Politique de divulgation coordonnée des vulnérabilités

La ORES Assets S.C., dont le siège est sis à 6041 Gosselies, Avenue Jean Mermoz, 14, inscrite à la Banque-Carrefour des entreprises sous le numéro 0543.696.579 ; ici représentée par sa filiale ORES S.C., dont le siège est sis à 6041 Gosselies, Avenue Jean Mermoz, 14, inscrite à la Banque-Carrefour des entreprises sous le numéro 0897.436.971 ; société représentée par Stéphane Baldino, CISO (chief information security officer) et Vinciane Royez, DPO (data protection officer) ;

ci-après dénommée l' « organisation », a adopté la présente politique.

1. Le champ d'application de la politique

Soucieux d'améliorer la performance et la sécurité de nos réseaux et systèmes d'information, nous avons choisi d'adopter une politique de divulgation coordonnée des vulnérabilités. Celle-ci donne la possibilité aux participants de rechercher, avec de bonnes intentions, de potentielles vulnérabilités dans les systèmes, les équipements et les produits de notre organisation ou de nous transmettre toute information découverte sur une vulnérabilité.

L'accès à nos systèmes et équipements informatiques est toutefois autorisé exclusivement avec l'intention d'en améliorer la sécurité, de nous informer des vulnérabilités existantes et dans le strict respect des autres conditions définies dans le présent document.

Notre politique concerne les vulnérabilités en matière de sécurité susceptibles d'être exploitées par des tiers ou de perturber le bon fonctionnement de nos produits, services, réseaux ou systèmes d'information.

Le divulgateur de vulnérabilités dispose également d'une autorisation d'introduire ou de tenter d'introduire des données informatiques dans notre système informatique, dans le respect des finalités et des conditions de la présente politique.

À savoir sur :

- les pages, formulaires web et services proposés sur le site www.ORES.be et autre services exposés par ORES sur internet ;

Par contre, sont strictement prohibés pour des raisons de sécurité et d'intégrité de ces réseaux, toutes tentatives sur le réseau de télécommunications d'ORES en ce compris, les installations électriques et gaz et équipements attenants (postes, cabines...) en gaz et électricité

Les systèmes qui dépendent de tiers sont exclus du champ d'application de la présente politique, sauf si ceux-ci marquent explicitement et préalablement leur accord sur les présentes règles. Par exemple, une solution SaaS n'entre pas dans le scope de cette politique de divulgation coordonnée des vulnérabilités car l'infrastructure est totalement gérée par un fournisseur. Si le divulgateur est en mesure de s'introduire dans la couche de virtualisation de service web, il doit préalablement demander l'accord d'ORES car, selon le type d'hébergement, cela pourrait avoir un impact sur d'autres entités/organismes.

Les recherches du participant sur des systèmes d'information non explicitement inclus dans le cadre de la présente politique pourraient entraîner des poursuites judiciaires à son encontre.

2. Les obligations réciproques des parties

a) La proportionnalité

Le divulgateur de vulnérabilités s'engage dans toutes ses actions à respecter scrupuleusement le principe de proportionnalité, c'est-à-dire à ne pas perturber la disponibilité des services fournis par le système et à ne pas faire usage de la vulnérabilité au-delà de ce qui est strictement nécessaire à la démonstration de la faille de sécurité. Son attitude doit rester proportionnée : si la démonstration est établie à petit échelle, il n'est pas nécessaire de l'étendre plus loin.

L'objectif de notre politique n'est pas de permettre la prise de connaissance intentionnelle du contenu de données informatiques, de données de communication ou de données à caractère personnel et une telle prise de connaissance ne pourrait intervenir que de manière fortuite dans le cadre de la recherche de vulnérabilités.

b) Les actions interdites

Le divulgateur de vulnérabilités ne peut recourir aux actions suivantes :

