnelles**

Le Groupe s'engage à se conformer avec ce qui est considéré comme "best industry practice" pour la sécurité des systèmes informatiques.

En complément, chaque entreprise du Groupe a adopté des mesures physiques, techniques et organisationnelles afin de garantir la sécurité des données personnelles. Cela comprend des mesures de prévention contre la perte ou l'endommagement, altération non autorisée, accès ou traitement, et d'autres risques qui pourraient survenir par action humaine ou l'environnement physique ou naturel.

Tandis que les mesures de sécurité varient et dépendent des membres du Groupe, les mesures suivantes sont considérées comme étant des garanties minimum de sécurité :

Toutes les données personnelles sont traitées avec les mesures de sécurité les plus élevées et doivent être stockées :

Dans une pièce fermée à clé et avec accès contrôlé ;

et/ou Dans un tiroir ou une armoire fermés à clé ; et/ou

Si informatisées, protégées par un mot de passe conforme avec les exigences du Groupe ; et/ou

Stockées sur un support informatique crypté, et pouvant être supprimées à tout moment.

Des registres manuels ne pourront être gardés dans des endroits accessibles par les membres du personnel non autorisés, et ne pourront être emportés en dehors des surfaces de bureau sans autorisation spéciale. Dès que les registres manuels ne sont plus requis pour le travail au quotidien, ils doivent être archivés de façon sécurisée.

Les données personnelles seront détruites ou éliminées uniquement en conformité avec le planning de conservation.

Le Groupe doit s'assurer que les Données Personnelles ne sont pas rendues accessibles à des tiers, y compris membres de la famille, amies, autorités gouvernementales sauf si requis par la loi. Chaque demande de fournir des données pour une de ces raisons doit être accompagnée par des documents appropriés et doit être autorisée par le Responsable pour la Protection des Données.

Chaque membre du Groupe s'assure que l'ensemble des employés adhèrent à cette procédure et au Code de Conduite. D'autre part, chaque membre du Groupe garantit que ses employés se sentent responsables dans l'exécution de la Procédure et sont correctement formés et accompagnés (voir également l'article 4.6).

#### **4.4. Violation des Données Personnelles**

**Une violation des données personnelles est une violation de la sécurité entraînant une destruction, perte, altération ou transmission non autorisée, ou accès non autorisé à, des Données Personnelles transmises, stockées ou autrement traitées. De tels incidents pourraient se produire techniquement ou physiquement.**

**Etant donné que de telles violations se produisent habituellement de façon surprenante, chaque membre du Groupe a préparé les actions nécessaires afin d'éviter que d'éventuelles violations entraînent des conséquences catastrophiques.**

**Chaque membre du Groupe a mis en place des procédures solides de détection, d'investigation et de reporting, relatives aux éventuelles violations.**

**Celles-ci sont décrites dans la procédure du Groupe concernant les violations des données. En complément, chaque membre du Groupe garde un registre des violations, dans lequel il conserve les informations sur les faits relatifs à toute violation de données personnelles, les effets des violations et les actions mises en place pour y remédier.**

**Tandis que les procédures des différents membres peuvent varier, chaque procédure de violation des données comportera les étapes suivantes :**

**Tous les employés doivent informer leur responsable hiérarchique immédiatement sur d'éventuels cas de violation de cette procédure de protection des données ou autres règles sur la protection des données personnelles (incidents de Protection des Données). Le responsable hiérarchique en informera à son tour le Responsable Local de la Protection des Données, le responsable « UE » de la Protection de Données ainsi que le Responsable Global de la Protection des Données.**

**Le Responsable de la Protection des Données décide si l'incident représente effectivement une forme de violation des données. Par exemple, clés USB perdues, ordinateurs portables volés, infections par des virus ou bases de données piratées sont considérés comme des violations de données personnelles. Une menace ou insuffisance constatées dans les mesures de sécurité, telles que des mots de passe faibles ou des firewalls inefficaces, ne sont pas considérées comme des violations de données personnelles dans la mesure où aucune donnée personnelle n'a fuitée.**

**S'il s'avère que l'incident constaté sur les données personnelles est effectivement une violation, les Responsables de la Protection des Données Personnelles enquêteront sur l'ampleur de cette violation, le nombre de personnes concernées par l'incident ; si la violation peut conduire à une menace des libertés et droits des personnes concernées et si les données impactées sont des données sensibles ; si les données compromises ont été sécurisées (cryptées ou autre) ; si d'autres parties ont pu être impactées par cette violation**

et si certaines mesures peuvent être mises en place afin de limiter la fuite (supplémentaire) de données personnelles.

