Règles d'entreprise contraignantes (Binding Corporate Rules, ou BCR) applicables aux transferts intragroupe de Données à caractère personnel vers des pays situés en dehors de l'EEE

1. INTRODUCTION

Le Groupe SOPRA HR SOFTWARE considère ses clients et ses employés comme ses actifs les plus précieux et s'engage par conséquent à leur accorder une attention particulière et un niveau de prestation optimal, dans un souci de confiance mutuelle. Dans ce contexte, le Groupe attache une grande importance au droit des clients et employés à la protection de leur vie privée.

Conformément aux dispositions du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, les transferts de Données à caractère personnel vers des pays situés en dehors de l'Espace économique européen doivent être assortis de garanties spécifiques visant à assurer le respect des principes européens en matière de protection des données. L'adoption et la mise en œuvre de Règles d'entreprise contraignantes (*Binding Corporate Rules*, ou BCR) au sein de SOPRA HR SOFTWARE ont pour objectif de réglementer les transferts intragroupes de Données à caractère personnel vers des pays situés en dehors de l'Espace économique européen (EEE), conformément aux dispositions du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016.

Au-delà de ces considérations, il est du devoir de SOPRA HR SOFTWARE et de ses employés de protéger et respecter les données à caractère personnel qui leur sont communiquées. Nos BCR représentent à cet égard un outil essentiel. Elles nous permettent de transmettre à l'ensemble du Groupe notre profond attachement à la protection de la vie privée.

Les entités et les employés concernés de SOPRA HR SOFTWARE sont tenus de respecter nos BCR, tout en se conformant à la législation applicable au niveau local.

Au niveau local, chaque Sous-traitant local doit, conformément aux stipulations de nos BCR, signer une Convention d'adhésion aux BCR et prendre toutes les mesures nécessaires pour garantir leur application. Le respect de ces stipulations et procédures reposera principalement sur la mise en œuvre, au quotidien, de programmes de formations et d'audit.

Du fait de leur large portée, les BCR permettront sans aucun doute de faciliter la gestion des questions de protection de la vie privée au niveau local et de garantir l'implication des représentants locaux en la matière.

En cas de violation avérée des BCR, le Responsable principal du traitement, le Responsable EMEA de la protection des données, le Responsable local du traitement ou le Responsable local de la protection des données pourra prendre les mesures correctives (juridiques, techniques ou organisationnelles) et sanctions (à l'encontre du Responsable local du traitement ou, selon le droit du travail applicable au niveau local, un employé local) qu'il jugera appropriées.

2. DÉFINITIONS ET PRINCIPES DE PROTECTION DES DONNÉES

2.1. DÉFINITIONS

Les termes et expressions utilisés dans les BCR sont définis en Annexe 1 et interprétés, en toutes circonstances, conformément au Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016.

2.2. PRINCIPES DE PROTECTION DES DONNÉES

Dans le cadre des BCR (se reporter à l'alinéa 3), les transferts de Données à caractère personnel vers un pays tiers ne garantissant pas un niveau de protection adéquat doivent systématiquement être conformes aux principes de protection des données visés aux alinéas concernés des BCR ou en Annexe 2, conformément aux dispositions du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016.

- **Base juridique du traitement des Données à caractère personnel et des Données sensibles :** Les Données à caractère personnel et les Données sensibles doivent être traitées conformément aux dispositions du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016.
- **Limitation des finalités :** Les Données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.
- **Qualité, minimisation et proportionnalité des données** Les Données à caractère personnel doivent être traitées de manière licite et loyale. Les Données personnelles doivent être adéquates, pertinentes et leur volume ne doit pas être excessif au regard des finalités pour lesquelles elles sont collectées et/ou traitées. Les Données à caractère personnel doivent être exactes et, au besoin, actualisées. Les Données à caractère personnel doivent être conservées sous une forme permettant l'identification des Personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement.
- **Décisions individuelles automatisées :** Chaque Personne concernée a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard, prise sur le seul fondement d'un traitement automatisé de données.
- **Droit d'information :** Les Données à caractère personnel doivent toujours être collectées puis traitées de manière transparente (se reporter à l'alinéa 4.1)
- **Droits d'accès, de rectification, d'effacement, de verrouillage des données, de limitation du traitement, d'opposition au traitement et à la portabilité :** Les Personnes concernées ont le droit de savoir quelles informations les concernant sont détenues par SOPRA HR SOFTWARE, et d'en garder le contrôle (se reporter à l'alinéa 4.2).
- **Sécurité et confidentialité :** Des mesures techniques et d'organisation appropriées doivent être mises en œuvre pour protéger les Données à caractère personnel contre la destruction fortuite ou illicite, la perte fortuite, l'altération, la diffusion ou l'accès non autorisés, ainsi que contre toute autre forme de traitement illicite (se reporter à l'alinéa 4.5).
- **Principe de licéité** : Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :
  - la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques
  - le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
  - le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis
  - le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement
- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.
- Ce dernier point ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

- Limitation de la conservation : Les Données Personnelles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.
- Garantie lors du traitement de catégorie particulière de données personnelles : les Données Personnelles particulières sont traitées par SOPRA HR SOFTWARE selon les modalités de l'annexe 2 des présentes.
- Protection des données dès la conception et protection des données par défaut : des mesures techniques et organisationnelles ont été mises en place de manière à préserver dès le départ la vie privée et les principes en matière de protection des données : notamment par la mise en place de limitation des champs à renseigner dans les applications SIRH , des durées de conservation adéquates et accessibilité limitée.

3. Exigences relatives aux transferts ultérieurs à des organismes non liés par les BCR : Ces transferts doivent répondre aux modalités de l'article 6.2 des présentes BCR.PORTÉE DES BCR

3.1. PORTÉE GÉOGRAPHIQUE

Les BCR s'appliquent aux transferts de Données à caractère personnel depuis des entités SOPRA HR SOFTWARE établies au sein de l'Union européenne vers d'autres entités du groupe établies dans le reste du monde, dont la liste figure en Annexe 3.

L'Annexe 3 répertorie l'ensemble des entités SOPRA HR SOFTWARE liées par les BCR.

3.2. PORTÉE MATÉRIELLE

La nature et les finalités des Données à caractère personnel transférées dans le cadre des BCR sont exposées en Annexe 4.

4. EFFICACITÉ DES BCR

4.1. TRANSPARENCE ET DROIT À L'INFORMATION

Afin d'assurer un traitement loyal des données, les Données à caractère personnel sont toujours collectées puis traitées de manière transparente. Par conséquent :

1. Les BCR doivent toujours être aisément accessibles par toutes les

Personnes concernées, et être disponibles par conséquent sur les sites Internet et l'Intranet de SOPRA HR SOFTWARE. Les Personnes concernées doivent en toute occasion pouvoir obtenir, sur demande, une copie des BCR auprès du Responsable local de la protection des données, du Responsable local du traitement ou du Responsable EMEA de la protection des données.