- la copie, la modification ou la suppression de données du système informatique ;
- la modification des paramètres du système informatique ;
- l'installation d'un logiciel malveillant (malware) : virus, vers (worm), chevaux de Troie (trojan horse, ou autre ;
- les attaques par déni de service (Distributed Denial Of Service - DDOS) ;
- les attaques par ingénierie sociale (social engineering) ;
- les attaques par hameçonnage (phishing) ;
- les attaques par courriels indésirables (spamming) ;
- le vol de mots de passe ou l'attaque en force de mots de passe (brute force) ;
- l'installation d'appareil permettant l'interception, la prise de connaissance ou l'enregistrement de communication non accessible au public ou d'une communication électronique ;
- l'interception, l'enregistrement ou la prise de connaissance intentionnelle d'une communication non accessible au public ou d'une communication électronique ;
- l'utilisation, la détention, la révélation, l'usage ou la divulgation intentionnelle du contenu de communications non accessibles au public ou de données d'un système informatique, dont le divulgateur de vulnérabilités ne peut raisonnablement ignorer qu'elles ont été obtenues illégalement ;

Si le divulgateur de vulnérabilités souhaite l'aide d'un tiers pour exécuter ses recherches, le divulagteur de vulnérabilités doit s'assurer que celui-ci prend préalablement connaissance de la présente politique et accepte, en offrant son assistance, d'en respecter les conditions.

De manière générale, le divulgateur de vulnérabilités s'interdira toute action susceptible d'interférer de manière directe ou indirecte avec le bon fonctionnement de nos systèmes et réseaux.

c) La confidentialité

Le divulgateur de vulnérabilités s'engage à ne pas partager ni divulguer à des tiers, de quelque manière que ce soit, les informations recueillies dans le cadre de notre politique, sauf accord préalable et explicite de notre part.

De même, il n'est pas permis de révéler ou de divulguer des données informatiques, des données de communication ou des données à caractère personnel à des tiers.

Dans le cas où la vulnérabilité peut également affecter d'autres organisations en Belgique, le divulgateur de vulnérabilités ou l'organisation responsable peuvent néanmoins en informer le CCB (vulnerabilityreport@cert.be).

d) L'exécution de bonne foi

Notre organisation s'engage à exécuter de bonne foi la présente politique et de ne pas poursuivre en justice, au civil ou au pénal, le divulgateur de vulnérabilités qui en respecte les conditions.

Le divulgateur de vulnérabilités doit être dénué d'intention frauduleuse, de dessein de nuire, de volonté de faire usage ou de provoquer un dommage au système visité ou encore à ses données. Cela vaut également pour les systèmes tiers situés en Belgique ou à l'étranger.

En cas de doute sur certaines des conditions de notre politique, le divulgateur de vulnérabilités doit interroger préalablement notre point de contact et obtenir son accord écrit avant d'agir.

e) Le traitement de données à caractère personnel

L'objet de cette politique n'est pas d'effectuer intentionnellement des traitements de données à caractère personnel mais il est possible que le divulgateur de vulnérabilités doive, même de manière fortuite, traiter des données à caractère personnel dans le cadre de ses recherches de vulnérabilités.

Or, le traitement de données à caractère personnel a une portée large et inclut notamment la conservation, la modification, l'extraction, la consultation, l'utilisation ou la communication de toute information pouvant se rapporter à une personne physique identifiée ou identifiable. Le caractère « identifiable » de la personne ne dépend pas de la simple volonté d'identification de celui qui traite les données mais de la possibilité d'identifier, directement ou indirectement, la personne à l'aide de ces données (par exemple : une adresse de courriel, numéro d'identification, identifiant en ligne, adresse IP ou encore des données de localisation).

Ainsi, il est possible que le divulgateur de vulnérabilités traite de manière limitée des données à caractère personnel. En cas de traitement de telles données, le divulgateur de vulnérabilités s'engage à respecter les obligations légales en matière de protection des données à caractère personnel[1] et les conditions de la présente politique, notamment :

- Le divulgateur de vulnérabilités s'engage à ne traiter des données à caractère personnel que selon les instructions de notre organisation, décrites dans la présente politique, et exclusivement afin de rechercher des vulnérabilités dans les systèmes, équipements ou produits de notre organisation. Tout traitement de données à caractère personnel pour une autre finalité est exclu.

