FR

COMMISSION EUROPÉENNE

Bruxelles, le 5.2.2010
C(2010)593 final

DÉCISION DE LA COMMISSION

du 5.2.2010

relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil

DÉCISION DE LA COMMISSION

du 5.2.2010

relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu 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], et notamment son article 26, paragraphe 4,

après consultation du contrôleur européen de la protection des données[2],

considérant ce qui suit:

(1) Conformément à la directive 95/46/CE, les États membres sont tenus de veiller à ce qu'un transfert de données à caractère personnel vers un pays tiers n'ait lieu que si le pays en question assure un niveau de protection adéquat des données et si les lois des États membres, qui sont conformes aux autres dispositions de la directive, sont respectées avant le transfert.

(2) Toutefois, l'article 26, paragraphe 2 de la directive 95/46/CE prévoit que les États membres peuvent autoriser, sous réserve de certaines garanties, un transfert, ou un ensemble de transferts, de données à caractère personnel vers des pays tiers n'assurant pas un niveau de protection adéquat. Ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

(3) Conformément à la directive 95/46/CE, le niveau de protection des données doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel instauré au titre de ladite directive a publié des lignes directrices afin de faciliter l'évaluation.

(4) Les clauses contractuelles types ne doivent concerner que la protection des données. L'exportateur de données et l'importateur de données sont donc libres d'inclure d'autres clauses à caractère commercial qu'ils jugent pertinentes pour le contrat à condition qu'elles ne contredisent pas les clauses contractuelles types.

(5) La présente décision ne doit pas affecter les autorisations nationales que les États membres peuvent délivrer conformément aux dispositions nationales mettant en œuvre l'article 26, paragraphe 2, de la directive 95/46/CE. Elle doit avoir pour seul effet d'obliger les États membres à ne pas refuser de reconnaître que les clauses contractuelles types qu'elle contient offrent des garanties adéquates et elle ne doit donc avoir aucun effet sur d'autres clauses contractuelles.

(6) La décision 2002/16/CE de la Commission du 27 décembre 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE[3] a été adoptée afin de faciliter le transfert de données à caractère personnel d'un responsable du traitement de données établi dans l'Union européenne vers un sous-traitant établi dans un pays tiers n'assurant pas un niveau de protection adéquat.

---

1 JO L 281 du 23.11.1995, p. 31.
2 JO […] du […], p. […].
3 JO L 6 du 10.1.2002, p. 52.

(7) Une expérience considérable a été acquise depuis l'adoption de la décision 2002/16/CE. En outre, le rapport sur la mise en œuvre des décisions relatives aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers[4] a mis en évidence un intérêt grandissant dans la promotion de l'utilisation des clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers n'assurant pas un niveau de protection adéquat. De plus, des parties prenantes[5] ont présenté des propositions visant à mettre à jour les clauses contractuelles types énoncées dans la décision 2002/16/CE pour tenir compte du développement rapide de la portée des activités de traitement de données dans le monde et pour aborder certains aspects non couverts par cette décision.

(8) Le champ d'application de la présente décision doit se limiter à établir que les clauses qu'elle énonce peuvent être utilisées par un responsable du traitement de données établi dans l'Union européenne pour offrir des garanties adéquates, au sens de l'article 26, paragraphe 2, de la directive 95/46/CE, pour le transfert de données à caractère personnel vers un sous-traitant établi dans un pays tiers.

(9) La présente décision ne doit pas s'appliquer au transfert de données à caractère personnel effectué par des responsables du traitement établis dans l'Union européenne vers des responsables du traitement établis en dehors de l'Union européenne qui relèvent du champ d'application de la décision 2001/497/CE de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE[6].

(10) La présente décision doit mettre en œuvre l'obligation prévue à l'article 17, paragraphe 3, de la directive 95/46/CE et ne doit pas affecter le contenu d'un contrat ou acte juridique établi conformément à cette disposition. Toutefois, certaines clauses contractuelles types, relatives en particulier aux obligations de l'exportateur de données, doivent être incluses dans le but d'accroître la clarté en ce qui concerne les dispositions qui peuvent être introduites dans un contrat entre un responsable du traitement et un sous-traitant.

(11) Les autorités de contrôle des États membres jouent un rôle clé dans ce mécanisme contractuel en garantissant la protection adéquate des données à caractère personnel après le transfert. Dans les cas exceptionnels où les exportateurs de données refusent ou ne sont pas en mesure d'instruire convenablement l'importateur de données et où il existe un risque imminent de dommage grave pour les personnes concernées, les clauses contractuelles types doivent permettre aux autorités de contrôle de soumettre les importateurs de données et les sous-traitants ultérieurs à des vérifications et, lorsque cela se révèle approprié, de prendre des décisions auxquelles ces derniers devront se plier. Les autorités de contrôle doivent avoir la faculté d'interdire ou de suspendre un transfert de données ou un ensemble de transferts basé sur les clauses contractuelles types dans les cas exceptionnels où il est établi qu'un transfert basé sur des termes contractuels risque d'avoir des conséquences négatives importantes pour les garanties et les obligations offrant un niveau de protection adéquat à la personne concernée.

(12) Les clauses contractuelles types doivent prévoir les mesures techniques et d'organisation à mettre en œuvre par les sous-traitants établis dans un pays tiers n'offrant pas un niveau de protection adéquat, afin d'assurer un niveau de sécurité adapté aux risques liés au traitement et à la nature des données à protéger. Les parties doivent prévoir dans le contrat les mesures techniques et d'organisation qui, eu égard au droit applicable à la protection des données, au niveau technologique et au coût de mise en œuvre, sont nécessaires 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 ou toute autre forme illicite de traitement.

