Mise en œuvre du RGPD

49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com
Société par actions simplifiée au capital de 1 100 000 euros - 305 163 040 RCS Lyon - Siret 305 163 040 00119 - Code APE 6202A - N° TVA intra FR28 305 163 040

Suite à l'entrée en vigueur de nouvelles règlementations en matière de protection des données à caractère personnel, Ciril GROUP met à la disposition de ses clients ce document détaillant les différentes mesures de sécurité mises en place par notre société dans le cadre de l'exécution de ses prestations. Ces mesures de sécurités seront présentées sous quatre angles :

- **Les mesures de sécurité physique (Chapitre 1)** : Rien ne sert de déployer des mesures de sécurité informatiques et organisationnelles poussées si les locaux où les prestations sont réalisées ne sont pas eux-mêmes sécurisés. A défaut de mesures de sécurité adéquates, une effraction ou un vol sont des risques réels. C'est pour cette raison que la société Ciril GROUP met un point d'honneur à sécuriser ses établissements ;

- **Les mesures de sécurité organisationnelles (Chapitre 2)** : Souvent oublié en matière de sécurité, le facteur humain est pourtant l'une des principales menaces pesant sur les systèmes d'information. Consciente de ces risques, la société Ciril GROUP a développé plusieurs stratégies pour les réduire ;

- **Les mesures de sécurité logiques (Chapitre 3)** : Ce n'est un secret pour personne, la sécurité des systèmes d'information est au cœur de la défense des intérêts des entreprises. La maturité de Ciril GROUP, œuvrant dans ce domaine depuis sa fondation en 1978, lui a permis au fur et à mesure des années de mettre en place des infrastructures de plus en plus sécurisées ;

- **Les mesures de sécurité fonctionnelles (Chapitre 4)** : Car la sécurité n'est pas que technique mais aussi juridique, nos solutions proposent des fonctionnalités directement conçues afin de faciliter la conformité de nos clients aux différentes règlementations.

Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

Sommaire

Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

Chapitre 1
Les mesures physiques mises en place

A/ Localisation des sites

Les équipes de CIRIL GROUP sont réparties sur 8 sites en France :

- Lille ;
- Paris (9ème);
- Paris (12ème) ;
- Rennes ;
- La Roche-Sur-Yon ;
- Villeurbanne ;
- Meylan ;
- Aix-En-Provence.

La répartition territoriale des sites permet d'assurer qu'en cas d'incident dans l'un d'eux, les autres peuvent prendre le relai. De plus, le choix délibéré de n'avoir des équipes de maintenance et d'assistance de Ciril GROUP qu'en France évite de ce point de vue tout risque de transfert de données en dehors de l'Union Européenne, que ce soit dans nos activités de maintenance, d'assistance ou d'hébergement. En effet, nos data-centers sont eux aussi exclusivement situés sur le sol français, à Villeurbanne et à Paris. Enfin, les systèmes informatiques de la filiale canadienne de Ciril GROUP « CIRIL GEO TECHNOLOGIES » ont été pensés dès leur conception dans une démarche de privacy by design et, à ce titre, aucune donnée personnelle traitée par Ciril GROUP ne lui est transférée.

B/ Sécurité des locaux

Nos locaux sont sécurisés et protégés par des dispositifs d'alarme et de télésurveillance. De plus, les locaux de nos data-centers (Villeurbanne et Paris) sont certifiés ISO-27001 et répondent donc aux exigences de sécurité physiques imposées par ce référentiel. Nous sommes également certifiés APSAD, certification attestant la qualité de nos systèmes anti-incendie, de détection d'intrusion et de télésurveillance. En

Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

particuliers, des périmètres de sécurité ont été définis pour protéger les zones de ces sites où sont traitées des informations sensibles ou critiques, il est nécessaire d'être doté d'un badge délivré par notre DSI après demande écrite pour y accéder et plusieurs mécanismes d'authentification différents sont nécessaires pour pénétrer dans les data-centers. Enfin, ces locaux sont protégés par des agents de sécurité de jour comme de nuit.