- Le divulgateur de vulnérabilités s'engage à limiter le traitement de données à caractère personnel à ce qui est nécessaire au regard de la finalité de recherche de vulnérabilités.

- Le divulgateur de vulnérabilités veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

- Le divulgateur de vulnérabilités met en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (p.ex. cryptage). Le divulgateur de vulnérabilités déclare qu'il comprend les risques liés à la mise en œuvre de la présente politique et qu'il a l'expertise et l'expérience nécessaires afin de tester les systèmes, équipements et produits de notre organisation en toute sécurité et en respectant les lois et réglementations applicables.

- Le divulgateur de vulnérabilités s'engage à nous assister, dans la mesure du possible et compte tenu de la nature du traitement et des informations à la disposition du participant, dans la mise en œuvre de nos obligations relatives à l'exercice des droits des personnes concernées, la sécurité du traitement et toute analyse d'impact éventuelle.

- Le divulgateur de vulnérabilités s'engage à nous informer, dans les meilleurs délais après en avoir pris connaissance, de toute violation[2] éventuelle de données à caractère personnel à l'adresse vulnerabilites@ores.be.

- Le divulgateur de vulnérabilités ne peut conserver plus longtemps que nécessaire les éventuelles données à caractère personnel traitées. Durant cette période, le divulgateur de vulnérabilités doit veiller à ce que ces données soient conservées en garantissant un niveau de sécurité adapté aux risques encourus (de préférence de manière

1 Règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD Règlement général sur la protection des données).

2 Une « violation de données à caractère personnel » consiste en une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé aux données à caractère personnel.

encryptée). A l'issue de sa participation à la politique, ces données doivent être supprimés immédiatement.

- Le divulgateur de vulnérabilités s'engage à tenir un registre des catégories d'activités de traitement effectuées pour le compte de notre organisation comprenant notamment une description des mesures de sécurité qu'il a mises en œuvre, conformément à l'article 30, § 2 du RGPD.

3. Comment signaler les vulnérabilités de sécurité ?

a) Le point de contact

Vous devez adresser exclusivement les informations découvertes à l'adresse de courriel suivante : vulnerabilites@ores.be.

b) Les informations à transmettre

Dès que possible après la découverte, adressez-nous les informations sur vos découvertes en utilisant le formulaire repris en annexe I.

4. La procédure

a) Découverte

Lorsqu'un participant découvre des informations relatives à une vulnérabilité potentielle, celui-ci devrait, dans la mesure du possible, réaliser au préalable des vérifications permettant de confirmer l'existence de la vulnérabilité et d'identifier les éventuels risques encourus.

b) Notification

Le divulgateur de vulnérabilités s'engage à notifier, dans les plus brefs délais, les informations techniques sur les éventuelles vulnérabilités au point de contact [ou au coordinateur (optionnel)], repris au point 3 a) de la présente politique. Le divulgateur de vulnérabilités doit respecter les moyens de communication sécurisés désignés.

Lorsqu'elle reçoit une notification, notre organisation s'engage à envoyer au participant, dans les plus brefs délais, un accusé de réception, [avec si possible sa référence interne, un rappel des principales obligations de la Politique] et les étapes suivantes de la procédure.

c) Communication

Les parties s'engagent à mettre tout en œuvre pour assurer une communication continue et efficace. Les renseignements fournis par le divulgateur de vulnérabilités peuvent, en effet, s'avérer très utiles pour identifier la vulnérabilité, y apporter une solution.

En l'absence de réaction de l'une des parties à la CVDP au-delà d'un délai raisonnable, les parties peuvent faire appel au Centre pour la Cybersécurité Belgique (CBB) (vulnerabilityreport@cert.be), comme coordinateur (par défaut).

d) Investigation

La phase d'investigation permettra à notre organisation de reproduire l'environnement et le comportement signalé afin de vérifier les informations communiquées.

Notre organisation s'engage à tenir informé de manière régulière le divulgateur de vulnérabilités des résultats des investigations et des suites données à sa notification.