(13) Afin de faciliter les flux de données provenant de l'Union européenne, il est souhaitable que les sous-traitants offrant des services de traitement des données à plusieurs responsables du traitement des données de l'Union européenne soient autorisés à appliquer les mêmes mesures techniques et d'organisation liées à la sécurité, quel que soit l'État membre d'où provient le transfert de données, notamment dans les cas où l'importateur de données reçoit, pour un traitement ultérieur, des données originaires de différents établissements de l'exportateur de

---

4 SEC(2006) 95 du 20.1.2006.

5 La Chambre de commerce internationale (CCI), l'Association des entreprises japonaises en Europe (JBCE), le Comité UE de la Chambre de commerce américaine en Belgique (Amcham) et la Fédération des associations européennes de vente directe (FEDMA).

6 JO L 181 du 4.7.2001, p. 19.

données dans l'Union européenne, auquel cas le droit de l'État membre d'établissement désigné doit s'appliquer.

(14) Il convient de définir les informations minimales que les parties doivent prévoir dans le contrat qui a trait au transfert. Les États membres doivent conserver la faculté de spécifier les informations que les parties doivent fournir. L'application de la présente décision doit être évaluée à la lumière de l'expérience acquise.

(15) L'importateur de données doit traiter les données à caractère personnel transférées pour le compte exclusif de l'exportateur de données et selon ses instructions et les obligations incluses dans les clauses. En particulier, l'importateur de données ne doit pas divulguer les données à caractère personnel à un tiers sans l'accord écrit préalable de l'exportateur de données. Ce dernier doit charger l'importateur de données, pendant la durée des services de traitement des données, de traiter les données conformément à ses instructions, au droit applicable à la protection des données et aux obligations contenues dans les clauses.

(16) Le rapport sur la mise en œuvre des décisions relatives aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers a recommandé l'élaboration de clauses contractuelles types adaptées sur les transferts ultérieurs d'un sous-traitant établi dans un pays tiers vers un autre sous-traitant (sous-traitance ultérieure) afin de tenir compte de l'évolution des pratiques des entreprises, qui tendent vers une mondialisation croissante de l'activité de traitement.

(17) La présente décision doit contenir des clauses contractuelles types spécifiques sur la sous-traitance, par un sous-traitant établi dans un pays tiers (l'importateur de données), de ses services de traitement à d'autres sous-traitants (ultérieurs) établis dans des pays tiers. Elle doit également définir les conditions à remplir par la sous-traitance ultérieure pour que la protection des données à caractère personnel transférées soit garantie malgré le transfert à un sous-traitant ultérieur.

(18) En outre, la sous-traitance ultérieure ne doit porter que sur les activités convenues dans le contrat conclu entre l'exportateur de données et l'importateur de données et intégrant les clauses contractuelles types prévues dans la présente décision, et ne doit pas avoir d'autres finalités ou concerner d'autres activités de traitement, de manière à ce que soit respecté le principe de la limitation des transferts à une finalité spécifique, énoncé dans la directive 95/46/CE. De plus, en cas de manquement par le sous-traitant ultérieur aux obligations en matière de traitement de données qui lui incombent conformément au contrat, l'importateur de données doit rester responsable envers l'exportateur de données. Le transfert de données à caractère personnel vers des sous-traitants établis en dehors de l'Union européenne ne doit rien enlever au fait que les activités de traitement doivent être régies par le droit applicable à la protection des données.

(19) Les clauses contractuelles types doivent être exécutoires non seulement par les organisations parties au contrat, mais également par les personnes concernées, en particulier lorsque ces dernières subissent un dommage en raison d'une rupture du contrat.

(20) La personne concernée doit avoir le droit d'exercer un recours et, lorsque cela se révèle approprié, d'obtenir réparation de l'exportateur de données qui est le responsable du traitement des données à caractère personnel transférées. À titre exceptionnel, la personne concernée doit aussi avoir le droit d'exercer un recours et, lorsque cela se révèle approprié, d'obtenir réparation de l'importateur de données pour manquement par l'importateur de données ou par tout sous-traitant ultérieur qui en dépend à l'une ou à l'autre de ses obligations visées à la clause 3, paragraphe 2, dans les cas où l'exportateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable. À titre exceptionnel, la personne concernée doit aussi avoir le droit d'exercer un recours et, lorsque cela se révèle approprié, d'obtenir réparation d'un sous-traitant ultérieur dans les cas où à la fois l'exportateur de données et l'importateur de données ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables. Cette responsabilité civile du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux clauses contractuelles.

(21) Si un litige entre la personne concernée qui invoque la clause du tiers bénéficiaire et l'importateur de données n'est pas résolu à l'amiable, l'importateur de données doit proposer à la personne concernée de choisir entre la médiation et la procédure judiciaire. La personne concernée aura réellement le choix dans la mesure où elle pourra disposer de systèmes de médiation fiables et reconnus. La médiation par les autorités de contrôle de la protection des

données de l'État membre dans lequel est établi l'exportateur de données doit être une option lorsqu'elles fournissent un tel service.

(22) Le contrat doit être régi par le droit de l'État membre dans lequel l'exportateur de données est établi et qui permet à un tiers bénéficiaire de faire exécuter un contrat. Les personnes concernées doivent pouvoir être représentées par des associations ou d'autres organismes si elles le souhaitent et si le droit national l'autorise. Le même droit doit également régir les dispositions relatives à la protection des données comprises dans tout contrat conclu avec un sous-traitant ultérieur concernant la sous-traitance ultérieure des activités de traitement de données à caractère personnel transférées par l'exportateur de données vers l'importateur de données en vertu des clauses contractuelles.