Pour des raisons évidentes de sécurité, ce document ne reprend pas de manière exhaustive et précise les mesures de sécurité mises en œuvre dans nos locaux. Des informations supplémentaires peuvent vous être communiquées sur demande motivée, sous réserve d'une consultation sur site et de la signature d'un accord de confidentialité.

C/ Redondance des infrastructures

Afin de garantir la meilleure résilience de nos systèmes informatiques et des infrastructures hébergées dans nos data-centers par nos clients, nos équipements sont entièrement redondés, de nos installations électriques (elles-mêmes secondées par notre groupe électrogène) aux fibres de connexion entre nos sites d'hébergement.

Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

Chapitre 2
Les mesures organisationnelles mises en place

A/ Rappel des règles éthiques et déontologiques

L'ensemble du personnel de Ciril GROUP est astreint à une obligation de confidentialité. De plus, le personnel de Ciril GROUP qui pourrait être amené à traiter des données pour le compte de nos clients dans le cadre d'opérations de maintenance ou d'assistance est soumis à une charte de déontologie lui interdisant de traiter les données autrement que dans la finalité définie par nos clients.

Cette charte de déontologie rappelle également qu'il est interdit de faire des copies de ces données autrement que pour l'exécution des prestations commandées, de communiquer ces données à d'autres personnes du personnel de Ciril GROUP n'appartenant pas aux services soumis à la charte, de réutiliser les données une fois l'opération de maintenance terminée et impose que les données soient supprimées à l'issue des prestations commandées par nos clients.

B/ Procédures rigoureuses

Nos procédures mises en place afin d'assurer une plus grande sécurité des données lors de l'exécution de nos prestations s'entendent tant lors de l'exécution de celles-ci qu'en amont et en aval.

Tout d'abord, lors de l'exécution de nos prestations, seul le personnel habilité de Ciril GROUP a accès aux interfaces de gestion des demandes de nos clients. Nos procédures internes nous permettent également de suivre le déroulement des prestations et les différentes actions effectuées lors de celles-ci.

A l'issue de ces prestations, un procès-verbal de suppression des données est effectué si nécessaire.

De plus, le personnel de Ciril GROUP amené à traiter les données les plus sensibles est recruté selon une procédure particulière respectant là aussi les exigences de la norme ISO-27001.

C/ Sensibilisation

Car nous considérons que la meilleure manière d'intégrer la protection des données à nos solutions est de diffuser directement la culture « Informatique et Libertés » au sein de notre société, des actions de sensibilisation à la protection des données et à la sécurité informatique sont également menées

Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

respectivement par le Délégué à la Protection des Données et par le Responsable de la Sécurité des Systèmes d'Information de Ciril GROUP.

D/ Analyses de risques

Conformément à la règlementation en matière de protection des données, nous effectuons des études d'impact sur la vie privée pour chacun de nos traitements lorsque cela s'avère nécessaire.

Surtout, au-delà de ces études d'impacts, des analyses de risques en matière de sécurité des systèmes d'information sont réalisées périodiquement par nos équipes. Ces analyses de risques sont effectuées selon la méthode EBIOS mise au point par l'ANSSI et selon la méthode de l'ISO 27002.

En complément, des tests d'intrusions sont réalisés tant sur nos infrastructures d'hébergement que sur nos applications.

E/ Procédures de gestion de crise

Afin de parer à tout incident dans les meilleurs délais, plusieurs cellules de crises ont été créées dans notre société, chacune ayant un périmètre précis d'intervention, qu'il s'agisse de problèmes affectant nos solutions d'hébergement, nos solutions SIG ou nos solutions Civil. Les équipes composant ces cellules ont été élaborées afin de réunir les compétences nécessaires pour répondre à toute sorte de difficulté. Des équipes suppléantes ont également été créées pour pouvoir réagir à ces évènements plus efficacement encore.

En pareilles circonstances, la communication auprès de nos clients est primordiale. Ainsi, en parallèle de la cellule de résolution d'incident, une équipe de communication est réunie afin de les tenir informer en temps réel de l'avancée de la résolution du problème. Le Délégué à la Protection des Données de Ciril GROUP fait notamment partie de cette équipe afin de veiller à la transmission à nos clients des informations nécessaires en cas de violation de données personnelles.