Durant ce processus, les parties veilleront à faire le lien avec les notifications similaires ou connexes, d'évaluer le risque et la gravité de la vulnérabilité, et de détermination les éventuels autres produits ou systèmes affectés.

e) Développement d'une solution

L'objectif de la politique de divulgation est de permettre le développement d'une solution afin de faire disparaître la vulnérabilité du système informatique, avant que des dommages ne soient causés.

En tenant compte de l'état des connaissances, des coûts de mise en œuvre, de la gravité des risques encourus par les utilisateurs et des contraintes techniques, notre organisation tentera de mettre au point une solution au plus tard dans les 90 jours calendrier.

Dans cette phase, notre organisation et ses partenaires s'engagent à mener, d'une part, des tests positifs pour vérifier que la solution fonctionne correctement et, d'autre part, des tests négatifs pour s'assurer que la solution ne perturbe pas le bon fonctionnement des autres fonctionnalités existantes.

f) Éventuelle divulgation publique

Notre organisation décidera, en coordination avec le divulgateur de vulnérabilités, des modalités pour rendre éventuellement public l'existence de la vulnérabilité. Cette divulgation publique devra se faire au plus tôt en même temps que le déploiement d'une solution et la diffusion d'un avis de sécurité destiné aux utilisateurs.

Dans l'hypothèse d'une vulnérabilité qui concernerait également d'autres organisations, l'organisation responsable se doit d'en informer, en tout état de cause, le Centre pour la Cybersécurité Belgique (vulnerabilityreport@cert.be), même si elle ne souhaite pas que la vulnérabilité soit divulguée publiquement.

Notre organisation s'engage également à recueillir les commentaires des utilisateurs sur le déploiement de la solution et de prendre les mesures correctives nécessaires pour régler les éventuels problèmes posés par la solution, notamment de compatibilité avec d'autres produits ou services.

5. Droit applicable

Le droit belge est applicable aux litiges liées à l'application de la présente politique.

Le CCB (vulnerabilityreport@cert.be) peut servir d'intermédiaire pour tenter de concilier notre organisation et le divulgateur de vulnérabilités pour les problèmes liés à l'application de la présente politique].

6. Durée

Les règles de la politique sont applicables à partir du 04/08/2025 jusqu'à leur éventuelle modification ou suppression par notre organisation. Ces modifications ou suppressions seront publiées sur le site internet de notre organisation et s'appliqueront automatiquement après un délai de 30 jours après leur publication.

Annexe I : Formulaire de notification de vulnérabilités

Fournissez suffisamment d'informations pour nous permettre de reproduire le problème et de le résoudre le plus rapidement possible.

Nous vous demandons de nous fournir au moins les informations pertinentes suivantes :

Nom : **Prénom :**	
(Adresse/Pays) :	
Adresse de courriel : **Numéro de téléphone :**	
Description de la vulnérabilité :	
Type de vulnérabilité :	
Détails de la configuration :	
Système d'exploitation :	

Opérations effectuées (logs) :	
Outils utilisés :	
Dates et heures des tests :	
Adresse IP ou de l'URL du système affecté :	
En cas de traitement de données personnelles :	• Types de données personnelles consultées/traitées : • Catégories de personnes concernées (client, employé, fournisseur) : • Transfert de données vers/accès depuis un pays situé en dehors de l'Union européenne ou de l'Espace économique européen ? Si oui: - indiquez le(s) pays concerné(s) : - retournez l'Annexe II complétée et signée.
Toute autre information pertinente :	
Annexes (captures d'écran) :	

Que faisons-nous avec vos données à caractère personnel ?

Nous vous invitons à lire notre politique de protection des données à caractère personnel disponible ici : https://www.ores.be/notice-vie-privee.

Annexe II – Transfert de données à caractère personnel par le divulgateur de vulnérabilités dans un pays situé en dehors de l'Union européenne ou Espace économique européen.