(23) La présente décision s'appliquant exclusivement à la sous-traitance par un sous-traitant établi dans un pays tiers de ses services de traitement à un sous-traitant ultérieur établi dans un pays tiers, elle ne doit pas s'appliquer à la situation dans laquelle un sous-traitant établi dans l'Union européenne et effectuant le traitement de données à caractère personnel pour le compte d'un responsable du traitement établi dans l'Union européenne sous-traite ses activités de traitement à un sous-traitant ultérieur établi dans un pays tiers. Dans une telle situation, les États membres sont libres de tenir compte ou non du fait que les principes et garanties des clauses contractuelles types énoncées dans la présente décision ont été utilisés pour sous-traiter des activités à un sous-traitant ultérieur établi dans un pays tiers dans le but d'assurer une protection adéquate des droits des personnes concernées dont les données à caractère personnel sont transférées dans le cadre d'activités de sous-traitance ultérieure.

(24) Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué en vertu de l'article 29 de la directive 95/46/CE a émis un avis sur le niveau de protection prévu par les clauses contractuelles types annexées à la présente décision. Cet avis a été pris en considération dans la préparation de cette dernière.

(25) Il convient d'abroger la décision 2002/16/CE.

(26) Les mesures prévues par la présente décision sont conformes à l'avis du comité institué en vertu de l'article 31 de la directive 95/46/CE,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Les clauses contractuelles types figurant en annexe sont considérées comme offrant des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants comme l'exige l'article 26, paragraphe 2, de la directive 95/46/CE.

Article 2

La présente décision concerne uniquement le caractère adéquat de la protection fournie par les clauses contractuelles types figurant en annexe pour le transfert de données à caractère personnel. Elle n'affecte pas l'application d'autres dispositions nationales mettant en œuvre la directive 95/46/CE qui se rapportent au traitement de données à caractère personnel dans les États membres.

La présente décision s'applique au transfert de données à caractère personnel par des responsables du traitement établis dans l'Union européenne à des destinataires établis en dehors du territoire de l'Union européenne qui agissent exclusivement en tant que sous-traitants.

Article 3

Aux fins de la présente décision, on entend par:

a) «catégories particulières de données»: les données visées à l'article 8 de la directive 95/46/CE;

b) «autorité de contrôle»: l'autorité visée à l'article 28 de la directive 95/46/CE;

c) «exportateur de données»: le responsable du traitement qui transfère les données à caractère personnel;

d) «importateur de données»: le sous-traitant établi dans un pays tiers 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 conditions de la présente décision 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;

e) «sous-traitant ultérieur»: tout 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 clauses contractuelles types énoncées dans l'annexe et aux termes du contrat écrit relatif à la sous-traitance ultérieure;

f) «droit applicable à la protection des données»: 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;

g) «mesures techniques et d'organisation liées à la sécurité»: 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.

Article 4

1. Sans préjudice de leurs pouvoirs de prendre des mesures visant à assurer le respect des dispositions nationales adoptées conformément aux chapitres II, III, V et VI de la directive 95/46/CE, les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent pour interdire ou suspendre les flux de données vers des pays tiers afin de protéger les individus à l'égard du traitement de leurs données à caractère personnel, et ce dans les cas où:

   a) il est établi que le droit auquel l'importateur de données ou un sous-traitant ultérieur est soumis oblige ce dernier à déroger au droit applicable à la protection des données au-delà des limitations nécessaires dans une société démocratique pour l'une des raisons énoncées à l'article 13 de la directive 95/46/CE lorsque cette obligation risque d'avoir des conséquences négatives importantes pour les garanties offertes par le droit applicable à la protection des données et les clauses contractuelles types,

   b) une autorité compétente a établi que l'importateur de données ou un sous-traitant ultérieur n'a pas respecté les clauses contractuelles types figurant en annexe, ou

   c) il est fort probable que les clauses contractuelles types figurant en annexe ne sont pas ou ne seront pas respectées et que la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves.

2. L'interdiction ou la suspension visée au paragraphe 1 est levée dès que les raisons qui la motivaient disparaissent.

3. Lorsque les États membres adoptent des mesures conformément aux paragraphes 1 et 2, ils en informent sans délai la Commission, qui transmet l'information aux autres États membres.

Article 5

La Commission évalue l'application de la présente décision, sur la base des informations disponibles, trois ans après son adoption. Elle présente au comité institué au titre de l'article 31 de la directive 95/46/CE un rapport sur les constatations effectuées. Le rapport comprend tout élément susceptible d'influer sur l'évaluation concernant le caractère adéquat des clauses contractuelles types figurant en annexe et tout élément indiquant que la présente décision est appliquée de manière discriminatoire.

Article 6

La présente décision s'applique à compter du 15 mai 2010.

Article 7

1. La décision 2002/16/CE est abrogée avec effet au 15 mai 2010.

2. Tout contrat conclu entre un exportateur de données et un importateur de données en vertu de la décision 2002/16/CE avant le 15 mai 2010 reste en vigueur dans son intégralité aussi longtemps que les transferts et les activités de traitement de données faisant l'objet du contrat restent inchangés et que les données à caractère personnel couvertes par la présente décision continuent d'être transférées entre les parties. Si les parties contractantes décident d'apporter des modifications à cet égard ou de sous-traiter les activités de traitement faisant l'objet du contrat, elles sont tenues de conclure un nouveau contrat conforme aux clauses contractuelles types figurant en annexe.