Basé sur les considérations susmentionnées, les Responsables de la Protection des Données décideront si l'autorité de surveillance compétente et la personne concernée doivent être informées de la violation. La notification de l'autorité de surveillance n'est pas requise si la violation des données personnelles est peu probable d'entraîner un risque pour les droits et les libertés de (ou des) individu(s).

Si une notification de la violation des données personnelles est nécessaire, le Groupe informera les autorités compétentes de surveillance et leur fournira toutes les informations nécessaires dans les 72 heures suivant la notification.

Si une violation des données personnelles est susceptible d'entraîner un « risque élevé » pour les droits et libertés des individus, le Groupe notifiera les parties concernées directement. « Risque élevé » signifie le seuil à partir duquel la notification directe des individus est plus importante que la notification de l'autorité de surveillance compétente. Si une notification à titre individuel représenterait un effort disproportionné pour le Groupe, celui-ci pourra utiliser des moyens de « communication publique » à condition que ce moyen soit aussi efficace qu'une information individuelle.

Afin de maintenir un niveau élevé de visibilité et de transparence, chaque membre du Groupe répertoriera tous les incidents concernant la Protection des Données (répertoriés ou non), y compris les faits relatifs à la violation, ses effets et les actions entreprises ou planifiées. Cette documentation devra permettre à l'autorité de Surveillance de vérifier la conformité avec les obligations de notification. Tous les faits de la violation des données doivent être répertoriés dans un formulaire « Registre des Violations de Données » (annexe 2).

## **4.5. Conservation et suppression de données**

Comme déjà évoqué dans le chapitre 4.1 de la présente procédure, les données personnelles ne pourront être traitées plus longtemps que nécessaire pour arriver à la finalité du traitement.

Chaque membre du Groupe a défini et mis en place un planning de conservation en conformité avec l'annexe 3. Les délais de conservation sont basés sur les obligations locales légales pour les différents types de catégories des données personnelles. Habituellement, la législation locale prend en considération les catégories suivantes de données personnelles :

1. Comptabilité et Finance
2. Contrats
3. Registres corporate
4. Correspondences et notes internes
5. E-mails et autres communications électroniques
6. Fichiers et autres papiers légaux
7. Fiches de paie

8. Documents relatifs à la retraite
9. Registres du personnel
10. Registres fiscaux

Dans tous les cas, toutes les données personnelles seront conservées pour une durée minimale permettant au Groupe de procéder à une demande d'indemnisation ou de se défendre selon la loi localement en vigueur.

#### **4.6. La formation du personnel**

Le Groupe s'engage à informer l'ensemble de ses salariés ayant accès aux Données Personnelles, de leur responsabilités relatives à cette procédure, et ceci comme partie intégrante de la formation d'intégration du personnel. En complément, chaque membre du Groupe fournit à ses employés des formations sur la Protection des Données ainsi qu'un accompagnement régulier concernant le respect des procédures.

Le responsable local de la Protection des Données est en charge de donner des formations appropriées à tous les employés. Le format de ces formations peut varier en fonction du type d'audience, le nombre de salariés à former et des objectifs de la formation et d'autres facteurs.

Les formations doivent avoir lieu à une fréquence régulière. Chaque membre du Groupe établit son propre planning précis ; toutefois, celui-ci doit être en phase avec les exigences/propositions du Responsable « UE » de la Protection des Données.

#### **4.7. Registre des opérations de traitement**

Chaque entreprise du Groupe a identifié les Données Personnelles qu'il traite et contrôle, et les liste dans un registre (annexe 4).

Ce registre garantit que les entreprises du Groupe sont en conformité avec les obligations requises sous le « RGPD » :

**Conserver des registres de toutes les opérations de traitement.**

**Conserver des registres de tous les accords conclus avec les processeurs de Données.**

**Conserver des registres de toutes les violations de données, y compris les notifications de violations faites aux autorités de surveillance compétentes et les personnes concernées.**

Tandis que le contenu du registre de données peut varier entre membres du Groupe, il contient au moins les informations suivantes relatives aux opérations de traitement :

**Nom et coordonnées du Groupe, et si applicable, le Contrôleur et son représentant.**

#### **La finalité des opérations de traitement.**

**La description des catégories de personnes concernées et des catégories de données personnelles.**

Les catégories de destinataires à qui les données personnelles ont été ou seront transférées, y compris les destinataires dans d'autres pays ou organismes internationaux ;

**Si applicable, transferts de Données Personnelles vers d'autres pays ou organismes internationaux, y compris l'identification de ces pays ou organismes internationaux ;**

**Si possible, les délais envisagés pour la suppression des différentes catégories de données. Si possible, une description générale des mesures de sécurité organisationnelles prises par le Groupe.**