Clauses contractuelles types de protection des données (n° 2010/87/EU)

Aux fins de l'article 26, paragraphe 2 de la directive 95/46/CE pour le transfert des données à caractère personnel vers des sous-traitants établis dans des pays tiers qui n'assurent pas un niveau adéquat de protection des données

Nom de l'organisation exportant les données (l'organisation responsable)

(ci-après dénommée l'« **exportateur** de données »)

d'une part, et

Nom de l'organisation important les données (le divulgateur de vulnérabilités)

(ci-après dénommée l'« **importateur** de données »)

d'autre part, ci-après dénommés individuellement une « partie » et collectivement les « parties »

SONT CONVENUS des clauses contractuelles suivantes (ci-après dénommées « les clauses ») afin d'offrir des garanties adéquates concernant la protection de la vie privée et des libertés et droits fondamentaux des personnes lors du transfert, par l'exportateur de données vers l'importateur de données, des données à caractère personnel visées à l'appendice 1.

Clause première
Définitions

Au sens des clauses :

a) « données à caractère personnel », « catégories particulières de données », « traiter/traitement », « responsable du traitement », « sous-traitant », « personne concernée » et « autorité de contrôle » ont la même signification que dans la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [1] ;

b) l'« exportateur de données » est le responsable du traitement qui transfère les données à caractère personnel ;

c) l'« importateur de données » est le sous-traitant qui accepte de recevoir de l'exportateur de données des données à caractère personnel destinées à être traitées pour le compte de ce dernier après le transfert conformément à ses instructions et aux termes des présentes clauses et qui n'est pas soumis au mécanisme d'un pays tiers assurant une protection adéquate au sens de l'article 25, paragraphe 1, de la directive 95/46/CE ;

d) le « sous-traitant ultérieur » est le sous-traitant engagé par l'importateur de données ou par tout autre sous-traitant ultérieur de celui-ci, qui accepte de recevoir de l'importateur de données ou de tout autre sous-traitant ultérieur de celui-ci des données à caractère personnel exclusivement destinées à des activités de traitement à effectuer pour le compte de l'exportateur de données après le transfert conformément aux instructions de ce dernier, aux conditions énoncées dans les présentes clauses et selon les termes du contrat de sous-traitance écrit ;

e) le « droit applicable à la protection des données » est la législation protégeant les libertés et les droits fondamentaux des personnes, notamment le droit à la vie privée à l'égard du traitement des données à caractère personnel, et s'appliquant à un responsable du traitement dans l'État membre où l'exportateur de données est établi ;

f) les « mesures techniques et d'organisation liées à la sécurité » sont les mesures destinées à protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement.

Clause 2
Détails du transfert

Les détails du transfert et, notamment, le cas échéant, les catégories particulières de données à caractère personnel, sont spécifiés dans l'appendice 1 qui fait partie intégrante des présentes clauses.

Clause 3
Clause du tiers bénéficiaire

1. La personne concernée peut faire appliquer contre l'exportateur de données la présente clause, ainsi que la clause 4, points b) à i), la clause 5, points a) à e) et points g) à j), la clause 6, paragraphes 1 et 2, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12 en tant que tiers bénéficiaire.

2. La personne concernée peut faire appliquer contre l'importateur de données la présente clause, ainsi que la clause 5, points a) à e) et g), la clause 6, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12 dans les cas où l'exportateur de données a matériellement disparu ou a cessé d'exister en droit, à moins que l'ensemble de ses obligations juridiques n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, à laquelle reviennent par conséquent les droits et les obligations de l'exportateur de données, et contre laquelle la personne concernée peut donc faire appliquer lesdites clauses.

3. La personne concernée peut faire appliquer contre le sous-traitant ultérieur la présente clause, ainsi que la clause 5, points a) à e) et g), la clause 6, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12, mais uniquement dans les cas où l'exportateur de données et l'importateur de données ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables, à moins que l'ensemble des obligations juridiques de l'exportateur de données n'ait été transféré, par contrat ou par effet de la loi, au successeur légal, auquel reviennent par conséquent les droits et les obligations de l'exportateur de données, et contre lequel la personne concernée peut donc faire appliquer lesdites clauses. Cette responsabilité civile du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.

4. Les parties ne s'opposent pas à ce que la personne concernée soit représentée par une association ou un autre organisme si elle en exprime le souhait et si le droit national l'autorise.