Article 8

Les États membres sont destinataires de la présente décision.Fait à Bruxelles, le 5.2.2010

Par la Commission
Jacques BARROT
Vice-président de la Commission

AMPLIATION CERTIFIEE CONFORME
Pour la Secrétaire générale,

Jordi AYET PUIGARNAU
Directeur du Greffe

ANNEXE

Clauses contractuelles types (sous-traitants)

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 : EVERIAL, dont le siège social est situé 27 rue de la Villette 69003 LYON , immatriculée au Registre du Commerce et des Sociétés de Lyon sous le numéro 350 553 863
Représentée par Lionel GARCIA agissant en qualité de Directeur Général
(ci-après dénommée l'«**exportateur de données**»)

d'une part, et

Nom de l'organisation important les données CEPALDATA sise E 43 rue Canelle, EBENE LINKS, EBENE CITY Mauritius , représentée par Catherine LAHEURTE agissant en qualité de Directrice
(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.

PREAMBULE

Activités de l'importateur et de l'exportateur, lien entre les deux dans le cadre de l'exécution des prestations et des CCT :

EVERIAL, spécialiste de la gestion de flux documentaires, valorise et gère les documents de l'entreprise en intégrant l'ensemble de la chaîne de service du document.

CEPAL DATA, filiale d'EVERIAL, est spécialisé dans la saisie et le traitement des données, dans l'indexation des documents numérisés et dans les actions spécifiques d'appels sortants. A ce titre, EVERIAL confie à CEPAL, l'enrichissement de sa base de données clients et prospects sur l'outil Dynamics CRM, des opérations de télémarketing, d'enquêtes de satisfaction et de saisie de données.

Ces CCT annulent et remplacent toutes versions antérieures.

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[7];

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

[7] Les parties peuvent reprendre, dans la présente clause, les définitions et les significations de la directive 95/46/CE si elles estiment qu'il est préférable que le contrat soit autonome.

disparu ou a cessé d'exister en droit, à moins que l'ensemble de ses obligations juridiques 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 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 informée 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 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[8]

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

---

8 Les exigences impératives de la législation nationale le concernant et qui ne vont pas au-delà de celles qui sont nécessaires dans une société démocratique pour l'un des intérêts énoncés à l'article 13, paragraphe 1, de la directive 95/46/CE, c'est-à-dire si elles constituent une mesure nécessaire pour sauvegarder la sûreté de l'État; la défense; la sécurité publique; la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas de professions réglementées; un intérêt économique ou financier important d'un État ou la protection de la personne concernée ou des droits et libertés d'autrui, ne vont pas à l'encontre des clauses contractuelles types. Parmi les exemples de ces exigences impératives qui ne vont pas au-delà de celles qui sont nécessaires dans une société démocratique figurent, notamment, les sanctions reconnues sur le plan international, les obligations de déclaration fiscale et les obligations de déclaration de lutte contre le blanchiment des capitaux.

clauses ou le contrat 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 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 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 la France.

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[9]. 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-

[9] Cette condition peut être réputée remplie si le sous-traitant ultérieur est co-signataire du contrat conclu entre l'exportateur de données et l'importateur de données conformément à la présente décision.

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 la France.

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 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.

Au nom de l'exportateur de données :

Nom (écrit en toutes lettres) : Lionel GARCIA
Fonction : Directeur Général EVERIAL
Adresse : 27 rue de la Villette 69003 LYON

Signature

(sceau de l'organisation)

Au nom de l'importateur de données :

Nom (écrit en toutes lettres) : Catherine LAHEURTE
Fonction : Directrice, CEPAL DATA
Adresse : E 43 rue Canelle, EBENE LINKS, EBENE CITY Mauritius

Signature

(sceau de l'organisation)

APPENDICE 1 DES CLAUSES CONTRACTUELLES TYPES

Le présent appendice fait partie des clauses et doit être rempli et signé par les parties.

Les États membres peuvent compléter ou préciser, selon leurs procédures nationales, toute information supplémentaire devant éventuellement être incluse dans le présent appendice.

Exportateur de données

EVERIAL

Importateur de données

CEPAL DATA

Personnes concernées

Les données à caractère personnel transférées concernent les catégories suivantes de personnes concernées :

- **clients et prospects**

Catégories de données

Les données à caractère personnel transférées concernent les catégories suivantes de données :

- **Identité des personnes concernées (nom et prénom, adresses mail, coordonnées téléphoniques)**

Catégories particulières de données (le cas échéant)

Les données à caractère personnel transférées concernent les catégories particulières suivantes de données :

- **Néant**

Traitement

Les données à caractère personnel transférées seront soumises aux activités de traitement de base suivantes :

- **Toutes opérations relatives à la gestion des clients et du suivi de la relation client**

EXPORTATEUR DE DONNÉES
Nom (écrit en toutes lettres) : Lionel GARCIA
Fonction : Directeur Général, EVERIAL
Adresse : 27 rue de la Villette 69003 LYON

IMPORTATEUR DE DONNÉES
Nom (écrit en toutes lettres) : Catherine LAHEURTE
Fonction : Directrice, CEPAL DATA
Adresse : E 43 rue Canelle, EBENE LINKS, EBENE CITY Mauritius

APPENDICE 2 DES CLAUSES CONTRACTUELLES TYPES

Le présent appendice fait partie des clauses et doit être rempli et signé par les parties.

