13 mai 2022

Gitec Human Resources

Code de conduite et de bonnes pratiques

RGPD

LEXING
ALAIN BENSOUSSAN AVOCATS

Diffusion du code

Gitec Human Resources, membre du réseau VNH (ci-après Gitec Human Resources), assure la diffusion du présent code de conduite au sein de ses membres adhérents.

Mise à jour du code

En fonction de la réglementation en vigueur et afin de tenir le code de conduite à jour, Gitec Human Resources pourra se réserver la faculté de mettre à jour le présent code de conduite.

La nouvelle version du code de conduite sera disponible sur les sites : https://vnh.fr/, https://gitec.fr/, https://sopratec.fr/, https://anov.fr/ .

Glossaire

Pour la lecture du présent code de conduite et une meilleure compréhension des termes ou expressions spécifiques en matière de protection des données à caractère personnel, les membres sont invités à consulter le « Glossaire ».

Table des matières

1 Préambule

1. La protection des *données à caractère personnel**[1] constitue un atout compétitif majeur et un facteur de confiance à l'égard des partenaires commerciaux, des consommateurs et des employés.

2. Gitec Human Resources, membre du réseau VNH (ci-après Gitec Human Resources), s'est engagée dans une politique d'entrepreneuriat fondée sur le respect de valeurs éthiques fortes. La confiance, l'intégrité et la protection des *données à caractère personnel** et de la vie privée sont au cœur de ses préoccupations et de celles de ses membres.

3. Le code des bonnes pratiques constitue un *code de conduite** permettant aux membres de Gitec Human Resources d'illustrer un comportement responsable et éthique qu'il faut observer à l'occasion de la *collecte** et du traitement de *données à caractère personnel**.

4. Le présent code est applicable à compter de la date d'adhésion d'une entité de Gitec Human Resources. Une entité de Gitec Human Resources est dénommée ci-après dans le présent code de conduite : l'entité.

2 Quel est l'objet de ce code ?

5. Le présent code a pour objet de préciser les bonnes pratiques, ainsi que les règles de bonne conduite pour assurer la protection des données personnelles et de la vie privée des personnes physiques et notamment de leurs clients, de leurs fournisseurs, partenaires commerciaux, ainsi que des salariés des entités, membres de Gitec Human Resources.

6. Ce présent *code de conduite** permet de préciser les modalités d'application du règlement UE 2016/679 relatif à la protection des données, RGPD, conformément à son article 40 :

> « Le code de conduite comprend les mécanismes permettant à toute entité, de procéder au contrôle obligatoire du respect de ses dispositions par les responsables du traitement ou les sous-traitants qui s'engagent à l'appliquer, sans préjudice des missions et des pouvoirs de l'autorité de contrôle qui est compétente ».
>
> « L'application d'un code de conduite approuvé comme le prévoit l'article 40 du règlement peut servir d'élément pour démontrer le respect des obligations incombant au responsable du traitement. »

3 A quelles conditions s'applique-t-il et qui est concerné ?

7. Le présent code s'applique pour le traitement des *données à caractère personnel** concernant tant les clients des entités de Gitec Human Resources que les *données à caractère personnel** relatives aux sous-traitants, autres partenaires contractuels, et aux salariés.

4 Quels sont les principes à mettre en œuvre lors d'un traitement de données à caractère personnel ?

8. La réglementation relative à la protection des données personnel implique de prendre en compte plusieurs grands principes présentés ci-après et qui doivent être observés scrupuleusement.

4.1 Comment réaliser une collecte de données à caractère personnel de manière licite et légale ? (Principe de légalité)

Article 5-1 a) et 6 du RGPD

9. Chaque entité s'interdit de réaliser un *traitement** à partir de données collectées de manière illicite.

[1] **Les mots en italiques suivis d'un astérisque sont définis dans le glossaire en annexe.**

10. Avant la mise en œuvre d'un *traitement**, chaque entité vérifie que l'objectif du traitement est en conformité avec la réglementation applicable à son secteur d'activité.

11. Chaque entité vérifie également auprès de son référent protection des données si le traitement envisagé doit faire l'objet de formalités préalables.