Clause 4
Obligations de l'exportateur de données

L'exportateur de données accepte et garantit ce qui suit :

a) le traitement, y compris le transfert proprement dit des données à caractère personnel, a été et continuera d'être effectué conformément aux dispositions pertinentes du droit applicable à la protection des données (et, le cas échéant, a été notifié aux autorités compétentes de l'État membre dans lequel l'exportateur de données est établi) et n'enfreint pas les dispositions pertinentes dudit État ;

b) il a chargé, et chargera pendant toute la durée des services de traitement de données à caractère personnel, l'importateur de données de traiter les données à caractère personnel transférées pour le compte exclusif de l'exportateur de données et conformément au droit applicable à la protection des données et aux présentes clauses ;

c) l'importateur de données offrira suffisamment de garanties en ce qui concerne les mesures techniques et d'organisation liées à la sécurité spécifiées dans l'appendice 2 du présent contrat ;

d) après l'évaluation des exigences du droit applicable à la protection des données, les mesures de sécurité sont adéquates pour protéger les données à caractère personnel contre une destruction fortuite ou illicite, une perte fortuite, une altération, une divulgation ou un accès non autorisé, notamment lorsque le traitement suppose la transmission de données par réseau, et contre toute autre forme illicite de traitement et elles assurent un niveau de sécurité adapté aux risques liés au traitement et à la nature des données à protéger, eu égard au niveau technologique et au coût de mise en œuvre ;

e) il veillera au respect des mesures de sécurité ;

f) si le transfert porte sur des catégories particulières de données, la personne concernée a été informée ou sera infor-

mée avant le transfert ou dès que possible après le transfert que ses données pourraient être transmises à un pays tiers n'offrant pas un niveau de protection adéquat au sens de la directive 95/46/CE ;

g) il transmettra toute notification reçue de l'importateur de données ou de tout sous-traitant ultérieur conformément à la clause 5, point b), et à la clause 8, paragraphe 3), à l'autorité de contrôle de la protection des données s'il décide de poursuivre le transfert ou de lever sa suspension ;

h) il mettra à la disposition des personnes concernées, si elles le demandent, une copie des présentes clauses, à l'exception de l'appendice 2, et une description sommaire des mesures de sécurité, ainsi qu'une copie de tout contrat de sous-traitance ultérieure ayant été conclu conformément aux présentes clauses, à moins que les clauses ou le contrat ne contienne(nt) des informations commerciales, auquel cas il pourra retirer ces informations ;

i) en cas de sous-traitance ultérieure, l'activité de traitement est effectuée conformément à la clause 11 par un sous-traitant ultérieur offrant au moins le même niveau de protection des données à caractère personnel et des droits de la personne concernée que l'importateur de données conformément aux présentes clauses ; et

j) il veillera au respect de la clause 4, points a) à i).

Clause 5
Obligations de l'importateur de données

L'importateur de données accepte et garantit ce qui suit :

a) il traitera les données à caractère personnel pour le compte exclusif de l'exportateur de données et conformément aux instructions de ce dernier et aux présentes clauses ; s'il est dans l'incapacité de s'y conformer pour quelque raison que ce soit, il accepte d'informer dans les meilleurs délais l'exportateur de données de son incapacité, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat ;

b) il n'a aucune raison de croire que la législation le concernant l'empêche de remplir les instructions données par l'exportateur de données et les obligations qui lui incombent conformément au contrat, et si ladite législation fait l'objet d'une modification susceptible d'avoir des conséquences négatives importantes pour les garanties et les obligations offertes par les clauses, il communiquera la modification à l'exportateur de données sans retard après en avoir eu connaissance, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat ;

c) il a mis en œuvre les mesures techniques et d'organisation liées à la sécurité spécifiées dans l'appendice 2 avant de traiter les données à caractère personnel transférées ;

d) il communiquera sans retard à l'exportateur de données :

   i) toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre, sauf disposition contraire, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière,

   ii) tout accès fortuit ou non autorisé, et

   iii) toute demande reçue directement des personnes concernées sans répondre à cette demande, à moins qu'il n'ait été autorisé à le faire ;

