

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

1. Introduction

1.1 Contexte du Règlement Général sur la Protection de Données (« RGPD »)

Le Règlement Général sur la Protection de Données édicté en avril 2016 remplace la Directive de Protection de Données de l'Union européenne de 1995 et remplace les lois des États membres qui ont été élaborées conformément à la Directive sur la Protection des Données 95/46/CE.

Son but est :

- d'établir des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données ;
- de protéger les libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel ;
- de permettre la libre circulation des données à caractère personnel au sein de l'Union, ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

1.2 Champ d'application

Le champ d'application matériel

Le RGPD s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Le champ d'application territorial

Le RGPD s'applique :

- au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union ;

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

- au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.
- au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.

1.3 Définitions utilisées par R2

Données à caractère personnel

Toute information relative à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

Catégories particulières de données à caractère personnel dites données sensibles

Données personnelles révélant l'origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, l'appartenance syndicale, traitement de données génétiques, données biométriques dans le but d'identifier de manière unique une personne physique, données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Traitement

Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, R2, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

Responsable de traitement

Personne physique ou morale, autorité publique, agence ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens d'un tel traitement sont déterminés par le droit de l'Union ou de l'État membre, le responsable du traitement ou les critères spécifiques de sa nomination peuvent être prévus par la législation de l'Union ou des États membres.

Sous-traitant

La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Établissement principal

L'établissement principal dans l'UE sera :

- en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal;
- en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent règlement.

Fichier

Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

Violation de données personnelle –

Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte,

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données

Consentement de la personne concernée -

Désigne toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

2. Déclaration de politique

La direction de R2, située 19 rue de Sèvres 750006 Paris s'engage à respecter son obligation de conformité avec le règlement de l'UE les lois de l'État Français ; en ce qui concerne les données personnelles et la protection "des droits et des libertés" de toute personne concernée que l'entreprise recueille et traite conformément au Règlement Général de Protection de Données (RGPD).

La conformité avec le RGPD est décrite par cette politique et d'autres politiques appropriées comme la charte informatique (**RGPD-8.1**), ainsi que des processus et procédures connexes.

Le RGPD et cette politique s'appliquent à toutes les fonctions de traitement des données personnelles de l'entreprise, y compris celles effectuées sur les données personnelles de ses clients, salariés, fournisseurs et partenaires et toutes autres données personnelles traitées par R2.

Le responsable du traitement avec l'aide du Délégué à la Protection des Données (DPD / DPO) est responsable et doit vérifier le registre de chaque traitement en fonction des changements apportés aux activités de l'Entreprise (telles que déterminées par des changements au registre des données, d'inventaire de données et examen de gestion) et aux exigences supplémentaires identifiées au moyen des analyses d'impact sur la protection de données. Ce registre doit être disponible à la moindre requête de l'autorité européenne de contrôle ou de la CNIL.

Cette politique s'applique à tous les employés / membres du personnel / prestataires de R2, y compris les fournisseurs externalisés.

Les partenaires et les tiers collaborant avec R2 ou pour son compte, et qui ont ou peuvent avoir accès aux données personnelles, devront respecter cette politique, pour en avoir été préalablement informés et avertis en l'ayant lue, comprise et approuvée. Aucun tiers ne peut avoir accès aux

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

données personnelles détenues par R2 sans avoir signé au préalable un engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel (**RGPD-5.3**) ou une clause contractuelle (**RGPD-5.2**), qui impose aux tiers des obligations équivalentes à celles auxquelles R2 s'est engagée et qui lui donne un droit légitime de vérifier leur conformité au regard de l'accord auquel les tiers se sont soumis.

3. Rôles et responsabilités

3.1 En tant que Responsable de traitement

R2 est un responsable de traitement conformément au RGPD.

La direction générale et les cadres managériaux exerçant dans l'entreprise sont responsables du développement des bonnes pratiques de traitement d'informations au sein de R2; les responsabilités sont exposées dans chaque description de poste individuel.

Le Délégué à la Protection des Données (DPD / DPO) dont les missions sont exposées dans le document missions du DPO (**RGPD-2.1**), a un rôle spécifique indiqué dans le RGPD, et il doit rendre compte à la direction de R2 de la gestion des données personnelles afin de s'assurer de la conformité de l'entreprise avec le RGPD de telle sorte que son obligation de moyen liée à sa mise en conformité et à sa bonne pratique puisse être démontrées.