4.2 Comment recueillir des données à caractère personnel pour une utilisation déterminée ? (Principe de finalité)

Article 5-1 b) du RGDP

12. Chaque entité s'interdit toute réutilisation des données pour des *finalités** incompatibles avec les *finalité*s** initiales.

4.3 Comment s'assurer qu'un traitement de données à caractère personnel est légitime ? (Principe de légitimité)

Article 5-1 c) d) e) du RGDP

13. Chaque entité définit clairement les objectifs de son traitement, les données doivent uniquement être collectées pour des *finalités** (*utilisations*) déterminées, explicites et légitimes et ne pas être traitées d'une manière incompatible avec ces *finalités**.

4.4 Comment s'assurer que la collecte des données à caractère personnel n'est pas excessive à l'objectif de la collecte ? (Principe de proportionnalité)

Article 5-1 c) d) e) du RGDP

14. Chaque entité ne doit pas être excessive dans la *collecte** des données et garder en tête que seules peuvent être collectées les données à caractère personnel strictement nécessaires à la réalisation du traitement.

15. En particulier, chaque entité s'interdit de *collecter** et de traiter des *données à caractère personnel sensibles** si ces données ne sont pas strictement indispensables à la *finalité** de son traitement.

16. Chaque entité doit vérifier auprès de son référent protection des données qu'il est autorisé à *collecter** ces données au titre de la règlementation en vigueur.

17. Chaque entité, dès la création de son traitement, définit la durée pendant laquelle il aura besoin de conserver les données pour pouvoir atteindre l'objectif du traitement.

18. Chaque entité s'assure que les données soient conservées pendant une durée n'excédant pas celle nécessaire au regard des *finalités** pour lesquelles elles sont traitées.

5 A quelles conditions puis-je adhérer à ce code ?

19. Le présent code doit être appliqué en intégralité par toute entité qui a manifesté son intention claire d'adhérer pour mettre en œuvre.

20. Une entité ne peut pas adhérer pour mettre en œuvre qu'une seule partie du présent code.

21. Afin d'adhérer au présent code, chaque entité doit remplir la déclaration d'adhésion figurant en annexe. L'auto-déclaration est le principe pour toutes les entités. La déclaration d'adhésion prouvera que l'entité s'est engagée à respecter les obligations issues du présent code de conduite.

22. La déclaration d'adhésion sera valable pour une durée initiale de 3 an(s) et devra être renouvelée à l'arrivée du terme de la durée initiale.

6 Comment réaliser un traitement loyal et transparent de données à caractère personnel ?

Considérants 39 et 60 du RGPD

23. Chaque entité doit être transparente vis-à-vis des personnes concernées : les données à caractère personnel ne doivent pas être collectées et traitées à l'insu des personnes concernées.

24. Avant de mettre en œuvre un traitement, chaque entité doit vérifier que les personnes concernées ont été informées :

- des traitements portant sur les données à caractère personnel les concernant ;
- de leurs droits (*droits d'accès**, de *rectification**, d'opposition, de portabilité, de suppression).

25. A défaut, chaque entité doit préparer une mention permettant de diffuser clairement cette information.

Exemple. Une mention d'information pour l'information des personnes concernées pourra être apposée sur votre site internet, lors de l'affichage d'un panneau, dans un contrat ou encore sur un bon de commande.

FAQ. Un générateur de mention d'information est présenté dans la FAQ.

26. Chaque entité ne doit pas se procurer des données à caractère personnel auprès de *tiers** sans s'être assurée au préalable que ces *tiers** ont les droits nécessaires pour *collecter** et céder de telles données.

Exemple. L'acquéreur d'un fichier client lors de la cession d'un fonds de commerce doit être également vigilant quant à la **qualité du fichier acquis**.

Avant d'acquérir un fichier clients, il est recommandé de s'assurer, voire d'obtenir la **garantie que le vendeur a informé et recueilli le *consentement** ** des personnes concernées lorsqu'il était nécessaire.

L'acquéreur doit obtenir la garantie que **les données personnelles de personnes qui auraient exprimé leur opposition ne figurent pas dans le fichier vendu/cédé** ou encore que les **données personnelles conservées sont en conformité avec la *durée de conservation** prévue.**

La loi Informatique et libertés oblige le nouveau responsable d'un traitement de données qui n'a pas directement recueilli les données des personnes concernées (notamment en cas de cession de clientèle par un fonds de commerces) de les informer de son **nom, la *finalité** du traitement, la *durée de conservation** des données et ce, dès l'enregistrement des données**.