F/ Documentation de la sécurité

L'ensemble des mesures et des procédures de sécurité appliquées par notre société dans le cadre de sa certification ISO 27001 est rigoureusement documenté. Cette documentation étant, pour des raisons évidentes, hautement confidentielle, sa consultation n'est possible qu'au siège de notre société et après signature d'un accord de confidentialité.

De plus, chaque trimestre, un comité de pilotage de la sécurité et du management des systèmes d'information (SMSI) est organisé au sein de notre société afin d'effectuer un suivi des règles de sécurité internes, des audits, des potentielles évolutions de notre PSSI ainsi que pour revenir sur les différents tests

Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

d'application effectués. En effet, des tests réguliers de nos infrastructures ont lieu afin d'en vérifier la fiabilité et la sécurité. Un rapport est rédigé à l'issue de chacun de ces comités.

Dans une autre mesure mais toujours au titre de cette documentation et en cas d'incident ou de faille de sécurité, des rapports sur ceux-ci sont également établis à leurs termes, et ce dans une démarche d'amélioration continue. Ces rapports permettent de mettre en avant les mesures correctives à mettre en œuvre.

Enfin, conformément à la législation relative à la protection des données, la société Ciril GROUP tient à jour un registre des traitements de données qu'elle effectue pour le compte de ses clients. Il est d'ailleurs rappelé à ces derniers qu'ils peuvent également être tenus d'élaborer leur propre registre. Un modèle de fiche de registre est à ce titre disponible sur le site internet de la Commission Nationale de l'Informatique et des Libertés. Les fiches des registres des clients de Ciril GROUP leur sont propres et doivent donc être réalisées par ces derniers. Les informations du présent document peuvent y être reprises si besoin et, pour tout renseignement complémentaire, les clients de Ciril GROUP ont la possibilité de contacter le dpo de Ciril GROUP à l'adresse dpo@cirilgroup.com.

G/ Audits, certification et agrément

Dans le cadre de notre certification ISO 27001, des audits sont menés chaque année par des auditeurs indépendants eux-mêmes certifiés. Ces audits de sécurité sont complétés par des audits internes menés régulièrement sur des thématiques précises et tenant autant à la sécurité technique des systèmes qu'à la conformité juridique des traitements de données opérés par notre société.

La certification ISO 27001 de notre société a pour périmètre la fourniture d'infrastructures techniques, informatiques et réseaux permettant l'hébergement d'applications ou services contenant des données sensibles et/ou personnelles fournies par nos clients.

De plus, notre société est agréée « HADS » par le ministère de la santé pour héberger des données de santé à caractère personnel.

Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

Chapitre 3
Les mesures logiques mises en place

A/ En matière d'hébergement

Evidemment, tous nos systèmes sont protégés par un pare-feu et par antivirus. Pour un maximum de sécurité notre pare-feu est un pare-feu physique qui est redondé sur nos différents sites. Le pare-feu que nous exploitons a en plus été recommandé par le NSS Lab et la gamme de produits que nous utilisons a reçu la certification EAL4.

En complément, une supervision de nos infrastructures en temps réel est réalisée, ce qui permet à nos équipes de pouvoir constamment veiller à leur stabilité. A ce titre, des équipes d'astreinte assurent leur surveillance de jour comme de nuit.

Un système de cloisonnement de notre réseau par VLAN garantit également la segmentation et l'imperméabilité des différentes plateformes mises à la disposition de nos clients.

Enfin, nous fournissons des prestations de sauvegarde et de PRA. Les bases de données de nos clients en SaaS bénéficient à ce titre d'une sauvegarde totale hebdomadaire et d'une sauvegarde incrémentale quotidienne. La durée de rétention de ces sauvegardes peut varier selon les demandes de nos clients.

B/ En matière de maintenance et d'assistance

Les prestations de maintenance et d'assistance que notre société peut être amenée à effectuer pour nos clients sont très variées. Toutefois, elles peuvent être classées en deux catégories : celles entrainant des transferts de données et celles n'en entrainant pas.