Le DPO, choisi par la direction de R2 selon sa qualification et son expérience, a été nommé pour s'assurer de la conformité de l'entreprise avec le RGPD et particulièrement rendre compte à la direction de l'entreprise du respect du RGPD. Sa désignation est consignée dans le document désignation du DPO (**RGPD-2.2**)

Le responsable du traitement et le DPO ont des responsabilités spécifiques en ce qui concerne certaines procédures comme la procédure de demande d'exercice des droits d'une personne concernée (**RGPD-7.1**), ouverte à tout Salarié/Personnel souhaitant une clarification sur n'importe quel aspect de la conformité de la protection de ses données.

Le respect du RGPD concerne tous les salariés/ membres du personnel de R2 qui traitent des données personnelles.

La politique de formation au RGPD de l'entreprise (**RGPD-3.1**) définit des exigences de formation

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

spécifique et de sensibilisation au regard des rôles spécifiques de chacun des Salariés/Membre du personnel de R2.

Les salariés/personnel de R2 sont responsables et doivent s'assurer que toutes données personnelles les concernant ou fournies par eux au nom de l'entreprise soient exactes et à jour.

3.2 En tant que sous-traitant

R2 est un sous-traitant agissant pour le compte de Responsables de traitement.

R2 s'engage à traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/ont l'objet de la sous-traitance

R2 traite les données conformément aux instructions documentées du responsable de traitement figurant sur le contrat (ou en annexe de celui-ci) avec ledit responsable de traitement. Si R2 considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable de traitement. En outre, si R2 est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public

R2 s'engage à garantir la confidentialité des données à caractère personnel traitées et à veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité

R2 s'engage à veiller à ce que les personnes autorisées à traiter les données à caractère personnel reçoivent la formation nécessaire en matière de protection des données à caractère personnel

R2 s'engage à prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut

En cas de recrutement d'autres sous-traitants ultérieurs, R2 doit recueillir l'autorisation écrite, préalable et spécifique ou générale du responsable de traitement (**RGPD-5.4**). R2 s'assure que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

exigences du règlement européen sur la protection des données. En outre, le sous-traitant ultérieur est tenu de respecter les instructions du responsable de traitement.

Sauf indications contractuelles, il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

R2 aide le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées: droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage) selon les indications contractuelles.

R2 notifie au responsable de traitement toute violation de données à caractère personnel selon les indications contractuelles.

R2 aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données. R2 aide également le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

Au terme de la prestation de services relatifs au traitement de ces données, R2 s'engage à : selon les indications contractuelles :

- détruire toutes les données à caractère personnel ou
- à renvoyer toutes les données à caractère personnel au responsable de traitement ou
- à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

R2 communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

R2 tient par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement

R2 met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

4. Principes de protection de données

Tout traitement de données à caractère personnel doit être effectué conformément aux principes de protection de données comme exposés dans l'Article 5 du RGPD. Les politiques et les procédures de l'entreprise sont conçues pour assurer le respect de ces principes.

4.1 Les données personnelles doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence)

Licéité - Identifier une base légale avant de pouvoir traiter des données personnelles. Celles-ci sont souvent mentionnées en tant que " conditions de traitement" (par exemple, le consentement).

Loyauté - Le traitement doit être loyal. A cette fin, le responsable du traitement doit mettre dans la mesure du possible certaines informations à disposition des personnes concernées. Ceci s'applique que les données personnelles aient été obtenues directement de la part la personne concernée ou d'autres sources.

Le RGPD a augmenté le niveau d'exigences afin que les informations mises à la disposition des personnes concernées soient couvertes par une exigence de Transparence.

Transparence - D'une manière transparente - le RGPD inclut des règles sur la communication des informations confidentielles relatives à la vie privée des personnes concernées aux articles 12, 13 et 14. Ceux-ci sont détaillés et spécifiques, soulignant la manière dont doivent être rendues les données à caractère personnel, c'est à dire compréhensible et accessible. Les informations doivent être communiquées aux personnes concernées dans une forme intelligible et dans la langue qu'elles comprennent de manière simple et claire.

La procédure d'information des personnes concernées (**RGPD-6.1**) et de demande d'exercice des droits des personnes concernées (**RGPD-7.1**) sont définies et documentées.