7 Comment recueillir le consentement de la personne concernée et s'assurer de sa validité ?

Considérants 32, 42 et 43 (principalement) et article 6 à 9 du RGPD.

27. Afin que le *consentement** de la *personne concernée** soit valable, il doit présenter les caractéristiques présentées ci-après.[2]

7.1 Le consentement doit avoir été librement donné

28. Cet élément constitutif suppose un réel choix et un réel contrôle de la *personne concernée**. De manière générale, le RGPD exclut toute validité du *consentement** en cas d'absence de liberté. Si le *consentement** est lié à une part non négociable de conditions contractuelles, il n'est pas présumé avoir été « librement donné ». Il en va de même si la *personne concernée** ne peut le retirer sans en subir un préjudice.

7.1.1 Le consentement ne peut être la contrepartie d'un contrat ou lié à la conclusion d'un contrat sur un produit ou un service (Notion de Conditionnalité)

29. Le RGPD indique que la *situation de* « package » c'est-à-dire la conclusion d'un contrat ou la vente d'un service associé à une demande de *consentement** à un traitement de données qui n'est pas absolument nécessaire est considéré comme hautement indésirable. Si le *consentement** est donné dans une telle situation, il est présumé ne pas être donné librement. Ce ***consentement** ne peut être la contrepartie d'un contrat*.

30. **La conclusion d'un contrat ou la vente d'un service ne doit pas être liée au *consentement** de la *personne concernée** à un traitement de données**.

31. Si un *responsable du traitement** cherche à traiter des données qui sont nécessaires pour l'exécution d'un contrat, il doit choisir le fondement contractuel. Dans cette hypothèse, il n'y a pas besoin d'utiliser un autre fondement, tel que le *consentement**.

32. En toute hypothèse en matière de *consentement**, il convient de noter que rend le *consentement** invalide :

- tout élément de pression ou d'influence inappropriée sur la *personne concernée**.

33. La charge de la preuve du *consentement** pèse sur le *responsable du traitement** en raison du principe d'*accountability**.

7.1.2 La personne exprimant son consentement doit être libre de choisir les finalités (les usages)

34. Un service peut impliquer de multiples opérations de traitement pour plusieurs *finalités**. Dans cette hypothèse, les personnes concernées doivent être libres de choisir quelle(s) *finalité**(s) elles acceptent plutôt que de devoir consentir à un ensemble de finalités. Par conséquent il faut recueillir différents *consentements** pour pouvoir commencer à offrir un service.

35. Si le *responsable du traitement** n'a pas cherché à recueillir ces différents *consentements**, il y a un manque de liberté pour la personne concernée. Il convient de détailler les *finalités** afin que le consentement puisse être qualifié de libre, en donnant à la personne concernée la liberté de choisir.

[2] Guidelines on Consent under Regulation 2016/679, Adopted on 28 November 2017 (WP259).

7.1.3 La personne exprimant son consentement doit être en mesure de refuser ou de retirer son consentement gratuitement

36. Le *responsable du traitement** doit démontrer qu'il est possible pour la personne concernée de refuser ou de retirer son *consentement** sans préjudice. Un préjudice s'entend ici d'un éventuel coût pour la *personne concernée** et donc un désavantage au fait de procéder de la sorte. D'autres exemples de préjudices sont : la tromperie, l'intimidation, la coercition ou la conséquence négative significative.

37. Si un *responsable du traitement** est capable de démontrer qu'un service inclus la possibilité de retirer son *consentement** sans aucune conséquence négative telle qu'une diminution des performances du service, ceci constitue un faisceau d'indices démontrant que le *consentement** a été donné librement.

7.2 Le consentement de la personne concernée doit être spécifique au regard des usages des données (Critère de spécificité du consentement)

38. Le *consentement** doit également être spécifique, ce qui permet à la *personne concernée** d'exercer un certain contrôle de sa part. Pour satisfaire ce critère, le *responsable du traitement** doit appliquer :

- une spécification des *finalités** comme protection contre les utilisations indésirables ;
- un niveau de détail très fin des demandes de *consentement** ;
- une séparation claire des informations nécessaires à l'obtention du *consentement** pour le traitement des données et des informations liées à d'autres thématiques.