Les téléassistances ou la hotline n'entrainent pas de transfert de données dans nos infrastructures. Tout au plus, notre personnel pourra être amené à consulter certaines données ou à interagir à distance avec ces dernières. Afin que ceci se fasse en toute sécurité, notre personnel est soumis à une charte de déontologie et à une obligation de confidentialité. De plus, le logiciel que nous utilisons pour effectuer ces prestations à distance permet un chiffrement de bout en bout de toutes les transmissions et une parfaite visibilité de nos clients sur les prestations. Chacune des opérations de prise en main à distance effectuées par ce biais nécessitent également une autorisation du client concerné.

En cas de transfert, et notamment en cas d'intégration de bases de données, nous mettons à disposition de nos clients un espace de stockage sécurisé afin qu'ils puissent y déposer leurs données. Nos clients ont la

Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

possibilité de chiffrer ces données avant dépôt, ce qui est très fortement recommandé. Le même procédé est employé pour la restitution de ces données.

C/ En matière d'infogérance

Dans le cas où nos clients n'hébergent pas leurs solutions dans nos infrastructures, ceux-ci doivent eux-mêmes réaliser l'infogérance de leurs serveurs. Il est rappelé que les solutions alors hébergées par les clients peuvent être amenées à contenir des données à caractère personnel et doivent donc être sécurisées par des mesures adéquates. A ce titre, une attention particulière doit être portée par les clients à la sécurité des infrastructures de stockage ainsi qu'à l'infogérance et à la maintenance des serveurs sur lesquels les solutions sont installées afin de garantir la sécurité et la confidentialité desdites données.

En revanche, en hébergeant leurs solutions dans nos infrastructures, les clients bénéficient du haut niveau de sécurité (tant physique que logique), de résilience et de disponibilité de notre Datacenter certifié ISO 27001. Ces clients sont également assurés qu'aucun transfert de données hors Union Européenne n'a lieu puisque toutes nos infrastructures sont situées en France, à Lyon pour notre site principal et à Paris pour notre site de secours. Le client n'a ainsi pas à prévoir l'encadrement légal de ces transferts et peut avancer notre certification comme preuve de sécurité aux termes de la législation relative à la protection des données.

Nos prestations d'infogérance sont elles aussi réalisées dans ce cadre sécurisé et bénéficient des mêmes garanties de sécurité.

Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

Chapitre 4
Les mesures fonctionnelles mises en place

En tant qu'éditeur de logiciel, et à moins d'héberger les solutions que nous fournissons à nos clients ou d'effectuer des opérations de maintenance et d'assistance, nous ne sommes pas sous-traitants des traitements de données effectués par les utilisateurs de celles-ci. Toutefois, afin de permettre à nos clients de respecter leurs obligations en matière de protection des données, les dernières versions de nos logiciels ont été pourvues de nouvelles fonctionnalités. Ces fonctionnalités, conçues dans une optique de Privacy by Design et by Default, s'articulent autour de deux axes : l'identification et la traçabilité des données sensibles ; l'information et la prise en compte des droits des personnes.

A/ Identification et traçabilité des données sensibles

Les données « sensibles » représentent des données personnelles que les clients souhaitent journaliser lors des actions de création, de modification et de suppression. Il peut également s'agir de données particulières que les clients souhaitent journaliser.

Du fait de la diversité des informations pouvant être intégrées à GEO par ses utilisateurs et ses administrateurs, ces derniers ont la possibilité d'identifier chacune d'elles en tant que « donnée sensible ».

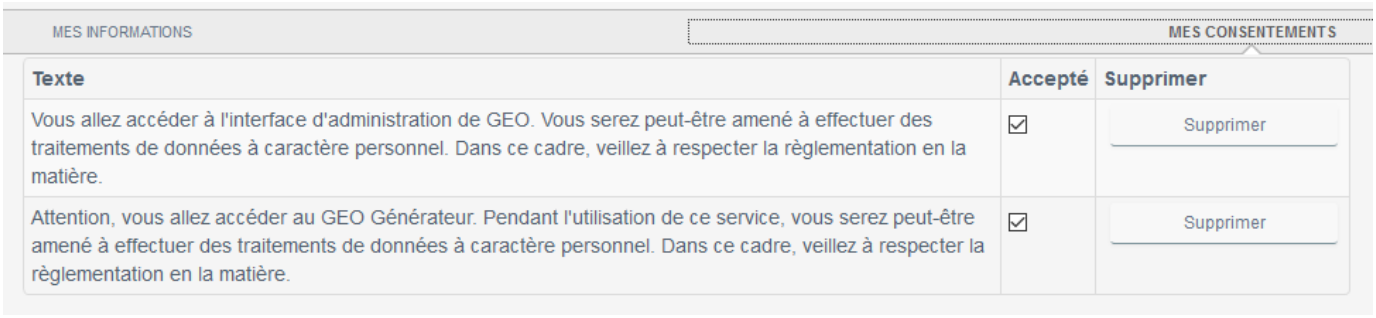
Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