e) il traitera rapidement et comme il se doit toutes les demandes de renseignements émanant de l'exportateur de données relatives à son traitement des données à caractère personnel qui font l'objet du transfert et se rangera à l'avis de l'autorité de contrôle en ce qui concerne le traitement des données transférées ;

f) à la demande de l'exportateur de données, il soumettra ses moyens de traitement de données à une vérification des activités de traitement couvertes par les présentes clauses qui sera effectuée par l'exportateur de données ou un organe de contrôle composé de membres indépendants possédant les qualifications professionnelles requises, soumis à une obligation de secret et choisis par l'exportateur de données, le cas échéant, avec l'accord de l'autorité de contrôle ;

g) il mettra à la disposition de la personne concernée, si elle le demande, une copie des présentes clauses, ou tout contrat de sous-traitance ultérieure existant, à moins que les clauses ou le contrat ne contienne(nt) des informations commerciales, auquel cas il pourra retirer ces informations, à l'exception de l'appendice 2, qui sera remplacé par une description sommaire des mesures de sécurité, lorsque la personne concernée n'est pas en mesure d'obtenir une

copie de l'exportateur de données ;

h) en cas de sous-traitance ultérieure, il veillera au préalable à informer l'exportateur de données et à obtenir l'accord écrit de ce dernier ;

i) les services de traitement fournis par le sous-traitant ultérieur seront conformes à la clause 11 ;

j) il enverra dans les meilleurs délais une copie de tout accord de sous-traitance ultérieure conclu par lui en vertu des présentes clauses à l'exportateur de données.

Clause 6
Responsabilité

1. Les parties conviennent que toute personne concernée ayant subi un dommage du fait d'un manquement aux obligations visées à la clause 3 ou à la clause 11 par une des parties ou par un sous-traitant ultérieur a le droit d'obtenir de l'exportateur de données réparation du préjudice subi.

2. Si une personne concernée est empêchée d'intenter l'action en réparation visée au paragraphe 1 contre l'exportateur de données pour manquement par l'importateur de données ou par son sous-traitant ultérieur à l'une ou l'autre de ses obligations visées à la clause 3 ou à la clause 11, parce que l'exportateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'importateur de données accepte que la personne concernée puisse déposer une plainte à son encontre comme s'il était l'exportateur de données, à moins que l'ensemble des obligations juridiques de l'exportateur de données n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, contre laquelle la personne concernée peut alors faire valoir ses droits.

   L'importateur de données ne peut invoquer un manquement par un sous-traitant ultérieur à ses obligations pour échapper à ses propres responsabilités.

3. Si une personne concernée est empêchée d'intenter l'action visée aux paragraphes 1 et 2 contre l'exportateur de données ou l'importateur de données pour manquement par le sous-traitant ultérieur à l'une ou l'autre de ses obligations visées à la clause 3 ou à la clause 11, parce que l'exportateur de données et l'importateur de données ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables, le sous-traitant ultérieur accepte que la personne concernée puisse déposer une plainte à son encontre en ce qui concerne ses propres activités de traitement conformément aux présentes clauses comme s'il était l'exportateur de données ou l'importateur de données, à moins que l'ensemble des obligations juridiques de l'exportateur de données ou de l'importateur de données n'ait été transféré, par contrat ou par effet de la loi, au successeur légal, contre lequel la personne concernée peut alors faire valoir ses droits. La responsabilité du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.

Clause 7
Médiation et juridiction

1. L'importateur de données convient que si, en vertu des clauses, la personne concernée invoque à son encontre le droit du tiers bénéficiaire et/ou demande réparation du préjudice subi, il acceptera la décision de la personne concernée :

   a) de soumettre le litige à la médiation d'une personne indépendante ou, le cas échéant, de l'autorité de contrôle ;

   b) de porter le litige devant les tribunaux de l'État membre où l'exportateur de données est établi.

2. Les parties conviennent que le choix effectué par la personne concernée ne remettra pas en cause le droit procédural ou matériel de cette dernière d'obtenir réparation conformément à d'autres dispositions du droit national ou international.

Clause 8
Coopération avec les autorités de contrôle

1. L'exportateur de données convient de déposer une copie du présent contrat auprès de l'autorité de contrôle si celle-

ci l'exige ou si ce dépôt est prévu par le droit applicable à la protection des données.