39. Si le *responsable du traitement** traite des données sur le fondement du *consentement** de la personne concernée et souhaite traiter des données pour une nouvelle *finalité*,* il doit obtenir un nouveau *consentement** de la part de la *personne concernée**. Cela devrait se traduire par des opérations spécifiques de recueil du consentement préalable de la personne concernée (*opt-in**) pour chaque *finalité**, pour permettre à l'utilisateur de donner un *consentement** réputé spécifique.

40. Le *consentement** donné par le client pour une enseigne ne peut alors être valable pour les deux autres enseignes exploités par la coopérative.

Exemple. Si la *personne concernée** n'a pas donné son *consentement** pour la *collecte** de données qui sont utilisées à des fins relatives à l'historique des réparations ce traitement ne sera pas licite.

Vous ne pouvez pas utiliser votre fichier pour un autre objectif que celui qui a été défini et dont la *personne concernée** a donné son *consentement**.

7.3 La personne doit être parfaitement informée

41. La transparence étant un des principes fondamentaux qui irrigue le RGPD, elle est étroitement liée aux principes d'équité et de licéité. Si le *responsable du traitement** ne fournit pas des informations aisément accessibles, le contrôle de la personne devient illusoire et le *consentement** ne sera pas un fondement valide du traitement de données.

7.3.1 Quelles sont les informations qui doivent être fournies par le responsable du traitement à la personne concernée ?

42. Ces informations concernent :

- l'identité du *responsable du traitement** ;
- la communication de chaque *finalité** pour chaque traitement, dès lors que le *consentement** de l'utilisateur est recherché ;
- l'indication du type de données utilisé ;
- l'existence d'un droit de retrait du *consentement** ;
- l'information à propos de l'utilisation des données en cas de process automatisés permettant la prise de décision, ce qui inclut le *profiling* ;
- lorsqu'il existe un ou des transfert(s) de données, l'indication des risques possibles de transferts à des pays tiers qui ne seraient pas titulaires d'une décision d'adéquation et des garanties suffisantes.

43. Dans l'hypothèse où le *consentement** recherché est susceptible d'être relié à des co-responsables du traitement ou si les données sont transférées ou traitées par d'autres responsables du traitement qui veulent s'appuyer sur le *consentement** originellement donné, il faut indiquer l'identité de chacune de ces entités. Les responsables du traitement doivent donc fournir une liste complète des *destinataires** de données ou des catégories de *destinataires** de données, cette liste devant comprendre en son sein les différents sous-traitants possibles.

7.3.2 Comment fournir l'information ?

44. **Il n'y a pas de forme particulière**, de nombreuses techniques peuvent être utilisées (écrit, audio, vidéo, oral…). Il faut utiliser un langage clair et précis dans tous les cas. Cela signifie que le message doit être facilement compréhensible pour un interlocuteur moyen. Les responsables du traitement ne peuvent utiliser des politiques de confidentialité longues et inintelligibles ou des déclarations complexes. Le *consentement** doit être clair et distinguable des autres questions abordées, et fourni d'une manière intelligible et accessible.

45. La description des *finalités** doit être toute aussi claire. Si le *consentement** est donné sous une forme électronique, la demande doit être claire et concise. Un responsable du traitement doit déterminer auprès de quelle audience il *collecte** ses données. Par exemple en cas de *collecte** auprès d'un jeune public, il faut s'assurer que le message soit compréhensible par des mineurs. En cas de contrat écrit qui contient un grand nombre d'informations, il faut isoler le *consentement**, en l'actant sur un document annexe par exemple.

7.4 Comment s'assurer qu'un consentement n'est pas ambigu ?

46. Le *consentement** requiert une déclaration de la part de la *personne concernée** sous la forme d'un ***acte positif**** ce qui signifie que le *consentement** doit être donné de manière active.

47. Il peut être obtenu au moyen d'une déclaration écrite ou orale, ce qui inclut les procédés électroniques. La forme prise par de telles déclarations peut revêtir de nombreuses formes. L'utilisation de cases pré-cochées n'est pas valable, de même le silence et l'inactivité ne peuvent être considérés comme une manière active d'indiquer son choix.