**Chaque membre du groupe est seul responsable de la tenue de ce registre.**

#### **4.8. Transfert de données**

**Afin de compenser un éventuel manque de Protection des Données, le transfert de Données Personnelles à des tiers est sujet à des mesures de sécurité complémentaires.**

**Le Groupe a identifié trois types de transferts de données au sein de son organisation, auxquels sont associées différentes mesures de sécurité :**

**Les transferts de données « Intragroupe » : afin de faciliter la transmission des données, des « Binding Corporate Rules » (règles obligatoires du Groupe) seront implémentées. Il s'agit de règles approuvées par l'autorité de Surveillance et obligatoires pour tous les membres du Groupe. Ces règles obligatoires spécifieront entre autres les finalités du transfert et les catégories de données concernées ; ils respectent les exigences du RGPD ; ils confirment que les données basées en « UE » doivent être respectées par tous les membres du Groupe ; ils expliquent les procédures de litiges ; ils fournissent des mécanismes pour garantir la conformité (p.ex. audits).**

**Transferts de données à des tiers au sein de l'Espace Economique Européen « EEA » (ou tout autre pays garantissant les mêmes protections) agissant en tant que Processeur : Ces données sont transférées sous le RGPD.**

Avant tout transfert de données à un tiers, chaque membre du Groupe a fait une enquête en bonne et due forme en appliquant la procédure et vérifie si le tiers se conforme aux règles applicables.

Suite à ces évaluations, chaque membre du Groupe doit conclure un accord avec chacun des « Processeurs » des tiers (le « Third party Processor's agreement »). Ces accords contiendront au moins les informations suivantes :

Concernant les transferts de données à des entités en dehors de notre Groupe et en dehors de l'EEA, et à condition que le « RGPD » s'applique (autrement dit : un membre du Groupe ou la personne concernée résidant dans un des pays de l'UE) :

De plus, chaque membre du Groupe doit vérifier si le tiers à qui il enverra les Données Personnelles applique des mesures de sécurité complémentaires. Si de telles mesures n'ont pas été prises, le Groupe ne transfère aucune donnée à ce tiers.

#### **4.9. Evaluation de l'impact de la Protection des Données**

Afin de garantir que toutes les exigences de la Protection des Données sont automatiquement identifiées et adressées lorsque de nouveaux systèmes ou de nouvelles procédures sont mises en place, ou lorsque les systèmes ou procédures existants sont revus ou élargis, chaque membre du Groupe doit s'assurer qu'une évaluation de l'impact de la Protection des données (« EIPD ») est effectuée pour tous les nouveaux systèmes ou nouvelles procédures pour lesquels il a la responsabilité.

Cette « EIPD » est réalisée en coopération avec les Responsables « Global » et « EU » de la Protection des Données. Si nécessaire, les services IT coopéreront avec le Responsable de la Protection des données afin d'évaluer l'impact de toute nouvelle technologie utilisée sur la sécurité des Données Personnelles.

#### **4.10. Les Responsables de la Protection des Données**

Puisque le Groupe opère dans différentes juridictions, y compris l'espace "UE", différents responsables de la Protection des Données seront nommés :

**Le responsable Global de la Protection des Données (responsable pour le Groupe)**

Le responsable Global de la Protection des Données est nommé à cette position (et pourra en être retiré) par le CEO, après consultation du Conseil Général et le CFO.

Le responsable global de la Protection des Données du Groupe est Aleksander Pusanov. Ses coordonnées : [Aleksander.Puzanov@eurochem.ru](mailto:Aleksander.Puzanov@eurochem.ru).

Le responsable « UE » de la Protection des Données (responsable des activités du Groupe au sein de l'UE):

Le responsable « UE » de la Protection des Données est nommé à cette position (et pourra en être retiré) par le CEO, après consultation du Responsable global de la Protection des Données.

Le responsable « UE » de la Protection des Données est Pieter Callens. Ses coordonnées : [Pieter.Callens@eurochem.be](mailto:Pieter.Callens@eurochem.be)

Le Responsable Local de la Protection des Données pour EuroChem Agro France est : Sébastien Louis. E-mail : [privacy-FR@eurochemgroup.com](mailto:privacy-FR@eurochemgroup.com)

Chaque membre du Groupe peut nommer un Responsable Local pour la Protection des Données. Le Responsable Local pour la Protection des Données est nommé par le CEO/Directeur Général de l'entité. Si aucun Responsable Local pour la Protection des Données n'a été nommé, le CEO/Directeur Général officiera en tant que Responsable Local pour la Protection des Données.