Description des mesures techniques et d'organisation liées à la sécurité mises en œuvre par l'importateur de données conformément à la clause 4, point d), et à la clause 5, point c) (ou document/législation jointe):

A. INSTALLATIONS CEPALDATA

1. INFRASTRUCTURE RESEAU

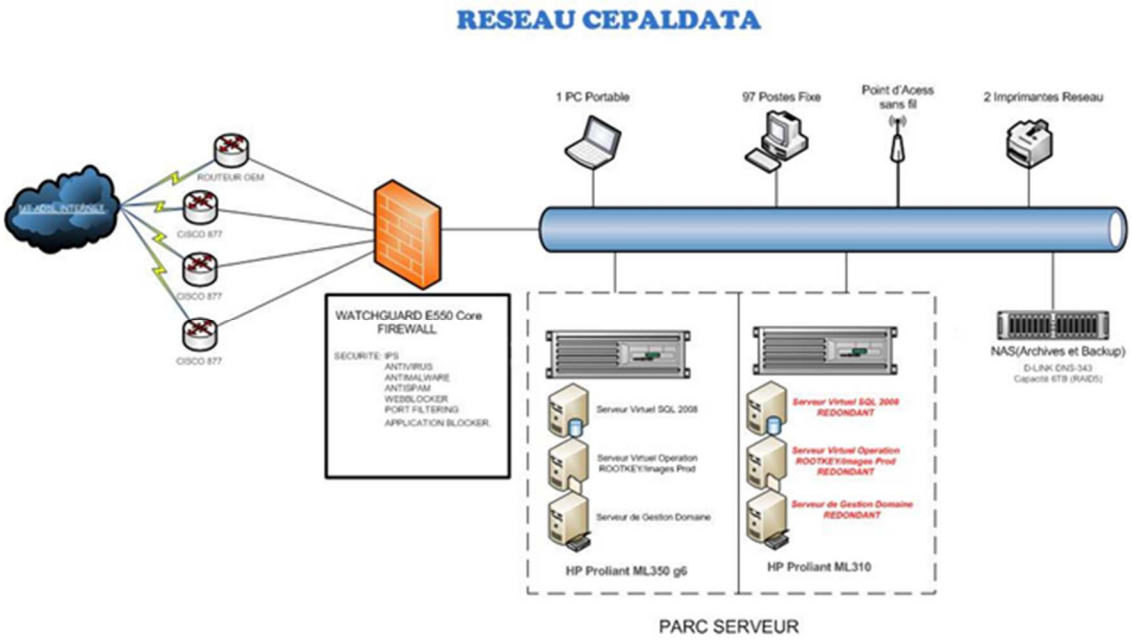
Le réseau informatique de Cepaldata Ltee est composé de plusieurs postes clients qui viennent se connecter à des serveurs sur lesquels résident les données, en l'occurrence ceux d'Everial.

Le serveur principal CEPALDATA comporte 3 disques durs de 146 Go assemblés selon la technologie RAID (acronyme de *Redundant Array of Independent Disks*, traduisez *Ensemble redondant de disques indépendants*). Celle-ci permet de constituer **une** unité de stockage à partir de plusieurs disques durs. L'unité ainsi créée (appelée **grappe**) a donc une grande tolérance aux pannes (haute disponibilité). La répartition des données sur plusieurs disques durs permet d'augmenter la sécurité et de fiabiliser les services associés. Sur ce serveur physique réside des serveurs dits virtuels ce qui permet une optimisation du système.

Un serveur redondant permettant une continuité d'activités est aussi en place, et est l'exacte copie du serveur principal.

Un Logiciel de sauvegarde automatique(R-Drive), basé sur la technologie de clonage des disques permet de faire une « photocopie » des données à tout instant et une restauration rapide en cas dysfonctionnement.

L'infrastructure est protégée par un pare-feu dit UTM (Unified Threat Management), qui protège le périmètre réseau de toutes attaques (pénétration, virus, etc…). L'équipement est de la marque Watchguard.



2. SALLE SERVEUR

La salle des serveurs est sous température et hygrométrie contrôlées.

Les périmètres fixés sont les suivants :

Température : 20-24°C

Hygrométrie : 40-60% d'humidité relative (HR)

3. NIVEAUX DE BACKUP

Les données informatiques sur le serveur Cepaldata sont sauvegardées suivant les systèmes de backup ci-dessous :

- Le Backup est constitué d'une sauvegarde des contenus des serveurs, en mode différentiel. Cette image est faite automatiquement sur une base journalière (du lundi au vendredi). Et une sauvegarde intégrale est faite chaque fin de semaine le samedi après-midi,
- toutes ces informations sont sauvegardées sur une unité de stockage spécialement conçue à cet effet appeler NAS (Network Attach Storage)

4. CHARTE INFORMATIQUE

CEPALDATA engage ses collaborateurs à respecter les conditions de la Charte des Systèmes d'Informations et recueille leur signature afin d'attester de leur bonne prise de connaissance.

Ci-dessous, extrait de la Charte :

« Chapitre 1. Périmètre d'application de la Charte.

1.1. Les acteurs.
La présente charte s'applique à toute personne utilisant les ressources informatiques et/ou téléphoniques de l'institution, y compris ceux dont l'institution autorise l'accès à distance directement ou en cascade.

1.2. Ressources matérielles.
Cette Charte établit les droits et les devoirs qui incombent aux utilisateurs des ressources informatiques et téléphoniques (poste de travail, périphériques, serveurs, réseaux, intranet, Internet, messagerie, téléphones, télécopieurs), afin d'en assurer une bonne utilisation dans le respect des lois, de la confidentialité, d'autrui et de l'établissement. L'utilisation des ressources informatiques et téléphoniques n'est autorisée que dans le cadre exclusif de l'activité professionnelle des utilisateurs.