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

Les informations spécifiques à fournir à la personne concernée, doivent inclure a minima :

- L'identité et les coordonnées du responsable de traitement et, le cas échéant, du représentant du responsable de traitement;
- Les coordonnées du Délégué à la Protection des Données (DPD / DPO);
- Les finalités du traitement pour lequel les données personnelles recueillies sont destinées sur le fondement d'une base légale du traitement qui doit aussi être renseignée;
- La période pendant laquelle les données personnelles seront stockées;
- L'existence du droit d'accès, de rectification, d'effacement ou d'élever une objection au traitement et les conditions (ou l'absence) d'exercice de ces droits, même si la légalité de traitement précédent en est affectée;
- Les catégories de données personnelles concernées ;
- Les destinataires ou les catégories des destinataires des données personnelles, le cas échéant;
- Les cas échéant que le responsable du traitement a l'intention de transférer des données personnelles à un destinataire dans un pays tiers et le niveau de protection accordé aux données;
- Toutes autres informations complémentaires nécessaires afin de garantir un traitement juste et équitable.

4.2 Les données personnelles ne peuvent être collectées qu'à des fins spécifiques, déterminées, explicites et légitimes.

Les données obtenues à des fins spécifiques ne doivent pas être utilisées à des fins différentes de celles officiellement notifiées à l'autorité de surveillance dans le cadre du registre de traitement RGPD de l'entreprise comportant la nature du traitement. La procédure générale d'information des personnes et transparence (**RGPD-6.1**) définit les procédures pertinentes.

4.3 Les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

Le responsable du traitement doit s'assurer que l'entreprise ne collecte pas d'informations qui ne sont pas strictement nécessaires au but recherché par l'entreprise et pour lequel les données sont obtenues.

Tous les formulaires de collecte de données (électronique ou papier), y compris les exigences de collecte de données dans de nouveaux systèmes d'information, doivent inclure une déclaration de traitement équitable ou un lien vers la déclaration de confidentialité approuvée par le responsable du traitement avec l'aide du Délégué à la Protection des Données (DPD / DPO).

Le responsable du traitement avec l'aide du Délégué à la Protection des Données (DPD / DPO) devra vérifier annuellement que la collecte des données rassemblées continue à être adéquate, pertinente et non excessive au regard du but recherché par l'entreprise.

4.4 Les données personnelles doivent être exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude)

Les données qui sont stockées par le responsable du traitement doivent être examinées et mises à jour si nécessaire. Aucune donnée ne devrait être conservée à moins qu'il ne soit raisonnable de supposer qu'elle est exacte et nécessaire.

Le Délégué à la Protection des Données (DPD / DPO) doit être mis en mesure de s'assurer que tout le personnel ait bien été formé à l'importance de collecter des données exactes et d'en assurer la mise à jour et la sauvegarde.

Il appartient également à la personne concernée de s'assurer que les données détenues par R2 sont exactes et à jour.

Les salariés, membre du personnel, clients et sous-traitants sont tenus de notifier à R2 tout changement de circonstance pour permettre la mise à jour en conséquence de leurs dossiers personnels.

L'entreprise, avec l'aide du Délégué à la Protection des Données (DPD / DPO) doit veiller à ce que des procédures et politiques appropriées soient mises en place afin de garder des données personnelles exactes et à jour, en tenant compte du volume de données collectées, de la rapidité avec laquelle elles peuvent changer et des autres facteurs pertinents.

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

Au moins une fois par an, R2, avec l'aide du Délégué à la Protection des Données (DPD / DPO) examine les dates de conservation de toutes les données personnelles traitées par l'entreprise, en se référant au registre des traitements (**RGPD-4.1**) et identifie toutes les données qui ne sont plus nécessaires et en conséquence plus exigées dans le contexte de la finalité de traitement. Ces données seront archivées/effacées/détruites en toute sécurité conformément à la procédure de destruction des données à caractère personnel et à la procédure d'archivage des données à caractère personnel.

R2, avec l'aide du Délégué à la Protection des Données (DPD / DPO) répond aux demandes de rectification des personnes concernées sous un mois. Ce délai peut être étendu à deux mois supplémentaires dans le cas de requêtes complexes. Si l'entreprise décide de ne pas donner suite à la requête, le responsable du traitement après avis du Délégué à la Protection des Données (DPD / DPO) doit répondre aux personnes concernées et les informer de leur droit de saisine de l'autorité de contrôle afin de lui soumettre leur plainte.

R2 préconise des dispositions appropriées relatives aux organisations tierces des données personnelles qui se révéleraient inexactes ou périmées, et à les informer que les informations sont inexactes et/ou périmées et ne peuvent plus être utilisées pour informer des décisions relatives aux personnes concernées, et s'efforceront d'orienter les tiers afin d'apporter les corrections nécessaires aux données personnelles lorsqu'elles seront exigées par les personnes concernées.