#### 4.10.1. Les responsabilités des Responsables de la Protection des Données

##### Responsable Global de la Protection des Données

Le Responsable Global de la Protection des Données doit être nommé sur la base de ses compétences professionnelles, et en particulier, ses connaissances approfondies des lois sur la Protection des Données ainsi que son expérience et ses capacités à remplir les obligations suivantes du Responsable Global de la Protection des Données :

- Apporter du conseil au Management du Groupe sur tous les sujets de la procédure et les aviser de tout risque majeur de la Protection des Données, des sujets et problèmes, au fur et à mesure que ceux-ci se posent ;
- Etablir et garantir un système de Protection des Données de haute qualité, au sein du Groupe ;
- Gérer la communication, les stratégies de formation et d'accompagnement, et prendre toutes les initiatives afin d'assurer le support de l'ensemble des Business Units dans les régions où la Protection des Données est nécessaire.
- Superviser le Responsable "UE" de la Protection des Données et les Responsables Locaux de la Protection des Données (si nommés).



**En coopération avec le Responsable “UE” de la Protection des Données et les Responsables Locaux de la Protection des Données (si nommés) :**

**Garantir que toutes les procédures sont mises en place dans le Groupe afin de garder les Données Personnelles exactes et actualisées ; en prenant en considération le volume des données collectées, la rapidité avec laquelle le volume pourrait évoluer et d’autres facteurs pertinents ;**

**Effectuer des formations régulières concernant la Protection des Données, apporter des explications sur les sujets et problèmes s’y afférant ;**

**Informers et aviser le Groupe et les employés qui traitent les données de leurs responsabilités dans le cadre de cette procédure ;**

**Contrôler la conformité avec cette procédure et réaliser des audits ;**

**Apporter du conseil sur demande au sujet de l’évaluation de l’impact de la Protection des Données ; contrôler sa performance ;**

**Contrôler et analyser les éventuels changements dans les textes de loi applicables ;**

**Réviser les délais de conservation de l’ensemble des Données Personnelles traitées par le Groupe ; identifier toutes les données qui ne seront plus nécessaires pour la finalité enregistrée ;**

**Prendre les dispositions nécessaires au cas où une information non exacte ou obsolète aurait été passée à un tiers ; de les informer que l’information est non exacte et/ou obsolète et qu’elle ne doit pas être utilisée pour prendre des décisions sur les individus concernés ; transmettre toutes les modifications nécessaires au tiers.**

**Evaluer l’importance des dommages ou des pertes qui pourraient être causées aux individus (employés ou tiers) si une violation de la sécurité devait avoir lieu ; les conséquences d’une telle violation de sécurité sur le Groupe lui-même et les dommages qui pourraient s’ensuivre en terme de perte d’image, y compris une éventuelle perte de confiance de la part des clients.**

### **Responsable “UE” de la Protection des Données**

**Le Responsable “UE” de la Protection des Données est un résident de l’UE et doit être nommé sur la base de ses compétences professionnelles, et en particulier, ses connaissances approfondies des lois sur la Protection des Données ainsi que son expérience et ses capacités à remplir les obligations suivantes, en complément aux obligations listées ci-dessus :**

- Coopérer avec les autorités de surveillance au sein de l’UE, avec le Responsable Global de la Protection des Données et les Responsables Locaux des Données (si nommés) ;**
- Etre l’interlocuteur pour les autorités de surveillance sur les sujets relatifs au traitement des données et leurs éventuelles violations.**
- Contrôler et analyser les changements dans les textes de la loi Européenne et les remonter au Responsable Global de la Protection des Données.**

## **Responsable Local de la Protection des Données**

Chaque membre du Groupe doit nommer un Responsable Local de la Protection des Données afin d'assister le Responsable Global et le Responsable "UE" de la Protection des Données dans l'exécution de leurs obligations susmentionnées.

## **5. Gouvernance de la procédure**

### **5.1. Responsabilité**

Chaque membre du Groupe est seul responsable de la conformité avec la présente Procédure, ses obligations légales et le traitement approprié des Données Personnelles. La conformité avec les exigences de la Procédure est obligatoire pour tous les employés impliqués dans ces process. S'il y a la moindre raison de croire que les obligations légales sont en contradiction avec les obligations énoncées dans cette Procédure de Protection des Données, l'entité du Groupe doit en informer le Responsable Global de la Protection des Données. En cas de conflit entre la législation nationale et la procédure, le Groupe travaillera avec l'entité du Groupe concerné afin de trouver une solution pratique en phase avec la finalité de la Procédure de la Protection des Données.