En on premise (qu'il s'agisse de on premise installé directement chez les clients ou de on premise « hébergé ») une fois les données sensibles identifiées, les actions à journaliser sur celles-ci peuvent être librement définies par l'administrateur de la solution. Ces actions à journaliser peuvent être la création, la modification, la suppression et la consultation de la donnée. L'administrateur peut également choisir le fichier de destination de ces journaux (et peut notamment choisir de les intégrer à un concentrateur de logs), leur durée de rétention et leur taille maximum.

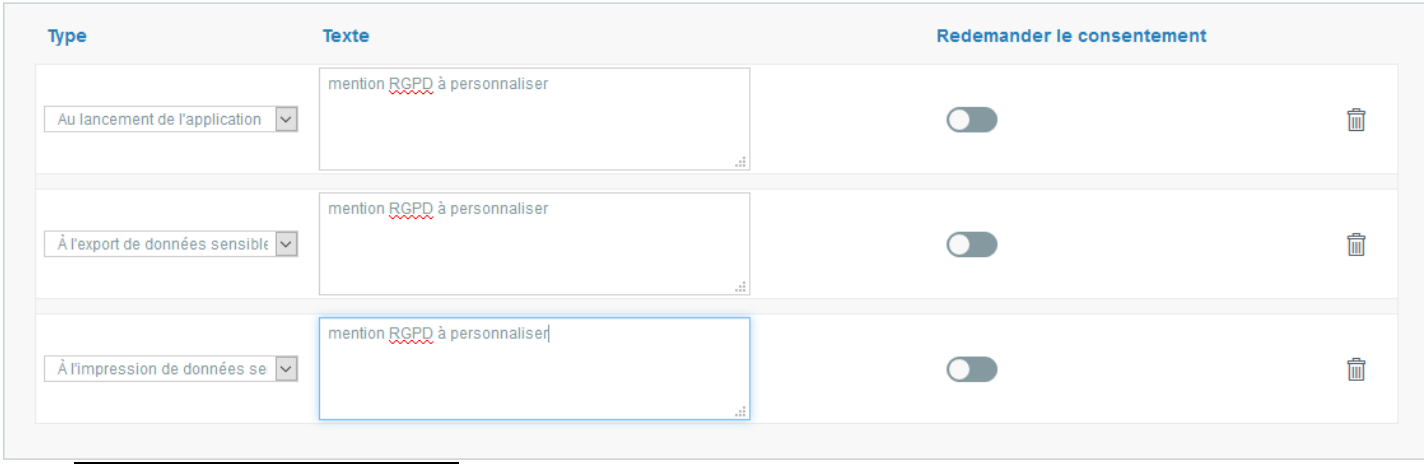
Dans le cas où la solution GEO est utilisée en SaaS, si l'administrateur choisit d'activer la journalisation, les journaux des actions sur les données désignées comme « sensibles » par ce dernier sont conservés dans le concentrateur de logs de Ciril GROUP, conformément aux préconisations de la Commission Nationale de l'Informatique et des Libertés sur le sujet[1], six mois.

B/ Information et prise en compte des droits des personnes

L'information des personnes est effectuée par l'affichage de mentions lors de la connexion à l'application ou au cours de la navigation. Ces mentions peuvent être accompagnées d'une question à la personne permettant de recueillir son consentement ou une confirmation de lecture. La réponse à cette question est journalisée, et les personnes concernées peuvent revenir à tout moment sur le consentement qu'ils ont donné à un traitement directement dans leur profil.