2. En outre, des FAQ dédiées doivent être mises à la disposition des Personnes concernées sur les sites Internet de SOPRA HR SOFTWARE, afin de répondre à leurs questions éventuelles concernant les BCR ou des sujets connexes, tels que la procédure de demande d'accès aux Données à caractère personnel (se reporter à l'alinéa 4.2) ou de réclamation (se reporter à l'alinéa 4.3).

3. Les opérations de traitement de données et, le cas échéant, les transferts de données entre entités SOPRA HR SOFTWARE situées dans le monde entier doivent faire l'objet d'avis relatifs à la protection des données.

Les Responsables locaux de la protection des données, en coordination avec le Responsable EMEA de la protection des données, doivent pouvoir fournir des avis types à chaque Responsable du traitement local au sein du groupe, à toute fin nécessitant la communication d'informations aux Personnes concernées.

SOPRA HR SOFTWARE communiquera aux Personnes concernées les informations suivantes au minimum, si celles-ci ne leur ont pas déjà été communiquées :

a. l'identité du responsable du traitement et de son représentant, ses coordonnées, les coordonnées du DPO, ainsi que, le cas échéant, le lieu d'implantation de l'Importateur local de données, en dehors de l'EEE ;

b. les finalités du traitement auquel les données sont destinées et, le cas échéant, la ou les finalités du transfert des données en dehors de l'EEE ;

c. toute information supplémentaire telle que :

- les catégories de données à caractère personnel concernées ;
- les Destinataires ou les catégories de Destinataires des données ;
- le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse ;
- l'information le cas échéant de l'intention du Responsable de traitement d'effectuer un transfert de données à caractère personnel à un destinataire dans un pays tiers.
- La durée pendant laquelle les données à caractère personnel seront conservées, ou les critères utilisés pour déterminer cette durée quand la durée n'est pas possible à déterminer.
- l'existence d'un droit d'accès aux données la concernant, d'un droit à la rectification ou à l'effacement de celles-ci, de limitation du traitement relatif à la personne concernée, le droit d'opposition au traitement, le droit de portabilité des données.

En cas d'ajout d'une nouvelle finalité ou d'une nouvelle catégorie de Destinataires à une procédure de traitement existante, l'avis d'information doit être modifié en conséquence et les Personnes concernées doivent être informées d'une telle modification.

Lorsque les données n'ont pas été collectées directement auprès de la Personne concernée, SOPRA HR SOFTWARE doit fournir les informations énumérées ci-dessus au moment de la collecte des Données à caractère personnel la concernant ainsi que la source d'où proviennent les données à caractère personnel et, le cas échéant , une mention indiquant qu'elles sont issues ou non de sources

accessibles au public ou, si la divulgation desdites données à un tiers est envisagée, lors de la première communication de données au plus tard.
Conformément au Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, et nonobstant toute disposition législative applicable au niveau national, l'obligation d'information prévue par la présente clause ne s'applique pas, à titre exceptionnel, si l'information de la personne concernée se révèle impossible ou implique un effort disproportionné, ou si la législation prévoit expressément l'enregistrement ou la communication des données (se reporter à l'alinéa 6.3).

DROITS D'ACCES, DE RECTIFICATION, D'EFFACEMENT, DE VERROUILLAGE DES DONNEES, DE LIMITATION DU TRAITEMENT, D'OPPOSITION, DROIT A LA PORTABILITE Les Personnes concernées ont le droit de savoir quelles informations les concernant sont détenues par SOPRA HR SOFTWARE, et d'en garder le contrôle. Par conséquent :

1. Toute Personne concernée a le droit d'obtenir de SOPRA HR SOFTWARE :

a. sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs et, le cas échéant, conformément au droit national :

- la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les Destinataires ou les catégories de Destinataires auxquels les données sont communiquées ;
- la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine des données ;
- la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, au moins dans le cas des décisions automatisées visées à l'alinéa 4.3 ;

b. selon le cas, accès, de rectification, d'effacement, de verrouillage des données, de limitation du traitement, droit à la portabilité des Données à caractère personnel en raison du caractère incomplet ou inexact des données ;

c. de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement.

Conformément au Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, l'exercice de ces droits peut être soumis à certaines restrictions.

2. Les Personnes concernées doivent être clairement informées, conformément à l'alinéa 4.1, de la manière de procéder afin d'exercer leurs droits.

3. Des lignes directrices et des procédures doivent être mises en place au sein du Groupe, au niveau local, afin de garantir l'exercice des droits énoncés ci-dessus.

Plus particulièrement, les employés de SOPRA HR SOFTWARE chargées de collecter ou de traiter les Données à caractère personnel ou y ayant accès doivent suivre une formation afin de reconnaître une demande d'accès, de rectification, d'effacement, de verrouillage des données, de limitation du traitement d'opposition, droit à la portabilité de Données à caractère personnel émanant d'une Personne concernée. Chaque demande doit faire l'objet d'un accusé de réception et être traitée conformément à la procédure applicable au niveau local. Une réponse spécifique doit être systématiquement adressée à la Personne concernée dans un délai

raisonnable. Si la demande est jugée légitime, SOPRA HR SOFTWARE doit prendre toutes les mesures nécessaires pour régler le problème en temps utile. En cas de rejet de la demande, la Personne concernée doit en être informée par écrit. Dans un tel cas, la Personne concernée peut utiliser le mécanisme interne de réclamation évoqué à l'alinéa 4.4.

4. Les Responsables locaux de la protection des données, en coordination avec le Responsable EMEA de la protection des données, doivent toujours se tenir à la disposition du Sous-traitant local et des Personnes concernées afin de les aider.

4.3 DÉCISION INDIVIDUELLE AUTOMATISÉE

Sous réserve du droit applicable au niveau local, toute Personne concernée a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, sa fiabilité, son comportement, etc.

