

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 04/03/2022

1. Introduction

1.1 Contexte et champ d'application 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. La loi n° 2018-493 du 20 juin 2018 est venue modifier la loi Informatique et Libertés afin de mettre en conformité le droit français avec le cadre juridique européen.

Le RGPD s'applique aux traitements, automatisés ou non, de données à caractère personnel contenues ou appelées à figurer dans un fichier.

1.2 Définitions utilisées par R2

Données à caractère personnel

Toute information relative à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») directement ou indirectement ou par combinaison d'information.

Données sensibles

Données personnelles révélant les prétendues origines raciales ou ethniques, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle ou l'orientation sexuelle, les données génétiques ou biométriques dans le but d'identifier de manière unique une personne physique, les données concernant la santé 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, la structuration, la conservation, l'adaptation ou la

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 04/03/2022

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.

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.

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.

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 personnelles

Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, 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 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, 75006 Paris s'engage à respecter son obligation de conformité avec le règlement de l'UE et les lois de l'État Français ; en ce qui concerne les données personnelles de toute personne concernée que R2 recueille et traite conformément au Règlement Général de Protection de Données (RGPD).

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 04/03/2022

La conformité avec le RGPD est décrite par cette politique de protection des données et d'autres politiques appropriées, ainsi que des processus et procédures connexes.

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

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 R2 doivent s'assurer du développement des bonnes pratiques de traitement d'informations au sein de R2.

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 R2 avec le RGPD. Le DPO a été nommé pour s'assurer de la conformité de R2 avec le 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**).

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

La politique de formation au RGPD de R2 (**RGPD-3.1**) définit des exigences de formation spécifique et de sensibilisation au regard des rôles spécifiques de chacun des salariés et membre du personnel de R2.

Les salariés et membres du personnel de R2 doivent s'assurer que toutes données personnelles les concernant ou fournies par eux au nom de R2 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.

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 04/03/2022

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 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

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 04/03/2022

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 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 R2 sont conçues pour assurer le respect de ces principes.

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 04/03/2022

4.1 Les données personnelles doivent être traitées de manière licite

Chaque traitement doit être licite.

Cela signifie d'abord qu'il doit être conforme au droit en général.

Cela signifie, ensuite, qu'il doit reposer sur l'une des six « bases légales » permises par le RGPD, c'est-à-dire l'une des hypothèses dans lesquelles le RGPD autorise un opérateur à traiter les données de personnes physiques :

- L'obtention du consentement préalable de la personne,
- L'exécution d'un contrat conclu avec elle,
- L'intérêt légitime
- L'accomplissement d'une mission d'intérêt publique,
- Le respect d'une obligation légale qui impose le traitement de ces données,
- La sauvegarde des intérêts vitaux

4.2 Les données personnelles doivent être traitées de manière transparente

Les personnes doivent être informées de l'utilisation des données les concernant et de la manière d'exercer leurs droits. L'information sur les traitements doit être fournie de manière transparente, compréhensible et aisément 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.

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

Les données personnelles collectées ne peuvent être traitées que pour une finalité légale, définie précisément et légitime.

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 04/03/2022

Un traitement de données doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation. Autrement dit, il n'est pas permis de collecter des données lorsque l'on ne sait pas quel usage en faire. Par ailleurs, en principe, la finalité initiale doit être respectée, afin d'éviter tout « détournement de finalité »

Les données obtenues à des fins spécifiques ne doivent pas être utilisées à des fins différentes de celles inscrites dans le registre des traitements (**RGPD-4.1**) de R2.

4.4 Les données personnelles doivent être adéquates, pertinentes et limitées (minimisation des données)

R2 doit s'assurer que R2 ne collecte pas d'informations qui ne sont pas strictement nécessaires au but recherché par R2 et pour lequel les données sont obtenues.

Le responsable du traitement avec l'aide du Délégué à la Protection des Données (DPD / DPO) devra vérifier périodiquement que les données rassemblées restent adéquates, pertinentes et non excessives au regard de la finalité de traitement recherchée par R2.

4.5 Les données personnelles doivent être exactes et, si nécessaire, tenues à jour

Les données qui sont stockées par R2 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.

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.

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 R2 décide de ne pas donner suite à la requête, R2 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 (la CNIL) afin de lui soumettre leur plainte.

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 04/03/2022

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 R2 au regard de toutes les circonstances, des opérations de contrôle et du traitement utilisé.

Au regard des risques, des mesures doivent être mises en œuvre pour s'assurer de la sécurité des données traitées. R2 met en place des mesures techniques et organisationnelles pour garantir la sécurité des données.

En fonction de leur sensibilité, des mesures spécifiques sont nécessaires en cohérence avec les risques pour les droits et libertés des personnes concernées (ex : usurpation d'identité).

Trois types de risques sont ainsi à considérer : l'accès illégitime à des données, leur modification non désirée et leur disparition.

4.7 R2 doit pouvoir démontrer sa conformité aux autres principes de RGPD

Le RGPD inclut les dispositions qui promeuvent la responsabilisation et la gouvernance. Le principe de responsabilité exige que R2 démontre qu'elle respecte les principes du RGPD.

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 des droits quant aux traitements de leurs données à caractère personnel effectués par R2. Ces droits sont le droit d'être informé, le droit d'accès, le droit de rectification, le droit à l'effacement, le droit à la limitation du traitement, le droit à la portabilité des données, le droit d'opposition et les droits liés à la prise de décision automatisée y compris le

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 04/03/2022

profilage. L'application de ces droits dépend de la base légale du traitement.

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.

6. Le consentement

Quand un traitement de données à caractère personnel se fonde sur la base légale du consentement, R2 doit pouvoir prouver que ce consentement a été obtenu. Les personnes concernées peuvent retirer leur consentement à tout moment.

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.

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 R2, soient conservées en toute sécurité et ne puissent être divulguées à aucun tiers à moins que ce tiers n'ait été spécifiquement autorisé par R2 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-5.2**).

Une fois le délai de conservation dépassé, Les données personnelles doivent être détruites de manière sécurisée.

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. Divulcation 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 et

POLITIQUE GÉNÉRALE DE PROTECTION DES DONNÉES

Contrôle des documents

Référence: RGPD-1.1

Date d'émission: 04/03/2022

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. Toute divulgation doit être spécifiquement autorisée par R2.

9. Conservation et mise à disposition de données

R2 ne gardera pas de données personnelles sous une forme qui permet l'identification des personnes 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. Les données doivent être archivées, supprimées ou anonymisées dès que la finalité pour laquelle elles ont été collectées est atteinte.

Périodiquement, 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 R2, en se référant au registre des traitements (RGPD-4.1 et RGPD-4.2) et identifie toutes les données qui ne sont plus nécessaires.

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 nécessite une décision d'adéquation, des Règles d'entreprise contraignantes ou des clauses contractuelles types.

11. Le registre des traitements

R2 a établi un registre des traitements pour son compte (**RGPD-4.1**) et pour le compte de ses clients (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: 04/03/2022

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).