48. Il faut veiller à ce que le *consentement** ne soit pas obtenu de la même manière que l'acceptation des autres conditions générales. Il ne faut utiliser de cases pré-cochées.

Exemple. Le professionnel doit solliciter le *consentement** de chaque *personne concernée** constituant un couple.

7.4.1 Le consentement peut-il être obtenu par des moyens électroniques ?

49. Quand le *consentement** est obtenu par des moyens électroniques, il peut être nécessaire d'interrompre l'expérience utilisateur pour donner toute son efficacité à la requête. Cependant les responsables du traitement ont toute latitude pour développer des procédures adaptées à leurs besoins : les mouvements physiques (tels que faire défiler latéralement un objet, un profil, en touchant l'écran, faire un signe devant une caméra, incliner son smartphone dans le sens des aiguilles d'une montre) peuvent être dans certaines hypothèses des indications claires du *consentement** de l'utilisateur.

50. Il peut résulter de ces nombreuses indications une situation dans laquelle les requêtes de *consentement** ne seraient plus réellement lues. C'est un risque particulier pour les personnes concernées et la recherche de manières d'empêcher de tels risques est mise à la charge des responsables du traitement.

51. En toute hypothèse, le *consentement** doit toujours être obtenu préalablement à la mise en place du traitement pour lequel le *consentement** est requis. Si cette demande de *consentement** peut n'être formulée qu'une seule fois, en revanche le *responsable du traitement** doit de nouveau obtenir le *consentement** si les *finalités** du traitement sont modifiées postérieurement à l'obtention du *consentement** ou si de nouvelles *finalités** sont envisagées.

7.5 Comment être certain que la personne concernée a bien exprimé son consentement et qu'il est explicite ?

52. Ce terme se réfère à la façon dont le *consentement** est exprimé par la *personne concernée**. Cela signifie que la *personne concernée** doit donner expressément son *consentement**. La manière la plus sûre serait de le confirmer par écrit. Le *responsable du traitement** peut s'assurer que la demande écrite est signée par la *personne concernée**, de façon à retirer tout doute possible et tout potentiel manque de preuve sur ce point.

53. Cependant une telle déclaration écrite et signée n'est pas le seul moyen de rendre le *consentement** explicite et d'autres formes sont envisageables, notamment les e-mails et signatures électroniques, la *vérification en deux étapes**…

7.6 Quelles sont les conditions supplémentaires de validité du consentement ?

7.6.1 Comment rapporter la preuve du consentement et sur qui pèse cette preuve ?

54. Cette obligation demeure aussi longtemps que le traitement lui-même. Une fois le traitement terminé, la preuve de ce *consentement** n'a pas besoin d'être conservée plus que nécessaire après computation des délais de prescription des actions, et des obligations légales résultant du cadre juridique applicable aux entités des différents secteurs d'activités de Gitec Human Resources.

55. Le *responsable du traitement** peut conserver un registre des *consentement*s** (document de preuve) donnés qui indique :

- si le *consentement** a été donné ;
- la façon dont le *consentement** a été donné (par quels moyens);
- quand il a été donné (date) ;
- les informations fournies à la *personne concernée*s**. ;
- la date éventuelle d'un retrait du *consentement**.

56. Il n'y a pas de limite fixée pour laquelle le *consentement** est réputé valide : la validité du *consentement** dépend du contexte et de son évolution. Le groupe de travail Article 29 (*G29**) recommande de mettre en place des mesures de renouvellement du *consentement**.

57. Cette obligation de rapporter la preuve du *consentement** pèse sur le *responsable du traitement**, qui doit développer des méthodes telles que le registre des *consentement*s** pour être en conformité avec le

RGPD. Cependant cette obligation ne doit pas conduire à traiter en plus des données de manière excessive et ne doit pas non plus conduire à une *collecte** supplémentaire excessive de données.

7.6.2 Le retrait du consentement est-il possible ?

58. Le retrait du *consentement** doit être aussi facile que le fait de donner son *consentement**, sans obligation de passer par les mêmes procédures.