4.4 MÉCANISME INTERNE DE RÉCLAMATION

Toute Personne concernée jugeant que les Données à caractère personnel la concernant ne sont pas traitées conformément aux BCR ou au droit applicable au niveau local peut formuler une réclamation afin d'obtenir l'adoption de mesures correctives et, le cas échéant, une indemnisation appropriée (se reporter aux alinéas 5.2 et 5.4). Par conséquent :

1. des lignes directrices et procédures spécifiques doivent avoir été mises en place au sein du Groupe au niveau local, afin de garantir la fiabilité du mécanisme de réclamation et de garantir que les Personnes concernées sont suffisamment informées des procédures de réclamation. Les plaintes doivent être traitées par un département clairement identifié au niveau local, bénéficiant d'un degré d'indépendance suffisant dans l'exercice de ses fonctions (le responsable local de la conformité ou le Directeur juridique, par exemple). Toute plainte enregistrée doit faire l'objet d'un accusé de réception et être traitée dans un délai raisonnable (un mois).
2. Lorsque les représentants de SOPRA HR SOFTWARE ne parviennent pas à traiter une plainte au niveau local, le mécanisme de réclamation doit permettre de remonter le problème au Responsable EMEA de la protection des données, qui est tenu de la traiter dans un délai de 1 mois. Les Responsables locaux du traitement et les Responsables locaux de la protection des données doivent rendre compte régulièrement au Responsable EMEA de la protection des données des plaintes traitées au niveau local afin de lui permettre de mettre en œuvre des mesures correctives et d'améliorer les lignes directrices et procédures mises en place au sein du Groupe si les plaintes révèlent une « défaillance » des mesures de protection de la vie privée.
3. Les représentants et employés de SOPRA HR SOFTWARE sont tenus de déployer leurs meilleurs efforts, au niveau local, pour aider le Sous-traitant local ou le Responsable local de la protection des données à traiter les plaintes reçues (se reporter à l'alinéa 5.3).

Avant d'introduire un recours auprès d'un tribunal compétent, chaque partie doit s'efforcer de régler le litige par le biais du mécanisme interne de réclamation décrit ci-dessus.

4.5 SÉCURITÉ ET CONFIDENTIALITÉ

EXPLICATIONS SUR LA FAÇON DONT LES DONNÉES PERSONNELLES SONT PROTÉGÉES LORSQU'IL EST FAIT APPEL À UN SOUS-TRAITANT ULTERIEUR QUI EST UNE FILIALE DU GROUPE

La protection des informations personnelles contre les atteintes à la sécurité des données constitue l'une des priorités de SOPRA HR SOFTWARE. Par conséquent :

1. Chaque Responsable local du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction fortuite ou illicite, la perte fortuite, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

Par conséquent, SOPRA HR SOFTWARE doit garantir la sécurité des informations grâce à la mise en place, au sein du groupe, de politiques et procédures appropriées, fixant l'ensemble des mesures physiques et logiques nécessaires pour empêcher la destruction ou la modification fortuite des Données à caractère personnel, ou toute diffusion ou accès non autorisé. Ces politiques et procédures doivent faire l'objet d'audits réguliers (se reporter à l'alinéa 4.7).

2. Les Données sensibles doivent faire l'objet de mesures de sécurité renforcées et spécifiques.
3. L'accès aux Données à caractère personnel est limité aux Destinataires, dans la seule mesure nécessaire à l'exécution de leurs obligations professionnelles. Les employés de SOPRA HR SOFTWARE qui ne respectent pas les politiques et procédures applicables en matière de sécurité des informations peuvent faire l'objet de sanctions disciplinaires.

Lorsqu'un Responsable local du traitement demande à une autre entité SOPRA HR SOFTWARE de traiter des Données à caractère personnel pour son compte (pour une courte ou une longue période, selon le cas), les garanties suivantes doivent être mises en place :

1. À l'endroit où les données sont traitées, le Sous-traitant local sélectionne un Sous-traitant fournissant des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et doit veiller au respect de ces mesures. L'entité SOPRA HR SOFTWARE ainsi sélectionnée s'engage par écrit à fournir de telles garanties. Les Responsables locaux de la protection des données doivent pouvoir fournir, en coordination avec le Responsable EMEA de la protection des données, des clauses types adaptées aux Responsables locaux du traitement faisant partie du Groupe.
2. L'entité SOPRA HR SOFTWARE ainsi sélectionnée ne peut traiter les données qui lui sont sous-traitées que sur instruction du responsable du traitement, sauf si le droit applicable lui impose de le faire.
3. Une fois le travail terminé, l'entité SOPRA HR SOFTWARE ainsi sélectionnée s'engage à supprimer l'ensemble des données transférées ou, si elle est soumise à des obligations légales de conservation des données, à conserver les données transférées en mettant en place des mesures techniques et d'organisation appropriées afin d'empêcher tout traitement illégal.

4.6 PROGRAMMES DE FORMATION

Les employés de SOPRA HR SOFTWARE chargés de la collecte et du traitement de Données à caractère personnel ou y ayant accès doivent suivre des programmes de formation spécifiques afin d'améliorer leurs connaissances et leurs compétences pratiques en matière de protection des données, et plus particulièrement sur les BCR :

1. Les BCR et les lignes directrices, procédures ou politiques applicables sont disponibles sur l'Intranet du groupe SOPRA HR SOFTWARE et peuvent être consultés à tout moment par l'ensemble des employés.
2. Chaque nouvel employé de SOPRA HR SOFTWARE peut consulter les BCR ainsi que l'ensemble des lignes directrices, procédures et politiques applicables en la matière. Des notes internes doivent également être diffusées au sein du groupe afin de mieux faire connaître les BCR.
3. Les nouveaux employés chargés de la collecte et du traitement de Données à caractère personnel ou y ayant accès doivent suivre un programme de formation sur la protection de la vie privée, qui doit également être dispensé régulièrement à tous les employés chargés de la collecte et du traitement de Données à caractère personnel ou y ayant accès. [Chaque employé doit se soumettre à un test de connaissances (certification) à l'issue de la formation, afin de vérifier ses connaissances et ses compétences en matière de protection de la vie privée].
4. Au niveau local, les responsables du traitement et/ou les Responsables locaux de la protection des données ont toute latitude pour améliorer les programmes de formation sur la protection de la vie privée décrits ci-dessus, en y intégrant des supports de formation adaptés.
5. Les programmes de formation sur la protection de la vie privée doivent être examinés et validés par des cadres de SOPRA HR SOFTWARE ayant une expérience dans ce domaine, en coordination avec le Sous-traitant local, le Responsable local de la protection des données et le Responsable groupe de la protection des données. Les procédures liées aux programmes de formation sur la protection de la vie privée doivent faire l'objet d'audits réguliers (se reporter à l'alinéa 4.7).

4.7 PROGRAMME D'AUDIT

Des audits réguliers doivent être réalisés (une fois tous les trois ans au moins, voire plus fréquemment si la législation locale impose des audits plus réguliers) par des équipes d'audit internes ou externes agréées, afin de s'assurer que les BCR et les politiques, procédures et lignes directrices s'y rapportant sont à jour et respectées :

1. Les audits relatifs à la protection des données doivent couvrir tous les aspects des BCR et des politiques, procédures et lignes directrices y afférentes, y compris les moyens utilisés pour garantir la mise en œuvre de mesures correctives. Toutefois, chaque audit peut également se concentrer sur certains aspects des BCR et/ou des politiques, procédures et lignes directrices uniquement, y compris sur les moyens utilisés pour garantir la mise en œuvre de mesures correctives.