4.5 Les données personnelles doivent être sauvegardées sous une certaine forme telle que la personne concernée ne puisse être identifiée que le temps nécessaire au traitement.

Lorsque les données personnelles sont conservées au-delà du délai prévu par le traitement, elles seront réduites au minimum, cryptées ou pseudonymisées pour protéger l'identité de la personne concernée en cas de violation de données.

Les données personnelles seront conservées conformément au registre des traitements (**RGPD-4.1**) et, une fois le délai de conservation dépassé, elles doivent être détruites de manière sécurisée comme exposé dans cette procédure.

Le responsable du traitement doit spécifiquement approuver toute conservation de données qui excède les périodes de conservation définies dans le registre des traitements (**RGPD-4.1**) et doit s'assurer que la justification est clairement identifiée.

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

4.6 Les données personnelles doivent être traitées de manière à garantir un niveau de sécurité appropriée

R2, avec l'aide du Délégué à la Protection des Données (DPD / DPO) effectue une évaluation de risque prenant en compte la finalité recherchée par l'entreprise au regard de toutes les circonstances, des opérations de contrôle et du traitement utilisé.

Pour déterminer le caractère approprié de la sécurité, le responsable du traitement avec l'aide du Délégué à la Protection des Données (DPD / DPO) devra aussi considérer l'étendue du préjudice inhérent aux dommages ou pertes pouvant être causés à la personne concernée (personnel ou client) en cas de violation de la sécurité et de tout dommage potentiel à la réputation, incluant la perte possible de confiance du client.

En évaluant des mesures techniques appropriées, le responsable du traitement avec l'aide du Délégué à la Protection des Données (DPD / DPO) considérera la chose suivante :

- Protection de mot de passe;
- Verrouillage Automatique de terminaux inoccupés;
- Suppression des droits d'accès pour les supports USB et d'autres supports de mémoire ;
- Logiciel anti-virus et pare-feu;
- Droits d'accès basés sur les rôles incluant ceux assignés au personnel temporaire ;
- Sécurité des dispositifs qui quittent les locaux de l'entreprise comme des ordinateurs portables;
- Sécurité des réseaux locaux et étendus;
- Technologies améliorant la confidentialité telles que la pseudonymisation et l'anonymisation;
- Identifier les normes de sécurité internationales appropriées pertinentes pour l'entreprise.

En évaluant des mesures organisationnelles appropriées l'entreprise, avec l'aide du Délégué à la Protection des Données (DPD / DPO), considère la chose suivante :

- Les niveaux de formation appropriés à chaque département de l'entreprise;
- Les mesures qui évaluent la fiabilité de salariés (comme des références etc.);
- L'inclusion de l'obligation de protection de données dans les contrats de travail;
- L'identification des actions disciplinaires pour violation de la protection des données;

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

- Contrôles physiques de l'accès aux documents électroniques et papier;
- Stockage de données sur papier dans des armoires sécurisées;
- Limitation de l'utilisation de dispositifs électroniques portables à l'extérieur du lieu de travail;
- Limitation de l'utilisation des appareils personnels des salariés utilisés sur le lieu de travail;
- Adoption de règles claires s'agissant des mots de passe;
- Faire des sauvegardes régulières de données personnelles et stockage du média hors-site;
- Imposition d'obligations contractuelles aux organisations importatrices afin qu'elles garantissent des mesures de sécurité appropriées lors du transfert des données à l'extérieur de l'UE.

Ces contrôles ont été choisis sur la base des risques identifiés pour les données personnelles et des risques de dommages potentiels (préjudices matériels ou physiques) pour les personnes concernées dont les données sont en cours de traitement.

4.7 Le responsable du traitement doit pouvoir démontrer la conformité de l'entreprise aux autres principes de RGPD

Le RGPD inclut les dispositions qui promeuvent la responsabilisation et la gouvernance. Ceux-ci complètent les exigences de transparence de RGPD. Le principe de responsabilité exige que R2 démontre qu'elle respecte les principes du RGPD. Le RGPD déclare explicitement qu'il en est de sa responsabilité.

R2 démontre sa conformité aux principes de protection de données en respectant les codes de conduite, en appliquant des mesures techniques et organisationnelles, et en adoptant des techniques telle que la protection de données dès la conception (privacy by default), des Analyses d'Impact sur la vie privée, des procédures de notification d'incident et des plans d'intervention.