59. Le *responsable du traitement** doit informer les personnes concernées du retrait de leur *consentement** avant que le *consentement** initial ne soit réellement donné. Une fois le *consentement** retiré, toutes les opérations de traitement qui étaient fondées dessus restent valides mais le *responsable du traitement** doit cesser les activités de traitement concernées et les données doivent être supprimées ou anonymisées.

7.7 Etes-vous en présence de données à caractère personnel concernant un enfant ?

7.7.1 Comment s'assurer que le consentement concernant des enfants est valide juridiquement ?

60. En matière de *consentement** des personnes vulnérables telles que les enfants, le plancher en dessous duquel le traitement n'est pas réputé légitime est l'âge de 16 ans, sauf si le *consentement** est donné par le titulaire de l'autorité parentale. Les législateurs nationaux pourront abaisser cet âge sans aller en dessous de 13 ans. Dans le projet de loi français relatif à la protection des données personnelles enregistré à la Présidence de l'Assemblée nationale le 13 décembre 2017 il est précisé que « le gouvernement ayant fait le choix de ne pas faire usage de cette marge de manœuvre, le projet de loi ne contient aucune disposition sur l'âge du consentement, le seuil de 16 ans fixé par le règlement s'appliquant ».

61. Comme indiqué précédemment, le langage utilisé pour obtenir le *consentement** doit être adapté, en termes de vocabulaire, au public visé.

7.7.1.1 Le cas du service offert directement à un enfant

62. C'est l'hypothèse dans laquelle le *responsable du traitement** indique clairement aux personnes concernées qu'il n'offre ses services qu'aux personnes âgées de 18 ans et plus, et que cette indication n'est pas combattue par d'autres éléments de preuve. Dans ce cas, le service n'est pas considéré « *offert directement à un enfant* ».

7.7.1.2 La prise en compte de l'âge de l'enfant

63. Le *responsable du traitement** doit faire les efforts nécessaires pour connaître les différentes lois nationales. En cas de services transfrontières, il ne faut pas seulement appliquer la loi de l'établissement principal mais celle de tous les pays sur lesquels le service est offert.

64. Le *responsable du traitement** doit fournir les efforts nécessaires de vérification de l'âge de la *personne concernée**. Si un enfant donne son *consentement** alors qu'il n'en avait pas la faculté, alors le traitement de données est illicite.

65. Là encore, la vérification de l'âge ne doit pas conduire à un traitement de données excessif.

7.7.1.3 La situation de la responsabilité parentale

66. Une fois atteint l'âge de la maturité pour consentir, le *consentement** donné par le titulaire de l'autorité parentale expire. A partir de cette date, le *responsable du traitement** doit obtenir un *consentement** valide auprès de la *personne concernée** elle-même.

8 Quels peuvent être les objectifs poursuivis pour un traitement et chaque objectif a-t-il un intérêt légitime ?

Considérants 47 à 49 et article 6 du RGPD.

67. La *finalité** d'un traitement peut être défini comme l'objectif poursuivi par le traitement. Les *finalités** du traitement peuvent être les suivantes :

- la gestion des clients (contrats, commandes, comptabilité, programme de fidélité, réalisation d'enquêtes de satisfaction ou de sondages…) ;
- la prospection ;
- l'élaboration de statistiques commerciales ;
- la cession, la location ou l'échange de fichiers de clients et de prospects ;
- la gestion des demandes de *droits d'accès**, de *rectification** et d'opposition ;
- la gestion des impayés et du contentieux ;
- la gestion des avis des personnes sur des produits, services ou contenus.

Exemple. Le *consentement** doit être préalable à l'insertion ou à la lecture de cookies

Tant que la personne n'a pas donné son *consentement**, ces cookies ne peuvent être déposés ou lus sur son terminal.

Attention, il doit être requis à chaque fois qu'une nouvelle *finalité vient s'ajouter aux *finalités** initialement prévues.**

L'utilisateur doit pouvoir accepter ou refuser le dépôt des cookies.
Le choix doit pouvoir être effectué pour chaque application et chaque site internet.

Enfin, le *consentement** doit pouvoir être retiré par l'internaute.

FAQ. Une partie explicative sur les cookies est disponible dans la FAQ.