2. Les audits relatifs à la protection des données doivent être menés sur décision du Département Conformité ou à la demande du Sous-traitant principal, d'un Responsable local de la protection des données ou du Responsable groupe de la protection des données. Les personnes chargées de mener des audits doivent jouir, en toutes circonstances, d'un niveau d'indépendance adéquat dans le cadre de l'exercice de leurs fonctions.

3. Les résultats de tous les audits doivent être communiqués au Responsable principal du traitement (et plus particulièrement à sa direction), au Responsable local du traitement et/ou au Responsable local de la protection des données et/ou au Responsable EMEA de la protection des données.
4. Les Autorités de protection des données compétentes doivent recevoir une copie de ces audits si elles en font la demande. Chaque Responsable local du traitement consent à se soumettre aux audits réalisés par les Autorités de protection des données et à suivre les conseils des Autorités de protection des données concernant toute question se rapportant aux BCR.
5. Conformément au point 3 de l'alinéa 5.1, les Responsables locaux de la protection des données doivent rendre compte chaque année au Responsable principal du traitement, en coordination avec le Responsable EMEA de la protection des données, de toutes les actions et mesures mises en œuvre en matière de Protection des données (programmes de formation, inventaire des moyens de traitement utilisés, gestion des plaintes, etc.). En outre, chaque Responsable local de la protection des données doit prendre les mesures nécessaires pour s'assurer du respect des BCR par les Sous-traitants locaux. À cette fin, une « Liste de contrôle relative aux BCR » doit être utilisée au niveau local, afin de procéder à des contrôles de conformité.
6. Le Responsable EMEA de la protection des données doit également rendre compte au Responsable principal du traitement, à intervalles réguliers, de la mise en œuvre des BCR au niveau de chaque Responsable local du traitement.
7. À partir des résultats d'audit et des comptes rendus évoqués ci-dessus, le Responsable principal du traitement (et plus particulièrement sa direction), et/ou le Responsable groupe de la protection des données doivent élaborer des mesures légales, techniques ou d'organisation appropriées afin d'améliorer la gestion de la protection des Données au sein du groupe, au niveau mondial et/ou local.

5. OPPOSABILITÉ DES BCR

5.1 RESPECT DES RÈGLES ET CONTRÔLE DE LEUR APPLICATION

Au niveau local, le Responsable local de la protection des données est responsable de la mise en œuvre des BCR. Par conséquent :

1. Chaque entité SOPRA HR SOFTWARE doit prendre les mesures nécessaires pour s'assurer du respect des BCR par les Responsables locaux du traitement. À cette fin, une « Liste de contrôle relative aux BCR » doit être utilisée au niveau local, afin de procéder à des contrôles de conformité. Les audits sur la protection des données décidés par le Département Conformité ou le Responsable EMEA de la protection des données peuvent se concentrer sur la manière dont ces contrôles de conformité sont menés au niveau local.
2. Les Responsables locaux de la protection des données, en coordination avec le Responsable EMEA de la protection des données, doivent toujours se tenir à la disposition du Responsable local du traitement et des Personnes concernées afin de les aider à régler tout problème lié à la protection des données, et plus particulièrement aux BCR.
3. Les Responsables locaux de la protection des données doivent rendre compte chaque année au Responsable principal du traitement, en coordination avec le Responsable EMEA de la protection des

données, de toutes les actions et mesures mises en œuvre en matière de Protection des données (programmes de formation, inventaire des moyens de traitement utilisés, gestion des plaintes, etc.), et plus particulièrement de la mise en œuvre des BCR.

4. Les Responsables locaux du traitement et les Responsables locaux de la protection des données doivent régulièrement rendre compte au Responsable EMEA de la protection des données des plaintes traitées au niveau local afin de lui permettre de mettre en œuvre des mesures correctives et d'améliorer les lignes directrices et procédures mises en place au sein du Groupe si les plaintes révèlent une « défaillance » des mesures de protection de la vie privée.

5. Les Responsables locaux de la protection des données, en coordination avec le Responsable EMEA de la protection des données, doivent pouvoir fournir à chaque Responsable local du traitement faisant partie du Groupe des documents types adaptés (avis d'information, clauses, etc.) en matière de protection des données.

En outre, des mesures de contrôle spécifiques doivent être mises en place afin de garantir la bonne application des BCR :

1. Le Responsable EMEA de la protection des données doit rendre compte au Responsable principal du traitement, à intervalles réguliers, de la mise en œuvre des BCR au niveau de chaque Responsable local du traitement.

2. Les audits relatifs à la protection des données doivent être menés sur décision du Département Conformité ou à la demande d'un Responsable local du traitement, d'un Responsable local de la protection des données ou du Responsable EMEA de la protection des données. Tous les résultats d'audit ou comptes rendus doivent être communiqués au Responsable principal du traitement (et plus particulièrement à sa direction), au Responsable local du traitement et/ou au Responsable local de la protection des données et/ou au Responsable EMEA de la protection des données.

3. À partir des résultats d'audit et des comptes rendus évoqués ci-dessus, le Responsable principal du traitement (et plus particulièrement sa direction), le Responsable EMEA de la protection des données, un Responsable local du traitement ou un Responsable local de la protection des données doit élaborer des mesures appropriées afin d'améliorer la gestion de la protection des Données au sein du groupe, au niveau global et/ou local.

4. En cas de violation avérée des BCR, le Responsable principal du traitement, le Responsable EMEA de la protection des données, un Responsable local du traitement ou un Responsable local de la protection des données pourra prendre les mesures correctives (juridiques, techniques ou organisationnelles) et sanctions (à l'encontre du Responsable local du traitement ou, selon le droit du travail applicable au niveau local, un employé local) qu'il jugera appropriées.

5. Les programmes de formation sur la protection de la vie privée doivent être examinés et validés par des cadres de SOPRA HR SOFTWARE, en coordination avec le Responsable EMEA de la protection des données et les Responsables locaux de la protection des données.

Les procédures liées aux programmes de formation sur la protection de la vie privée doivent faire l'objet d'audits réguliers (se reporter à l'alinéa 4.7).