1.3. Habilitations - accès aux ressources informatiques et téléphoniques.
Le droit d'accès au système informatique est personnel et non cessible. Il engage la responsabilité individuelle de chaque utilisateur.
- La saisie du nom d'utilisateur permet l'identification ; la saisie du mot de passe l'authentification et donnent accès aux informations correspondant au profil utilisateur.
-A chaque utilisateur relié au réseau informatique interne de l'établissement est associé un compte utilisateur, un mot de passe personnel, ainsi qu'une adresse de messagerie électronique, le cas échéant.
- cela permet une traçabilité intégrale des accès au réseau.
Pour chaque fonction, un profil de droit d'accès au système d'information du CEPALDATA Ltee est établi. Ce profil tient compte du service d'affectation et des différents domaines accessibles (Ressources Humaines, Gestion administrative, Financière, Logistique, Internet, Messagerie électronique…).
Le droit d'accès est temporaire et limité à des activités conformes aux missions de l'établissement. Il est retiré dans les cas suivants :

- L'utilisateur quitte l'établissement.
- La fonction de l'utilisateur ne le justifie plus.
- Non-respect de la présente Charte.

Le manquement aux stipulations de la présente Charte expose leur auteur à des sanctions disciplinaires, ainsi que, le cas échéant, à la mise en cause de leur responsabilité civile et/ou pénale.

Chapitre.2 : Respect des lois et de la confidentialité.

2.1. Respect de la confidentialité

2.1.1. La confidentialité des données, des ressources et services

- Les fichiers individuels ou collectifs sont confidentiels : la possibilité matérielle de lire un fichier n'implique pas l'autorisation de le lire.
- Les fichiers stocké sur les périphériques externes ne doivent être lus ni récupérés en dehors du réseau de l'établissement.
- Le poste de travail et les périphériques sont réservés à l'utilisation des opérateurs du CEPALDATA Ltee : toute personne étrangère à l'établissement n'est pas autorisé à les utiliser sauf conditions particulières.
- L'accès aux différents services et applicatifs du Système d'Information est soumis à la gestion des droits d'accès .et à des règles de sécurité.

  Le Code Pénal punit de peines correctionnelles les diverses atteintes aux systèmes de traitements automatisés de données (ordinateur, fax, …). Ainsi en est-il de l'utilisation frauduleuse du code confidentiel d'autrui ou de l'introduction de virus.

2.2 Respect d'autrui et de l'établissement.

Le contenu des informations véhiculées à l'intérieur et à l'extérieur de l'établissement est sous l'entière responsabilité personnelle de l'émetteur ; il doit respecter les règles suivantes :
- droit à l'image
- protection de la vie privée d'autrui
- ***protection juridique de Cepaldata Ltee sur le fondement du droit à l'honneur. Toute publication outrageante et/ou injurieuse à l'encontre de l'établissement engage la responsabilité pénale et civile de son auteur.***

Les règles d'utilisation du logo et de la charte graphique de l'établissement, doivent être conformes aux règles de la propriété intellectuelle.

2.2.1. La protection de la vie privée d'autrui.

- Il est interdit de mettre ou conserver en mémoire informatique, sauf accord exprès de la direction, des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des
- L'utilisateur doit s'imposer le respect des lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique ou diffamatoire.
- Les messages électroniques sont assimilés à des messages privés et ont donc un caractère confidentiel. Le contenu des informations véhiculées, par quelque moyen que ce soit, à l'intérieur ou à l'extérieur de l'établissement, est sous l'entière responsabilité de l'émetteur ; en aucun cas l'établissement ou la direction ne sauraient être tenus responsables d'une utilisation malveillante ou frauduleuse qui aurait causé des préjudices à des tiers.

2.2.2. Respect des droits de propriété

L'utilisation d'un logiciel est généralement soumise à licence, sauf pour les logiciels dits "libres".
Cela implique :
- Interdiction d'effectuer des copies de logiciels pour quelque usage que ce soit, hormis une copie de sauvegarde, réalisée exclusivement par le service informatique, dans les conditions prévues par le code de la propriété intellectuelle.
- Interdiction de contourner les restrictions d'utilisation d'un logiciel.
- modalités d'installation de logiciels uniquement réalisées par le Service Informatique.

2.2.3. Droit de propriété intellectuelle :

- Droit d'auteur défini par le Code de la Propriété intellectuelle :

C'est un droit de propriété composé d'attributs d'ordre :
- intellectuel : s'attache à toute œuvre de l'esprit, quelles qu'en soit la forme, le genre, la destination ;
- indépendant de la propriété de l'œuvre : l'auteur possède pendant toute la durée de vie de l'œuvre un droit de regard sur celle-ci ;
- exclusif : seul l'auteur est en possession de ce droit moral sur l'œuvre ;
- patrimonial : outre le droit moral, l'auteur a le droit de disposer de l'œuvre et d'en autoriser certaines exploitations ;
-opposable à tous : ce droit peut être opposé à toute personne morale ou physique, de droit privé ou public.

- Toute atteinte à un droit de propriété intellectuelle est sanctionnée par : l'indemnisation de la victime, le recours à des mesures préventives et enfin des sanctions pénales pour :

-intrusion dans le système d'autrui avec ou sans dommages
-contrefaçon (copie, diffusion)
-entrave au système (virus)
-introduction, modification, suppression de données (falsification)
-atteinte aux bonnes mœurs et à la protection des mineurs.

Chapitre.3 : Respect des règles d'usage du Système d'Information.