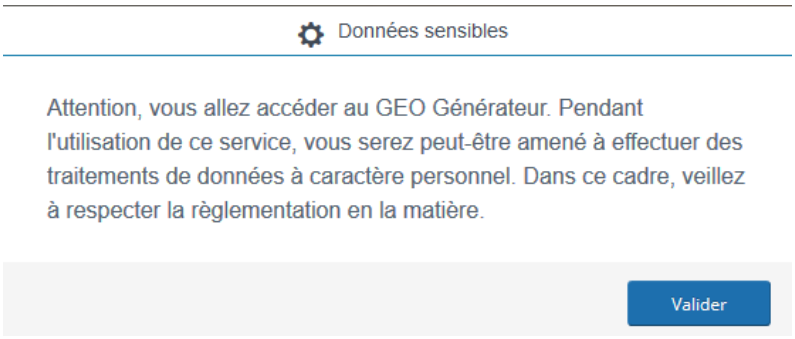
Ces mentions sont entièrement configurables par les administrateurs de la solution et, dans le cas où elles devraient être modifiées, il est possible pour ces derniers de demander aux personnes concernées de renouveler leur consentement ou leur acceptation.



[1] https://www.cnil.fr/fr/securite-tracer-les-acces-et-gerer-les-incidents

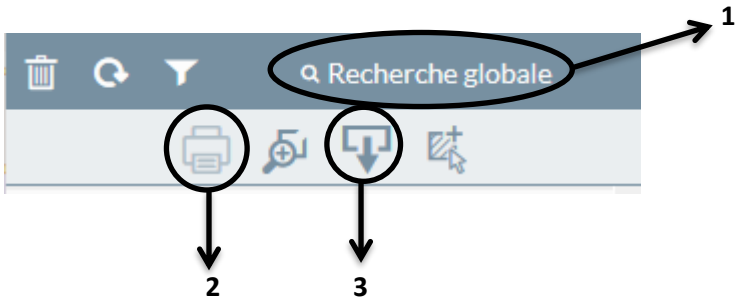
Ciril GROUP SAS - 49 avenue Albert Einstein - BP 12074 - 69603 Villeurbanne CEDEX - France - T. +33 (0)4 72 69 16 80 - F. +33 (0)4 78 93 85 00 - contact@cirilgroup.com - www.cirilgroup.com

A toute fin utile, une mention est également affichée lors du premier démarrage de la solution afin de rappeler aux administrateurs qu'ils sont susceptibles de traiter des données personnelles dans l'application et qu'ils doivent à ce titre veiller au respect de la législation en la matière.



Afin de vérifier la cohérence du positionnement des mentions et des données identifiées comme sensibles, le client a la possibilité d'activer une fonctionnalité « Vérifier la cohérence RGPD » afin de vérifier que l'accès aux données sensibles ou à certaines fonctionnalités ne soit possible qu'après lecture d'une mention d'information ou après recueil du consentement.

En matière de respect des droits des personnes et afin de pouvoir répondre le plus rapidement et le plus efficacement possible aux demandes d'exercice de droits des personnes, les administrateurs de la solution GEO ont la possibilité d'utiliser la fonctionnalité standard de recherche.



Cette fonctionnalité de recherche (1) permet d'interroger les données intégrées à la solution GEO. Les résultats de ces recherches peuvent être directement imprimés (2) ou exportés (3) sous différents formats. Il est également possible, à partir de ces résultats de recherche, d'imprimer ou d'exporter les fiches donnant le détail des données interrogées. Une intervention dans les bases de données permet quant à elle de supprimer les données en question en cas de demande de suppression.

Remarque : La mise en place du protocole https est fortement recommandée. Celle-ci peut être effectuée directement par les clients de Ciril GROUP ou par Business Geografic sur devis. Pour toute information sur ces points, n'hésitez pas à nous contacter. Nos équipes se tiennent à votre disposition pour tout renseignement complémentaire.

Ciril GROUP

49 avenue Albert Einstein - BP 12074
69603 Villeurbanne CEDEX - France

Tél : +33 (0)4 72 69 16 80
Fax : +33 (0)4 78 93 85 00
contact@business-geografic.com