5.2 DROITS DE TIERS BÉNÉFICIAIRES

Une Personne concernée peut, en qualité de tiers bénéficiaire, faire appliquer les stipulations des BCR relatives :

- à la limitation des finalités, à la qualité des données et aux principes de proportionnalité et de légitimité (se reporter à l'alinéa 2.2 et à l'Annexe 2)
- au principe de transparence et à la facilité d'accès aux BCR (se reporter à l'alinéa 4.1)
- aux droits d'accès, de rectification, d'effacement et de verrouillage des données, et à l'objet du traitement, d'opposition, à la portabilité (se reporter à l'alinéa 4.2)
- aux droits en cas de décisions individuelles automatisées (se reporter à l'alinéa 4.3)
- aux principes de sécurité et de confidentialité (se reporter à l'alinéa 4.5)
- aux restrictions aux transferts ultérieurs en dehors du groupe (se reporter à l'alinéa 6.2)
- à la législation nationale entravant le respect des BCR (se reporter à l'alinéa 6.3)
- au droit de déposer une plainte par l'intermédiaire du mécanisme interne de réclamation (se reporter à l'alinéa 4.4)
- au devoir de coopération avec les Autorités de protection des données (se reporter à l'alinéa 5.6)
- à la responsabilité et aux voies de recours (se reporter aux alinéas 5.3 et 5.4)

5.3 RESPONSABILITÉ

La responsabilité de l'Importateur ou de l'Exportateur local de données est engagée en cas de manquement aux BCR, selon les conditions suivantes :

1. Dans les cas impliquant des allégations de manquement dans le chef de l'Importateur local de données, la Personne concernée doit d'abord demander à l'Exportateur local de données de prendre des mesures appropriées pour faire valoir ses droits à l'encontre de l'Importateur local de données. Si l'Exportateur local de données ne prend pas ces mesures dans des délais raisonnables (qui, dans des circonstances normales, seraient d'un mois), la Personne concernée peut alors faire valoir ses droits à l'encontre de l'Importateur local de données directement. Une Personne concernée est également en droit de procéder directement à l'encontre d'un Exportateur local de données qui n'a pas entrepris de démarches raisonnables pour déterminer que l'Importateur de données est à même de satisfaire à ses obligations au titre des BCR. L'Exportateur local de données et l'Importateur local de données accepteront de prendre les mesures nécessaires pour réparer les actes pour lesquels ils auront été reconnus responsables et verser une indemnité pour tout préjudice réel résultant de tels actes. L'Exportateur local de données et l'Importateur local de données disposent par conséquent chacun de ressources financières suffisantes pour couvrir le montant de l'indemnité due en cas de manquement aux BCR. La responsabilité entre les parties se limite au dommage effectif subi. Les dommages et intérêts indirects ou punitifs sont expressément exclus.
2. C'est à l'Exportateur local de données que revient la charge de prouver que l'entité SOPRA HR SOFTWARE établie en dehors de l'EEE n'est pas responsable de la violation ayant abouti à la demande de réparation de la Personne concernée.

C'est également à l'Exportateur local de données que revient la charge de prouver qu'il a entrepris des démarches raisonnables pour déterminer que l'Importateur local de données est à même de satisfaire à ces obligations au titre des BCR. L'Importateur local de données et l'Exportateur local de données peuvent être exonérées totalement ou partiellement de cette responsabilité si elles prouvent que le fait à l'origine du dommage ne leur est pas imputable ou que l'Exportateur local de données a entrepris des démarches raisonnables pour déterminer que l'Importateur

local de données est à même de satisfaire à ses obligations au titre des BCR.

3. En cas de violation avérée des BCR, le Responsable principal du traitement, le Responsable EMEA de la protection des données, le Responsable local du traitement ou le Responsable local de la protection des données devra prendre les mesures correctives (juridiques, techniques ou organisationnelles) et sanctions (à l'encontre du Responsable local du traitement ou, selon le droit du travail applicable au niveau local, un employé local) qu'il jugera appropriées.

5.4 VOIES DE RECOURS

1. Chaque Personne concernée est en droit de saisir, à sa convenance, l'autorité de contrôle dans l'État membre de sa résidence habituelle, de son lieu de travail ou du lieu où la violation aurait été commise (conformément à l'art. 77 RGPD) ou devant la juridiction compétente des États membres de l'UE (au choix de la personne concernée devant les juridictions où l'exportateur de données dispose d'un établissement ou celui dans lequel la personne concernée a sa résidence habituelle (article 79 RGPD),

en cas de manquement aux BCR.

2.

3. Conformément aux stipulations applicables de l'alinéa 5.3, chaque Personne concernée ayant subi des dommages peut prétendre à réparation (recours juridictionnels, par exemple) si le mécanisme interne de réclamation n'a pas permis de régler le litige (se reporter à l'alinéa 4.4), le cas échéant.

4. Les BCR doivent toujours être aisément accessibles par toutes les Personnes concernées, conformément aux stipulations de l'alinéa 4.1. En outre, les Personnes concernées doivent en toute occasion pouvoir obtenir, sur demande, une copie des BCR auprès du Responsable local de la protection des données, du Responsable local du traitement ou du Responsable EMEA de la protection des données.

5.5 SANCTIONS

Toute violation des BCR par un représentant ou un employé du Responsable local du traitement peut donner lieu à des sanctions disciplinaires ou à des poursuites judiciaires, conformément au droit du travail applicable, sur décision du Responsable du traitement principal, du Responsable EMEA de la protection des données, du Responsable local du traitement ou du Responsable local de la protection des données.

Par conséquent, le Responsable local du traitement et le Responsable local de la protection des données doivent prêter une attention particulière à tout résultat d'audit (se reporter à l'alinéa 4.7) laissant apparaître des problèmes de conformité concernant certains représentants ou employés, notamment les problèmes suivants :

- violation des Principes de protection des données énoncés à l'alinéa 2.2 et en Annexe 2 ;
- non-respect des lignes directrices ou procédures relatives à l'exercice des droits énoncées aux alinéas 4.1, 4.2 et 4.4 (droits d'information, d'accès, de rectification, d'effacement, de verrouillage, de réclamation interne, d'opposition, droit à la portabilité) ;

- violation des politiques de sécurité conçues en vue de la mise en œuvre de mesures techniques et d'organisation appropriées, destinées à protéger les Données à caractère personnel ;
- non-respect des obligations relatives aux programmes de formation destinés à sensibiliser les employés aux questions de Protection des données.

5.6 ENTRAIDE ET COOPÉRATION AVEC LES AUTORITÉS DE PROTECTION DES DONNÉES

Toutes les entités SOPRA HR SOFTWARE s'engagent à coopérer pleinement avec les autorités de protection des données compétentes au sein de l'EEE. Par conséquent :

- les Autorités de protection des données concernées doivent recevoir, sur demande, une copie actualisée des BCR et de l'ensemble des procédures, politiques ou lignes directrices y afférentes ;
- Le Responsable local du traitement est tenu de répondre dans un délai raisonnable à toute demande adressée par une Autorité de protection des données compétente, et notamment à toute demande d'audit.
- Le Responsable local du traitement est tenu de mettre en application les recommandations ou conseils émanant d'Autorités de protection des données compétentes et portants sur la mise en œuvre des BCR.
- Le Responsable local du traitement est tenu de respecter les décisions finales, contre lesquelles aucun recours n'est possible, émanant d'Autorités de protection des données compétentes et portants sur la mise en œuvre des BCR.
- Le Responsable EMEA de la protection des données doit se tenir à la disposition des Autorités de protection des données compétentes pour discuter de toute question liée à la mise en œuvre des BCR.