5. Les droits des personnes concernées

Les personnes concernées ont les droits suivants quant au traitement de leurs données et des données qui sont enregistrées les concernant :

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

- avoir été avisées de la nature des informations collectées et des personnes physiques ou morales auxquelles elles pourraient être divulguées ;
- empêcher le traitement susceptible d'endommager leurs données ou de leur causer un préjudice ;
- empêcher le traitement à des fins de marketing direct ;
- être informé de la mécanique de processus automatisé de prise de décision qui les affecte significativement ;
- subir des décisions significatives qui les affectent, uniquement par le processus automatisé ;
- poursuivre en justice en réparation du préjudice qu'elles subissent du fait d'une infraction au RGPD ;
- agir, pour rectifier, pour bloquer, pour effacer, y compris le droit à être oublié, ou détruire des données inexacts ;
- demander à l'autorité de contrôle d'évaluer si une disposition au RGPD a été enfreinte ;
- obtenir les données personnelles les concernant dans un format structuré, communément utilisé et dans un format lisible par machine, et le droit de transmettre ces données à un autre responsable de traitement ;
- élever une objection à n'importe quel profilage automatisé qui survient sans leur consentement.
-

Les personnes concernées peuvent solliciter des demandes d'accès aux données comme décrit dans la procédure de demande d'exercice des droits d'une personne concernée (**RGPD-7.1**); cette procédure décrit aussi comment R2 s'assurera que sa réponse à la demande d'accès aux données est bien conforme aux exigences du RGPD.

Les personnes concernées ont le droit de porter plainte concernant le traitement de leurs données personnelles et le traitement d'une demande d'une personne concernée.

6. Le consentement

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

R2 entend par "consentement" qu'il a été explicitement et librement donné, ce après que les personnes concernées aient reçue une information spécifique, et l'indication sans équivoque de leurs propres souhaits s'agissant de leurs données personnelles et que, par une déclaration ou par une action affirmative claire de leur part, les personnes concernées signifient leur accord au traitement de données personnelles les concernant.

Les personnes concernées peuvent retirer leur consentement à tout moment.

R2 entend par "consentement" qu'il signifie que les personnes concernées ont été pleinement informées de la finalité du traitement et ont signifié leur accord de manière libre et éclairée et sans contrainte.

Le consentement obtenu sous la contrainte ou sur la base d'une erreur induite d'informations ne constitue pas une base légale pour réaliser le traitement

Une communication active doit exister entre les parties pour démontrer le consentement actif. Le consentement ne peut pas être déduit de la non-réponse à une communication. Le responsable du traitement doit pouvoir prouver que ce consentement a été obtenu pour l'opération de traitement.

Pour des données sensibles, le consentement explicite par écrit est obligatoire de la part de la personne concernée et doit être obtenu à moins qu'une base légitime alternative pour le traitement n'existe.

Lorsque R2 fournit des services en ligne aux enfants, l'autorisation parentale doit être obtenue.

7 . La sécurité de données

Tous les salariés et membres du personnel doivent s'assurer que toutes données personnelles qu'ils collectent pour le compte de l'entreprise, soient conservées en toute sécurité et ne puissent être divulguées à aucun tiers à moins que ce tiers n'ait été spécifiquement autorisé par l'entreprise à recevoir des informations et soit signataire de l'engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel (**RGPD-5.3**).

Les données personnelles ne devraient être accessibles seulement par ceux qui doivent les utiliser et cet accès ne peut être accordé que conformément à sa Politique.

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

Toutes les données personnelles doivent être traitées avec la plus haute sécurité et doivent être conservées:

- dans une pièce verrouillable avec accès contrôlé; et / ou
- dans un tiroir ou un classeur verrouillé; et / ou
- s'il est informatisé, protégé par mot de passe conformément aux exigences de l'entreprise ; et / ou
- stockées sur des supports informatiques (amovibles) cryptés.

Des précautions doivent être prises pour s'assurer que les écrans de PC et les terminaux ne soient pas visibles sauf aux employés/membres du Personnel autorisés par l'entreprise.

Des documents papiers ne doivent pas être laissés en libre accès au personnel non autorisé et ne peuvent pas être enlevés des locaux sans autorisation écrite explicite.

Des données personnelles doivent être supprimées et, une fois le délai de conservation dépassé, elles doivent être détruites de manière sécurisée comme exposé dans cette procédure.

Le traitement de données personnelles "hors site" présente un risque potentiellement plus élevé de perte, vol ou de détérioration de données personnelles. Le personnel doit être spécifiquement autorisé à traiter des données hors-site.