3.1. Usage des applicatifs métiers et services (y compris ressources partagées).

Les droits d'accès aux applicatifs métiers sont gérés par des référents métiers de chaque domaine fonctionnel. Chaque agent dispose de droits d'accès en fonction de son appartenance à une fonction et à son d'affectation

3.2. Usage des services Internet.

-Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable et présente une utilité au regard des fonctions exercées.
La politique de sécurité du CEPALDATA Ltee ferme l'accès aux sites illicites par filtrage automatique des mots clé (violents, pornographiques, racistes, révisionnistes, jeux d'argent). La liste des sites internet accessibles aux professionnels est définie par la direction. La gestion des ouvertures est assurée par le Service Informatique, qui rend compte à ladite direction.
-L'accès au réseau Internet passe par une identification nominative
Le téléchargement de documents, de logiciels, de vidéos, images animées, banques de son non liées à l'activité professionnelle de l'utilisateur est interdite.
•La diffusion par messagerie d'informations associatives n'est autorisée que pour les associations avec lesquelles le CEPALDATA Ltee a passé convention.
•L'utilisation de la diffusion générale de tout document (fonction « à tout le monde » d'Outlook) est soumise à des restrictions qui incluent courriel en chaine, et autres de même nature.

•Les forums dans le cadre de groupes de travail reconnus par l'institution sont soumis à autorisation de la direction
•Le principe de la « chaîne » : diffusion collective démultipliée par le biais du receveur d'information est interdit.
•L'utilisation privée de la messagerie à des fins personnelles doit être limitée (cf. chapitre 4).
•L'accès aux messageries personnelles et privées à partir des ressources informatiques du CEPALDATA Ltee n'est pas autorisé.

Afin de garantir au mieux la sécurité du système d'information et le respect des règles, la Direction a fait le choix de mettre en œuvre les moyens suivants :
Pour le filtrage des sites Internet, l'établissement a fait l'acquisition d'un logiciel, qui s'appuie sur un Proxy (ensemble logiciel et matériel constituant le système de filtrage). Deux niveaux d'analyse sont exécutés par cet outil, selon des règles de filtrage fixées par la Direction de l'établissement:
Le premier concerne la reconnaissance du Site concerné par la requête de l'utilisateur.
Le deuxième concerne le contenu de la page retournée suivant une liste de phrases et de mots clés pour déterminer si la page est autorisée.

Au niveau du proxy sont disponibles :
les listes non-exhaustives suivantes:

- des sites interdits classés par catégories (adulte, pornographique, Xénophobe, violent, Chat, Forum, Drogue, Piratage informatique, publicité, jeux)
- des phrases et mots clés à filtrer
- des extensions de fichiers non acceptées (.mp3 ; .exe,…).

L'ensemble des requêtes refusées et la raison du refus des trois listes précédentes.
Des statistiques d'usage du web par mois et par jour.

Au niveau du Firewall (pare-feu) sont disponibles :
les traces, non nominatives, des requêtes par poste de travail (adresse IP du jour) dans des fichiers de journalisation.

Le croisement de l'ensemble des données statistiques et des fichiers traces permet de repérer l'origine de la requête.
De ce fait, les utilisations des ressources matérielles ou logiciels informatiques, ainsi que des échanges via le réseau, peuvent être analysées et contrôlées dans le respect des lois en vigueur.
La prise de main à distance pour détecter et réparer les pannes à distance sur les postes de travail est réalisée par l'ensemble des informaticiens du service avec des outils appropriés avec l'accord préalable de l'utilisateur.
Les utilisateurs engagent de manière pleine et entière leur responsabilité personnelle au titre des informations qu'ils véhiculent aussi bien à l'intérieur de l'établissement que vers l'extérieur. L'hôpital ne peut en aucun cas être tenu pour responsable de leurs agissements malveillants et/ou frauduleux qui auraient causé des dommages à des tiers.**3.3. Usage des services téléphoniques.**
Seuls ont vocation à être appelés les numéros de téléphone présentant un lien direct et nécessaire avec l'activité professionnelle. La durée de communication doit être raisonnable et en adéquation avec les fonctions exercées.
L'accès au réseau téléphonique passe par une identification nominative de la ligne

Chapitre 4 : Engagement des utilisateurs

4.1. Droits et devoirs des utilisateurs.

- Tout utilisateur est responsable de l'usage de tous les services et ressources auxquels il a accès ; il a aussi la charge, à son niveau, de contribuer à la sécurité générale et à celle de l'institution.
- Par sécurité, il est conseillé de ne pas divulguer son adresse électronique dans les forums et sur les sites Internet non professionnels, en raison du risque accru de virus sur le réseau Internet et de surcharge inutile de sa boîte aux lettres.
- De même, ne pas installer de programmes, de matériels ou autres outils informatiques sans l'accord du service informatique.
- Les agents se doivent d'user des différents outils de télécommunications mis à leur disposition conformément aux principes énoncés, à savoir ceux du respect d'autrui et de bonne conduite professionnelle, sous peine de sanctions disciplinaires.
- L'utilisateur s'engage à respecter le matériel, ne pas le manipuler de façon anormale, ni à introduire des logiciels parasites, ni à utiliser les périphériques (écrans, claviers, souris…) pour ses besoins personnels.

1. La connexion d'un équipement sur le réseau est soumise à autorisation. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers.