En outre, les entités SOPRA HR SOFTWARE doivent coopérer et s'entraider dans le cadre de la gestion des demandes ou des plaintes de particuliers (se reporter à l'alinéa 4.4) ou des demandes d'informations émanant d'Autorités de protection des données.

6. STIPULATIONS FINALES

6.1. LIENS ENTRE LA LÉGISLATION NATIONALE ET LES BCR

SOPRA HR SOFTWARE s'engage à faire en sorte que les entités et les employés concernés du groupe SOPRA HR SOFTWARE respectent les BCR ainsi que le Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 et le droit applicable au niveau local. Si la législation locale exige un degré supérieur de protection des Données à caractère personnel, celle-ci prime sur les BCR.

6.2. RESTRICTIONS AUX TRANSFERTS

AUX TRANSFERTS ULTÉRIEURS À DES RESPONSABLES DU TRAITEMENT ET À DES SOUS-TRAITANTS ULTERIEURS EXTERNES

Lorsqu'un Responsable local du traitement demande à une entité ne faisant pas partie du groupe SOPRA HR SOFTWARE de traiter des Données à caractère personnel, les garanties suivantes doivent être mises en place :

1. Les Sous-traitants externes établis dans l'EEE ou dans un pays reconnu par la Commission européenne comme garantissant un niveau adéquat de protection seront liés par contrat écrit stipulant que le Sous-traitant n'agit que sur seule instruction du responsable du traitement et est responsable de la mise en œuvre des mesures de sécurité et de confidentialité adéquates (se reporter à l'alinéa 4.5). Les Responsables locaux de la protection des données doivent pouvoir fournir, en coordination avec le Responsable EMEA de la protection des données, des clauses types adaptées aux Responsables locaux du traitement faisant partie du Groupe.
2. Tous les transferts de Données à caractère personnel à des Responsables externes du traitement établis en dehors de l'EEE doivent respecter les règles européennes relatives aux flux transfrontaliers de données, au moyen, par exemple, des Clauses contractuelles types approuvées par la Commission européenne.
3. Tous les transferts de Données à caractère personnel à des Sous-traitants externes établis en dehors de l'EEE doivent respecter les règles concernant les flux transfrontaliers de données, au moyen, par exemple, des Clauses contractuelles types approuvées par la Commission européenne, mais aussi les règles relatives aux Sous-traitants.

6.3. ACTIONS DANS LE CAS OU LA LÉGISLATION NATIONALE ENTRAVE LE RESPECT DES BCR

Lorsqu'un Responsable local du traitement a des raisons de croire que la législation qui lui est applicable risque de l'empêcher de remplir ses obligations en vertu des BCR et d'avoir un impact négatif sur les garanties fournies, ledit Responsable local du traitement est tenu d'en informer immédiatement le Responsable EMEA de la protection des données (à moins que cela ne soit interdit par une autorité chargée d'assurer le respect de la loi, comme, par exemple, une interdiction prévue par le code pénal pour préserver le secret de l'instruction).

En cas de conflit entre la législation nationale et les engagements en vertu des BCR, le Responsable local de la protection des données et le Responsable local du traitement, en coordination avec le Responsable EMEA de la protection des données, prendra une décision responsable sur l'action à entreprendre et, en cas de doute, consultera les Autorités de protection des données compétentes.

6.4. MISE À JOUR DES BCR

En cas de modification de la législation, par exemple, ou d'évolution des procédures de SOPRA HR SOFTWARE, les BCR peuvent être mises à jour à l'initiative du Responsable principal du traitement, en coordination avec le Responsable EMEA de la protection des données.

Toute modification substantielle ou non des BCR est consignée et conservée par le Responsable EMEA de la protection des données. Le Responsable EMEA de la protection des données tient également une liste complète et à jour des membres du Groupe. [1]

Toute modification substantielle ou non entraînera l'envoi à chaque entité SOPRA HR SOFTWARE d'une nouvelle version des BCR pour signature.

SOPRA HR SOFTWARE s'engage à informer une fois par an les Personnes concernées, les

Responsables locaux du traitement concernés et les Autorités de protection des données compétentes de toute modification substantielle apportée aux BCR.

Aucun transfert ne peut être effectué vers une nouvelle entité SOPRA HR SOFTWARE tant que celle-ci n'est pas véritablement liée par les BCR et tant qu'elle n'est pas en mesure de les respecter.

DÉROGATIONS PREVUES L'ARTICLE 49 DU REGLEMENT (UE) 2016/679 DU PARLEMENT EUROPEEN ET DU CONSEIL DU 27 AVRIL 2016

Conformément à l'article 49 du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 et au Droit local applicable, un Responsable local du traitement des données peut procéder à un transfert ou à un ensemble de transferts de Données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat, à condition que :

- la Personne concernée ait indubitablement donné son consentement au transfert envisagé ;
- le transfert soit nécessaire à l'exécution d'un contrat entre la Personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la Personne concernée ;
- le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la Personne concernée, entre le responsable du traitement et un tiers ;
- le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice ;
- le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la Personne concernée ;
- le transfert intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

6.5. DROIT APPLICABLE / VOIES DE RECOURS / RÉSILIATION / INTERPRÉTATION

Les BCR sont adoptées par le Responsable principal du traitement, en coordination avec le Responsable EMEA de la protection des données.

Les BCR prennent effet à la date à laquelle chaque entité SOPRA HR SOFTWARE les signe et devient, de ce fait, juridiquement liée par les BCR. Chaque entité SOPRA HR SOFTWARE reconnaît être liée par les BCR à compter de la date de signature de l'accord s'y rapportant et, sans qu'aucune autre formalité ne soit nécessaire, avec les autres entités SOPRA HR SOFTWARE déjà liées par les BCR ou s'apprêtant à le devenir suite à leur signature, quels que soient la date et le lieu de signature de la convention d'adhésion aux BCR par les autres entités SOPRA HR SOFTWARE concernées, et sous réserve que les stipulations des BCR signées par chaque entité soient strictement identiques. Les entités SOPRA HR SOFTWARE renoncent expressément et irrévocablement à leur droit de contester le fait qu'elles sont liées par les termes des BCR, sauf si elles sont en mesure de prouver que les BCR qu'elles ont signées ne sont pas strictement identiques aux BCR signées par d'autres entités.

En cas de manquement important ou persistant aux termes des BCR par un Responsable local du traitement, le Responsable principal du traitement peut temporairement

suspendre le transfert de Données à caractère personnel jusqu'à ce que le Responsable local du traitement y remédie. Si le Responsable local du traitement ne remédie pas au manquement dans les délais requis, le Responsable principal du traitement prendra l'initiative de résilier l'Accord relatif aux BCR.