9 Quels sont les destinataires des données à caractère personnel ?

Considérants 61 et 63 et article 4du RGPD

68. Chaque entité s'engage à ce que - dans la limite de leurs attributions respectives – n'ont accès aux données personnelles que :

- le personnel habilité du service marketing, du service commercial, des services chargés de traiter la relation client et la prospection, des services administratifs, des services logistiques et informatiques ainsi que leurs responsables hiérarchiques ;
- le personnel habilité des services chargés du contrôle ;
- le personnel habilité des sous-traitants dès lors que le contrat signé entre les sous-traitants et le responsable du traitement fait mention des obligations incombant aux sous-traitants en matière de protection de la sécurité et de la confidentialité de données et précise notamment les objectifs de sécurité devant être atteints.

69. Peuvent aussi être des *destinataires** des données :

- les partenaires, les sociétés extérieures ou les filiales d'un même groupe de sociétés dans les conditions prévues par l'article 6 de la norme ;
- les organismes, les auxiliaires de justice et les officiers ministériels, dans le cadre de leur mission de recouvrement de créances ;
- l'organisme en charge de la gestion de la liste d'opposition au démarchage téléphonique.

10 Comment s'assurer que seule une collecte des données nécessaires est effectuée ? (Principe de minimisation)

Article 4, article 5 c), article 25 et article 47.1 du RGPD

70. Chaque entité s'engage à minimiser le traitement des données dès que possible en garantissant que par défaut que seules les données nécessaires à la *finalité** du traitement sont traitées.

Exemple.

Les données personnelles nécessaires seront relatives notamment[3] :

- l'**identité** : civilité, nom, prénoms, adresse, numéro de téléphone (fixe et/ou mobile), numéro de télécopie, adresses de courrier électronique, date de naissance, code interne de traitement permettant l'identification du client (ce code interne de traitement ne peut être le numéro d'inscription au répertoire national d'identification des personnes physiques (numéro de sécurité sociale), ni le numéro de carte bancaire, ni le numéro d'un titre d'identité). Une copie d'un titre d'identité peut être conservée aux fins de preuve de l'exercice d'un *droit d'accès**, de *rectification** ou d'opposition ou pour répondre à une **obligation légale** ;

- les **données relatives au moyen de paiement** : relevé d'identité postale ou bancaire, numéro de chèque, numéro de carte bancaire, date de fin de validité de la carte bancaire, cryptogramme visuel (ce dernier ne devant pas être conservé, conformément à l'article 5) ;

- les **données relatives à la transaction** : telles que le numéro de la transaction, le détail de l'achat, de l'abonnement, du bien ou du service souscrit.

- les **situations familiale, économique et financière** : vie maritale, nombre de personnes composant le foyer, nombre et âge du ou des enfant(s) au foyer, profession, domaine d'activité, catégorie socioprofessionnelle, présence d'animaux domestiques.

- les **données relatives au suivi de la relation commerciale** : demandes de documentation, demandes d'essai, produit acheté, service ou abonnement souscrit, quantité, montant, périodicité, adresse de livraison, historique des achats et des prestations de services, retour des produits, origine de la vente (vendeur, représentant, partenaire, affilié) ou de la commande, correspondances avec le client et service après-vente, échanges et commentaires des clients et prospects, personne(s) en charge de la relation client.

- les **données relatives aux règlements des factures** : modalités de règlement, remises consenties, reçus, soldes et impayés n'entraînant pas une exclusion de la personne du bénéfice d'un droit, d'une prestation ou d'un contrat soumis à autorisation de la Commission telle que prévue par les dispositions de l'article 25-I-4° de la loi du 6 janvier 1978 modifiée. Les informations relatives aux crédits souscrits (montant et durée, nom de l'organisme prêteur) peuvent également être traitées par le commerçant en cas de financement de la commande par crédit

- les **données nécessaires à la réalisation des actions de fidélisation, de prospection, d'étude, de sondage, de test produit et de promotion**.

[3] Liste de données à caractère personnelle non exhaustive.

11 Quels sont les droits des personnes concernées et comment les informer ?

11.1 Quelles sont les informations à fournir ?

Chapitre III Section 2 et article 13 du RGPD :

71. Avant la *collecte** de données chaque entité s'engage à informer la *personne concernée** de :
- l'identité du *responsable du traitement** ;
- la *finalité** du fichier ;
- le caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse ;
- les *destinataires** de données ;
- leurs droits ;
- les éventuels transferts de données vers des pays hors UE.