- L'accès à la salle informatique est strictement réservé aux informaticiens. Tout prestataire devant intervenir dans la salle devra obligatoirement être accompagné d'un membre de l'équipe.
- L'accès aux locaux techniques (baies, réseau, éléments actifs..) est strictement réservé aux informaticiens, les personnels des services techniques accèdent uniquement aux onduleurs.
- L'utilisateur ne doit pas tenter, directement ou indirectement, de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre.
- Attention à ne pas divulguer par quelque moyen que ce soit (téléphone, fax, Internet, courrier…) une information à caractère confidentiel.
- L'utilisateur doit être vigilant par rapport aux personnes utilisant son poste de travail (par exemple, un fournisseur doit impérativement être accompagné d'un membre de l'équipe informatique, ou annoncé et autorisé par lui, pour assurer toute intervention sur place ou à distance de type télémaintenance, postes multiutilisateurs, …).
- L'utilisateur ne doit pas quitter son poste de travail en laissant des ressources ou services accessibles sans se déconnecter et/ou veiller au verrouillage de sa session.
- L'utilisateur différenciera le contenu professionnel et le contenu personnel en demandant à ses correspondants d'indiquer la mention "personnel" ou "privé", et en créant un répertoire "personnel" ou "privé" pour stocker ses documents et messages personnels. En échange, il s'engage à ne pas transformer des informations professionnelles en informations personnelles.
- Quoi qu'il en soit, leur utilisation doit être conforme aux principes de courtoisie. De son côté, l'employeur qui respecte le droit à la vie privée des utilisateurs s'engage à ne pas lire le courrier électronique contenu dans le répertoire "personnel" ou "privé" de l'utilisateur.

4.2. Règles d'utilisation, de sécurité et de bon usage.

Il appartient à chaque utilisateur de :

- Modifier ses mots de passe régulièrement et de les garder secrets.
- Protéger ses données d'une éventuelle intrusion ; il est responsable des droits qu'il donne aux autres utilisateurs. Il ne doit pas mettre à la disposition d'utilisateurs non autorisés un accès au système ou aux réseaux, à travers des matériels dont il a l'usage.
- protéger ses données d'une éventuelle défaillance du disque dur du poste de travail en les sauvegardant régulièrement. L'utilisateur est seul responsable de ses sauvegardes.
- Ne pas utiliser des comptes autres que les siens.
- Signaler toute tentative de violation de son compte et toute anomalie.
- Ne pas déposer des documents confidentiels et des fichiers nominatifs sur l'espace disque de partage accessible à tous, et sur les espaces réservés par service. Ces espaces doivent être soumis aux mêmes règles de confidentialité.

Chapitre 5 : Engagement des informaticiens.

5.1 Engagement des informaticiens

Les informaticiens dûment habilités par le responsable informatique, et qui doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes, peuvent être conduits par leurs fonctions à avoir accès à l'ensemble des informations relatives aux utilisateurs, y compris celles qui sont enregistrées sur le disque dur du poste de travail, dans le respect du secret professionnel.Toute prise en mains à distance nécessite l'accord préalable de l'utilisateur du poste de travail.

5.2 Rôles des Informaticiens :

- Sont responsables de la qualité de service des ressources qu'ils ont en charge.
- Doivent appliquer la politique de sécurité informatique définie par l'établissement et donc appliquer les recommandations fournies par la Direction et le responsable informatique de l'établissement.
- Doivent avertir le responsable informatique de l'établissement lorsqu'ils détectent (ou sont informés par un utilisateur) des problèmes liés à la sécurité informatique. En fonction de la nature des problèmes et de son degré de gravité, la Direction du système d'information et le responsable informatique déclenchent un audit de sécurité avec l'informaticien. Il en sera rendu compte à la Direction.
- Doivent respecter la confidentialité des fichiers utilisateurs, des courriers et des sorties imprimantes auxquels ils peuvent être amenés à accéder lors des tâches d'administration et/ou lors d'audits de sécurité (cf. secret professionnel).
- Assurent la sauvegarde de l'ensemble des données, à l'exception des données bureautiques locales, ainsi que des ressources :
  •espace partagé pour toutes les personnes d'un ou plusieurs services
  •espace personnel sur les serveurs de fichiers afin d'y stocker ses documents
  •espaces publics

Rappel : Seules les données bureautiques stockées sur les postes de travail ne sont pas sauvegardées par le service informatique, elles sont à la charge de l'utilisateur.

5.3 Rôle des informaticiens dans la fonction d'administrateur :

Afin d'assurer le bon fonctionnement des systèmes informatiques et du réseau, sous couvert du responsable informatique, l'informaticien-administrateur :

- Est responsable de la distribution et du retrait des droits d'accès.
- Doit faire respecter les droits et responsabilités des utilisateurs sur les ressources.
- Peut accéder à des fichiers ou des courriers (réaliser un diagnostic, une correction d'un problème…).
- Peut prendre toutes dispositions nécessaires (arrêts de travaux, suppression de droits d'accès, verrouillage de fichiers…) en vue de :
  - •Contrôler la bonne utilisation des ressources
  - •Figer un état lors de problèmes liés à la sécurité des systèmes informatiques
  - •Arrêter un engorgement de ces ressources
  - •Permettre le fonctionnement optimal des ressources informatiques qu'il a en charge. »

EXPORTATEUR DE DONNÉES
Nom (écrit en toutes lettres) : Lionel GARCIA
Fonction : Directeur Général, EVERIAL
Adresse : 27 rue de la Villette 69003 LYON

IMPORTATEUR DE DONNÉES
Nom (écrit en toutes lettres) : Catherine LAHEURTE
Fonction : Directrice, CEPAL DATA
Adresse : E 43 rue Canelle, EBENE LINKS, EBENE CITY Mauritius