8. Divulgence de données

R2 s'assure que des données personnelles ne soient pas divulguées aux tiers non autorisés qui incluent les membres de la famille, les amis et les administrations publiques. Tous les employés/membres du personnel sont soumis à une obligation de prudence dès lors qu'est sollicitée la divulgation de données personnelles, par toute personne autre que celle concernée, au bénéfice d'un tiers. Il est important de savoir évaluer le degré de risque relatif à la divulgation des informations (est-elle pertinente ou nécessaire) au regard de la nature de l'activité de l'entreprise.

Toutes les demandes de divulgation des données pour l'une de ces raisons doivent être répertoriées par écrit dans un registre approprié et toute divulgation doit être spécifiquement autorisée par l'entreprise.

9. Conservation et mise à disposition de données

R2 ne gardera pas de données personnelles sous une forme qui permet l'identification des personnes

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

concernées pendant une période plus longue que nécessaire, eu égard à la finalité de traitement pour laquelle les données ont été à l'origine collectées.

R2 peut stocker des données pendant des périodes plus longues si les données personnelles sont traitées aux fins d'archivage dans l'intérêt public, de recherche scientifiques ou historiques ou à des fins statistiques, sous réserve de l'application de mesures techniques et organisationnelles appropriées pour sauvegarder les droits et les libertés de la personne concernée.

Les données personnelles doivent être éliminées de manière sécurisée conformément au sixième principe du RGPD - c'est à dire traitées d'une manière appropriée afin de maintenir un niveau élevé de sécurité, protégeant ainsi "les droits et les libertés" des personnes concernées.

10. Transfert de données

Tous les transferts de données hors de l'Union Européenne doivent garantir "un niveau approprié de protection pour les droits fondamentaux de la personne concernée".

Le transfert de données personnelles en dehors de l'UE est interdit à moins qu'une ou plusieurs des exceptions spécifiées ci-dessous ne s'appliquent

- Une décision d'adéquation

La Commission Européenne peut évaluer les pays tiers, un territoire et/ou des secteurs spécifiques au sein de pays tiers afin de déterminer s'il existe un niveau approprié de protection pour les droits et les libertés de personnes physiques.

Dans ces cas aucune autorisation n'est nécessaire.

- Les pays qui sont les membres de l'Espace Economique Européen (EEE), mais pas de l'UE sont considérés comme remplissant les conditions d'une décision d'adéquation.

Une liste des pays qui satisfont actuellement aux exigences d'adéquation de la Commission est publiée dans le Journal Officiel de l'Union européenne. [Http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en .htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

- Règles d'entreprise contraignantes.

R2 peut adopter des règles d'entreprise contraignantes obligatoires et approuvées pour le transfert de données à l'extérieur de l'UE. Ceci exige la soumission à l'autorité de contrôle pour l'approbation

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

des règles sur lesquelles l'entreprise cherche à s'appuyer.

- Clauses contractuelles types.

R2 peut adopter des clauses contractuelles types approuvées pour le transfert de données à l'extérieur de l'UE.

- Les exceptions

En absence d'une décision d'adéquation, de règles contraignantes d'entreprise et/ou des clauses contractuelles types, un transfert de données personnelles vers un pays tiers ou à une organisation internationale aura seulement lieu si une des conditions suivantes est remplie :

- La personne concernée a explicitement consenti au transfert proposé, après avoir été informée des risques éventuels d'un tel transfert pour ses données collectées en raison de l'absence d'une décision d'adéquation et de garanties appropriées;
- Le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable de traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée;
- Le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne morale ou physique;
- Le transfert est nécessaire pour des raisons importantes d'intérêt public;
- Le transfert est nécessaire pour l'établissement, l'exercice ou la défense de réclamations légales; et/ou
- Le transfert est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée est physiquement ou légalement incapable de donner son consentement.

11. Le registre des traitements

R2 a établi un registre des traitements pour son compte (**RGPD-4.1**) et un registre de sous-traitant (**RGPD-4.2**) dans le cadre de son approche visant à prévenir les risques de non-conformité au RGPD.

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 25/01/2022

Propriétaire du document et approbation

R2 est le propriétaire de ce document. Elle en est responsable et doit s'assurer que cette politique soit conforme aux exigences du RGPD.

Une version actuelle de ce document est disponible pour tous les membres du personnel sur le système d'information de l'entreprise et est publiée.

Cette politique a été approuvée par la direction de R2 et est publiée sous le contrôle du Directeur Général (DG).