Dans un tel cas, le Responsable local du traitement devra prendre toutes les mesures nécessaires pour se conformer aux règles européennes sur les flux de données transfrontaliers, en utilisant, par exemple, les Clauses contractuelles types approuvées par la Commission européenne.

Les stipulations des BCR sont régies par le droit de l'État membre de l'EEE dans lequel l'Exportateur local de données est situé.
Conformément aux alinéas 5.2 et 5.4, tout litige résultant des BCR relève de la compétence des tribunaux de l'Importateur local de données ou de l'Exportateur local de données.
Les BCR priment systématiquement sur les annexes en cas de conflit. Les BCR priment systématiquement sur les autres politiques, procédures ou lignes directrices applicables au niveau mondial ou local en cas de conflit ; en cas de conflit ou d'incohérence, les BCR sont toujours interprétées et régies par les dispositions du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016.

7. ANNEXES

Annexe 1 - Définitions
Annexe 2 - Principes de protection des données
Annexe 3 - Liste des entités SOPRA HR SOFTWARE liées par les BCR
Annexe 4 – Nature et finalités des données, types de traitements et types de personnes concernées
Annexe 5 – Accord contractuel

ANNEXE 1 : DÉFINITIONS

Les termes et expressions utilisés dans les BCR sont définis dans la présente Annexe et sont interprétés, en toutes circonstances, conformément au Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016.

« SOPRA HR SOFTWARE » désigne SOPRA HR SOFTWARE et/ou toute personne morale dont SOPRA HR SOFTWARE détient directement ou indirectement le contrôle, conformément aux dispositions de l'article L. 233-3 du Code de commerce.

« Responsable principal du traitement » désigne le siège de SOPRA HR SOFTWARE situé en France, qui détermine les finalités et les moyens du traitement de données à caractère personnel et qui est responsable de l'adoption formelle des BCR devant être mises en œuvre au sein de SOPRA HR SOFTWARE.

« Responsable local du traitement » désigne l'entité SOPRA HR SOFTWARE qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire.

« Exportateur local de données » désigne l'entité SOPRA HR SOFTWARE, située au sein de l'EEE, qui transfère les Données à caractère personnel en dehors de l'EEE.

« Importateur local de données » désigne l'entité SOPRA HR SOFTWARE, située en dehors de l'EEE, qui reçoit les Données à caractère personnel de l'Exportateur local de données en vue de leur traitement.

« Responsable local de la protection des données » désigne un cadre expérimenté de SOPRA HR SOFTWARE, travaillant pour un Responsable local du traitement, dont la fonction est de faire en sorte que les employés connaissent et respectent le Droit applicable à la protection des données et les politiques, procédures et lignes directrices de SOPRA HR SOFTWARE en la matière, et plus particulièrement les BCR.

« Responsable EMEA de la protection des données » désigne le cadre dirigeant chargé, au niveau du Groupe, de veiller à la connaissance et au respect par tous du Droit applicable à la protection des données et des politiques, procédures et lignes directrices de SOPRA HR SOFTWARE en la matière, et plus particulièrement des BCR.

« RGPD » désigne le Règlement (UE) 2016/679 du Parlement Européen et du Conseil 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

« Données à caractère personnel » : désigne toute information concernant une personne physique identifiée ou identifiable (« Personne concernée ») ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

« Traitement de données à caractère personnel » désigne toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données à

caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

« Sous-traitant » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des Données à caractère personnel pour le compte du responsable du traitement.

« Destinataire » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données, qu'il s'agisse ou non d'un tiers ; les autorités qui sont susceptibles de recevoir communication de données dans le cadre d'une mission d'enquête particulière ne sont toutefois pas considérées comme des Destinataires.

« Données sensibles » désigne les Données à caractère personnel révélant directement ou indirectement l'origine raciale ou ethnique d'une personne physique, ses opinions politiques, ses convictions philosophiques ou religieuses, son appartenance à un syndicat ou toute donnée relative à sa santé ou sa vie sexuelle.

« Tiers » désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la Personne concernée, le responsable du traitement, le Sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du Sous-traitant, sont habilitées à traiter les données.

« Consentement de la personne concernée » désigne toute manifestation de volonté, libre, spécifique et informée par laquelle la Personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

« Droit applicable à la protection des données » désigne 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 de l'EEE où l'Exportateur local de données est établi.

« Mesures techniques et d'organisation liées à la sécurité » désigne 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.

ANNEXE 2 : PRINCIPES DE PROTECTION DES DONNÉES

Dans le cadre des BCR, les transferts de Données à caractère personnel vers un pays tiers ne garantissant pas un niveau de protection adéquat doivent systématiquement être conformes aux principes de protection des données suivants, fixés par le Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016.

BASE JURIDIQUE DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Le traitement des Données à caractère personnel ne peut être effectué que si :

- la personne concernée a indubitablement donné son consentement ;
- le traitement est nécessaire à l'exécution d'un contrat auquel la Personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- le traitement est nécessaire à la sauvegarde de l'intérêt vital de la Personne concernée ;
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;

- le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la Personne concernée, qui appellent une protection.

BASE JURIDIQUE DU TRAITEMENT DES DONNÉES SENSIBLES

Le traitement des Données sensibles, et plus particulièrement des Données à caractère personnel relatives à la santé, ne peut être effectué que si :

- la Personne concernée a donné son consentement explicite au traitement des données sensibles en question, sauf dans les cas où la législation l'interdit ;
- le traitement est nécessaire aux fins du respect des obligations et droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates ;
- le traitement est nécessaire à la défense des intérêts vitaux de la Personne concernée ou d'une autre personne dans le cas où la Personne concernée serait dans l'incapacité physique ou juridique de donner son consentement ;
- le traitement est effectué par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale dans le cadre de leurs activités légitimes et avec des garanties appropriées, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers en rapport avec les objectifs poursuivis par celui-ci et que les données ne soient pas communiquées à des tiers sans le consentement des Personnes concernées ;

- le traitement porte sur des Données sensibles manifestement rendues publiques par la Personne concernée ;
- le traitement des Données sensibles est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- le traitement des Données sensibles est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé, dans la mesure où le traitement de ces données est effectué par un praticien de la santé soumis au secret professionnel en vertu du droit national ou de réglementations arrêtées par les autorités nationales compétentes, ou par une autre personne également soumise à une obligation de secret équivalente.

LIMITATION DES FINALITÉS

Les Données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. Un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible pour autant que les États membres prévoient des garanties appropriées.
Conformément aux dispositions du Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, seules les Données sensibles font l'objet de garanties supplémentaires.