2. Les parties conviennent que l'autorité de contrôle a le droit d'effectuer des vérifications chez l'importateur de données et chez tout sous-traitant ultérieur dans la même mesure et dans les mêmes conditions qu'en cas de vérifications opérées chez l'exportateur de données conformément au droit applicable à la protection des données.

3. L'importateur de données informe l'exportateur de données, dans les meilleurs délais, de l'existence d'une législation le concernant ou concernant tout sous-traitant ultérieur faisant obstacle à ce que des vérifications soient effectuées chez lui ou chez tout sous-traitant ultérieur conformément au paragraphe 2. Dans ce cas, l'exportateur de données a le droit de prendre les mesures prévues par la clause 5, point b).

Clause 9
Droit applicable

Les clauses sont régies par le droit de l'État membre où l'exportateur de données est établi, à savoir :

.....

Clause 10
Modification du contrat

Les parties s'engagent à ne pas modifier les présentes clauses. Les parties restent libres d'inclure d'autres clauses à caractère commercial qu'elles jugent nécessaires, à condition qu'elles ne contredisent pas les présentes clauses.

Clause 11
Sous-traitance ultérieure

1. L'importateur de données ne sous-traite aucune de ses activités de traitement effectuées pour le compte de l'exportateur de données conformément aux présentes clauses sans l'accord écrit préalable de l'exportateur de données. L'importateur de données ne sous-traite les obligations qui lui incombent conformément aux présentes clauses, avec l'accord de l'exportateur de données, qu'au moyen d'un accord écrit conclu avec le sous-traitant ultérieur, imposant à ce dernier les mêmes obligations que celles qui incombent à l'importateur de données conformément aux présentes clauses [(3)]. En cas de manquement, par le sous-traitant ultérieur, aux obligations en matière de protection des données qui lui incombent conformément audit accord écrit, l'importateur de données reste pleinement responsable du respect de ces obligations envers l'exportateur de données.

2. Le contrat écrit préalable entre l'importateur de données et le sous-traitant ultérieur prévoit également une clause du tiers bénéficiaire telle qu'énoncée à la clause 3 pour les cas où la personne concernée est empêchée d'intenter l'action en réparation visée à la clause 6, paragraphe 1, contre l'exportateur de données ou l'importateur de données parce que ceux-ci ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables, et que l'ensemble des obligations juridiques de l'exportateur de données ou de l'importateur de données n'a pas été transféré, par contrat ou par effet de la loi, à une autre entité leur ayant succédé. Cette responsabilité civile du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.

3. Les dispositions relatives aux aspects de la sous-traitance ultérieure liés à la protection des données du contrat visé au paragraphe 1 sont régies par le droit de l'État membre où l'exportateur de données est établi, à savoir :

   .....

4. L'exportateur de données tient une liste des accords de sous-traitance ultérieure conclus en vertu des présentes clauses et notifiés par l'importateur de données conformément à la clause 5, point j), qui sera mise à jour au moins une fois par an. Cette liste est mise à la disposition de l'autorité de contrôle de la protection des données de l'exportateur de données.

Clause 12
Obligation après la résiliation des services de traitement des données à caractère personnel

1. Les parties conviennent qu'au terme des services de traitement des données, l'importateur de données et le sous-traitant ultérieur restitueront à l'exportateur de données, et à la convenance de celui-ci, l'ensemble des données à caractère personnel transférées ainsi que les copies, ou détruiront l'ensemble de ces données et en apporteront la preuve à l'exportateur de données, à moins que la législation imposée à l'importateur de données ne l'empêche de restituer ou de détruire la totalité ou une partie des données à caractère personnel transférées. Dans ce cas, l'importateur de données garantit qu'il assurera la confidentialité des données à caractère personnel transférées et qu'il ne traitera plus activement ces données.

2. L'importateur de données et le sous-traitant ultérieur garantissent que si l'exportateur de données et/ou l'autorité de contrôle le demandent, ils soumettront leurs moyens de traitement de données à une vérification des mesures visées au paragraphe 1.