Si opportun, un membre du Groupe peut imposer des règles qui, soit, complètent la procédure, soit, s'en différencient. Ces règles doivent être approuvées par le Responsable Global de la Protection des Données du Groupe.

### **5.2. Contrôle**

Chaque membre du Groupe garantit aux salariés que le fait de se conformer aux obligations de cette procédure, ou le fait d'alerter sur d'éventuelles violations déjà survenues ou à venir, ne portera aucun préjudice à l'employé concerné. Toutefois, le Groupe n'acceptera aucune action de ses employés qui pourrait être contraire à cette procédure.

Le Groupe part du principe et attend de ses salariés qu'ils remontent tous les cas de violation avérés ou potentiels via le « Donner d'alerte ». Les détails de ces guidelines sont accessibles publiquement et disponibles sur le portail du Groupe.

Le Groupe se réserve le droit de vérifier à intervalle régulier les connaissances de ses salariés sur la Protection des Données Personnelles, de réaliser des audits, d'appliquer cette Procédure et de faire une analyse de son efficacité.

### **5.3. Confidentialité**

Comme décrit dans l'article 4.4, les Données Personnelles sont sujettes à des obligations de confidentialité.

Toutefois, sous certaines conditions, il est permis de partager les Données Personnelles sans en avertir la personne concernée et/ou sans demander son consentement. Cela est le cas lorsque la diffusion des Données Personnelles est nécessaire dans les buts suivants :

**Prévention ou détection d'un crime.**

**L'appréhension ou persécution des délinquants.**

**L'évaluation ou la collection des taxes ou des droits de douane. Par l'ordre d'un tribunal ou tout article de loi.**

Si n'importe quel membre du Groupe traite les données personnelles dans l'un de ces buts, il peut contourner les obligations de confidentialité, mais uniquement en cas de préjudice présumé.

Si l'un des membres du Groupe reçoit une demande de la part d'un tribunal ou de toute autre autorité en lien avec la législation pour transmettre une information relative à une personne concernée, l'entité doit immédiatement notifier le Responsable Global de la Protection des Données qui fournira des conseils et une assistance clairs.

#### **5.4. Révision de la Procédure**

Cette procédure doit être révisée régulièrement par le Responsable Global de la Protection des Données ; au moins une fois par an afin de garantir que la Procédure est actualisée et toujours conforme avec toutes les règles applicables et avec la législation.

Tout amendement sera remonté immédiatement au Groupe qui implémentera les modifications.

La dernière version en date de la Procédure de Protection des Données est accessible sur le site web du Groupe : [www.eurochemgroup.com](http://www.eurochemgroup.com)

#### **5.5. Réclamations et questions**

Toute question ou interrogation concernant cette Procédure et ses annexes peut être envoyée au Responsable Global de la Protection des Données ou le Responsable Local de la Protection des Données en charge.

Les personnes concernées par une réclamation relative au traitement de leurs Données Personnelles doivent transmettre leur demande par écrit au Responsable Global de la Protection des Données. Chaque enquête sur les réclamations sera effectuée de façon appropriée au cas spécifique. Le Responsable Global de la Protection des Données informera la personne concernée sur les suites données à la réclamation dans un délai de temps raisonnable.

Si le problème ne peut être résolu par une consultation entre la personne concernée et le Responsable Global de la Protection des Données, la personne concernée peut, au choix, avoir recours à un médiateur, à un processus d'arbitrage exécutoire, à un contentieux ou à une réclamation déposée auprès de l'autorité de la Protection des Données en charge dans la juridiction concernée.

## Annex 1. Références

№	ID	Titre du document	Remarques
<b>Regulatory document</b>			
1		<b>Procédure de “Compliance” (Conformité) EuroChem Group AG</b>	
2		<b>Code de Conduite EuroChem Group AG</b>	
3		<b>Loi Fédérale sur la Protection des Données (« FADP »)</b>	

## Annexe 2. Registre de violations de Données Personnelles

<b>N°</b>	<b>Membre du Groupe</b>	<b>Catégorie de Donnée Personnelle</b>	<b>Description</b>	<b>Nombre de personnes concernées</b>	<b>Coordonnées de la personne concernée</b>	<b>Conséquences potentielles</b>	<b>Mesures prises ou à prendre</b>

### Annexe 3. Planning de conservation

N°	Membre du Groupe	Catégorie de Personnelle	de Donnée	Type de registre	Délai de conservation

## Annexe 4. Registre des données

N°	Membre du Groupe*	Catégorie et description des données personnelles*	Finalité du traitement*	Catégories de destinataires*	Transfert à des tiers	Délai avant suppression	Mesures de sécurité

Colonnes marquées avec un \* sont des champs obligatoires.