QUALITÉ ET PROPORTIONNALITÉ DES DONNÉES

Les Données à caractère personnel doivent être traitées de manière licite et loyale.
Les Données à caractère personnel doivent être adéquates, pertinentes et leur volume ne doit pas être excessif au regard des finalités pour lesquelles elles sont transférées et traitées, exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées.
Les Données à caractère personnel doivent être conservées sous une forme permettant l'identification des Personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Les États membres prévoient des garanties appropriées pour les Données à caractère personnel qui sont conservées au-delà de la période précitée, à des fins historiques, statistiques ou scientifiques.

DÉCISION INDIVIDUELLE AUTOMATISÉE

Sous réserve du droit applicable au niveau local, toute Personne concernée a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, sa fiabilité, son comportement, etc.

ANNEXE 3 : LISTE DES FILIALES DE SOPRA HR SOFTWARE LIÉES PAR LES BCR.

1. Entités SOPRA HR SOFTWARE locales établies dans l'EEE

RESPONSABLE PRINCIPAL DU TRAITEMENT	**Sopra HR Software**
Forme	Société par Actions Simplifiée
Adresse	PAE Les Glaisins 74940 Annecy-le-Vieux France
N° de TVA intracommunautaire	FR61 519 319 651
Représentant légal	Edgard DAHDAH
Responsable groupe de la protection des	Eric Miroglio
Responsable local de la protection des données	Eric Miroglio

EUROPE

SOUS-TRAITANT LOCAL	**Sopra HR Software Limited**
Forme	Société à responsabilité limitée
Adresse	30 Old Broad Street London EC2M 1RX Royaume-Uni
Responsable local de la protection des données	Alan Brennan

SOUS-TRAITANT LOCAL	**Sopra HR Software SPRL**
Forme	Société privée à responsabilité limitée
Adresse	15-23 avenue Arnaud Fraiteurlaan 1050 Bruxelles Belgique
Responsable local de la protection des données	Julia Mateffi

SOUS-TRAITANT LOCAL	Sopra HR Software SARL
Forme	SARL
Adresse	8308 Capellen 89 E, Parc d'activités, Capellen Luxembourg
Responsable local de la protection des données	Julia Mateffi

SOUS-TRAITANT LOCAL	Sopra HR Software GmbH
Forme	GmbH
Adresse	Valoisplatz 2 26382 Wilhelmshaven Allemagne
Responsable local de la protection des données	Martin Junge

SOUS-TRAITANT LOCAL	Sopra HR Software SRL
Forme	SRL
Adresse	Assago, Strada Palazzo A7 4 cap 20090, frazione Milanofiori Italie
Responsable local de la protection des données	Pablo Roldan Jimenez

SOUS-TRAITANT LOCAL	Sopra HR Software , S.L.U
Forme	Société à responsabilité limitée
Adresse	Avenida de Manoteras 48 Planta 1 - Edificio B 28050 Madrid Espagne
Responsable local de la protection des données	Pablo Roldan Jimenez

Entités SOPRA HR Software locales établies en dehors de l'EEE

SOUS-TRAITANT LOCAL	Sopra HR Software SaRL
Forme	Société à responsabilité limitée
Adresse	18 avenue Louis Casai 1209 Genève Suisse
Responsable local de la protection des données	Eric Miroglio

AFRIQUE

SOUS-TRAITANT LOCAL	Sopra HR Software SARL
Forme	SARL à associé unique
Adresse	92, bd Anfa, Etage 6 20100 Casablanca Maroc
Responsable local de la protection des données	Zied Mokni

SOUS-TRAITANT LOCAL	Sopra HR Software SARL
Forme	SARL société à responsabilité limitée
Adresse	Immeuble Tunimara Rue du Lac Constance 1053 Les Berges du Lac Tunisie
Responsable local de la protection des données	Zied Mokni

ANNEXE 4 : NATURE, FINALITÉS DES DONNÉES, TYPES DE TRAITEMENTS ET TYPES DE PERSONNES CONCERNEES

Types de traitement et ses finalités	Nature et catégorie des données transférées
La gestion de la relation clients, prospects, partenaires et fournisseurs, incluant : la fourniture et la facturation des produits et services achetés ; le traitement des paiements électroniques ; le traitement des échanges électroniques de documents (ex : les appels d'offres publics dématérialisés) ; la fourniture aux clients d'un service plus personnalisé ; la fourniture d'un accès aux services Sopra HR Software (ex : système de support technique) et aux applications et environnements du client ; la conduite d'études de marché, d'enquêtes de satisfaction et de contrôle qualité ; la prospection commerciale et la promotion des ventes ; la réponse à toute demande du client (information, réclamation, etc.) ; l'organisation d'évènements spéciaux pour les clients ; la gestion et le paiement des fournisseurs ; l'administration globale de la tenue des dossiers.	informations de contact (nom, sexe, adresse, société, fonction, date et lieu de naissance, e-mail, etc.) ; produits ou services achetés, lieu d'achat, demandes spéciales, remarques concernant les préférences en matière de service, etc.) ; informations de facturation (nombre de ventes, coordonnées bancaires, etc.) ; informations relatives aux préférences commerciales ou informations communiquées dans le cadre d'enquêtes ou d'offres promotionnelles.

Types de traitement et ses finalités	Nature et catégorie des données transférées
La gestion des ressources humaines, incluant : la gestion de la paie ; la gestion administrative ; la gestion des carrières et de la mobilité ; l'organisation du travail ; la formation des salariés ; la gestion des outils informatiques et de communication mis à la disposition des salariés ; le contrôle d'accès aux locaux et la vidéosurveillance ; la gestion des données des salariés pour les déplacements ; la gestion des organigrammes et des annuaires des salariés ; la gestion des assurances santé et de retraite.	données d'identification (ID entreprise, nom, sexe, lieu et date de naissance, nationalité, coordonnées professionnelles, coordonnées personnelles, numéro interne, numéro d'urgence, coordonnées bancaires, données économiques destinées à la gestion de la paie, déplacements et frais, impôts, etc.) ; coordonnées de contact professionnelles (numéro de téléphone professionnel, adresse e-mail, etc.) ; informations relative à la carrière des employés (date et conditions d'embauche, modification de statut, simulation et développement de carrière, sanctions disciplinaires, évaluation professionnelle, formations suivies, historique des évaluations de la performance, évaluation des connaissances, etc.) ; informations relatives aux déplacements (informations figurant sur le passeport) ; informations sur les congés ; Photos Informations sur la famille (identification des enfants et conjoints) ; Pour les plans de retraite, informations sur les bénéficiaires (s'il ne s'agit pas des bénéficiaires légaux).

Conformément au champ matériel et à la description des transferts couverts par les BCR «responsable de traitement» du groupe Sopra HR Software et à leurs annexes, peuvent être transférées, dans le cadre des finalités décrites ci-dessus, les données à caractère personnel relatives aux catégories de personnes suivantes :

– salariés et assimilés (anciens salariés, candidats, stagiaires et intérimaires)
– clients (actuels ou potentiels)
– partenaires
– fournisseurs.