72. Chaque entité varie en fonction des caractéristiques du fichier support d'information : panneau d'information pour une vidéosurveillance, mention d'information sur un formulaire, lecture de cette information en cas de recueil de données par téléphone, conditions générales de vente, certificat d'authentification, factures.

73. Chaque entité s'engage à recueillir le *consentement** préalable de la *personne concernée** notamment :
- en cas de *collecte** de *données sensibles** ;
- de réutilisation des données à d'autres fins ;
- d'utilisation de cookies pour certaines *finalités** ;
- d'utilisation des données à des fins de prospection commerciale.

FAQ. Une partie explicative sur le droit des personnes est disponible dans la FAQ.

11.2 Quels sont les droits des personnes concernées ?

Articles 15 à 18 et 20 à 21 du RGPD

74. Chaque entité s'engage à donner aux personnes concernées les moyens d'exercer leurs droits.

75. Les personnes concernées ont le droit d'accéder aux données qui les concernent et d'en demander l'accès, la rectification ou l'effacement dans certains cas.

76. Ces personnes peuvent également s'opposer au traitement notamment à des fins de prospection commerciale. Sous certaines conditions, les personnes concernées ont le droit d'obtenir la limitation du traitement et la portabilité de leurs données.

77. Chaque entité s'engage à respecter les droits des personnes concernées et à répondre dans les meilleurs délais aux demandes qui lui sont adressées en faisant remonter toute demande à son référent protection des données.

FAQ. Une partie explicative sur le droit des personnes est disponible dans la FAQ.

11.3 Comment prendre en compte les directives d'une personne sur ses données après son décès ?

Article 40-1 Loi 78-17 du 6 janvier 1978

78. Chaque entité s'engage à permettre aux personnes concernées de donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès.

12 Comment limiter la durée de conservation des données ?

Article 5 du RGPD

79. Chaque entité s'engage à limiter la *durée de conservation** des données.

Exemple. Au vu des exigences du règlement européen et de la loi Informatique et libertés il semble difficile de maintenir un droit de conservation de longue durée à hauteur de 99 ans pour une application du concept de marque transgénérationnelle.

Exemple. La durée légale du livre de police est de 6 ans.
Au-delà de la durée nécessaire à la *finalité** du traitement, lorsqu'elles présentent encore un intérêt administratif pour l'entité, les données pourront être conservées en **archives intermédiaires**.

Cette conservation des données en archives intermédiaires (avec des accès limités) peut tout d'abord être justifiée par l'observation des **durées légales de prescription** définies par la réglementation en matière civile, commerciale, fiscale, pénale et sociale.

La *durée de conservation** sera par conséquent la durée légale de 6 ans augmentée de la durée de la prescription applicable.

Exemple. En cas de régularisation de l'impayé, les informations relatives à la *personne concernée** doivent être effacées du fichier **au plus tard dans les 48 heures à partir du moment où la personne vous notifie qu'elle vous a payé la somme due** ;

En cas de non-régularisation, les informations ne peuvent être conservées dans le fichier que pour une durée limitée dans la limite de **3 ans à compter de la survenance de l'impayé**, sauf à justifier (par écrit et de manière étayée) de la nécessité de garder les informations plus longtemps.

La durée de prescription légale applicable peut justifier la nécessité de gardes les informations pour une durée plus longue.

FAQ. La FAQ précise comment encadrer le fichier dit de « mauvais payeur ».

Exemple. Les données traitées pour gérer un précontentieux doivent être supprimées dès le règlement amiable du litige ou, à défaut, dès la prescription de l'action en justice correspondante.

Les données traitées pour gérer un contentieux doivent être supprimées lorsque les recours ne sont plus possibles contre la décision rendue pour la faire exécuter.

A l'expiration du délai de prescription, les données sont supprimées de manière sécurisée ou archivées dans les conformément à la délibération de la Commission n° 2005-213 du 11 octobre 2005 concernant l'archivage électronique pour les organismes du secteur privé.

Les décisions prononcées peuvent être conservées par le *responsable du traitement** à titre d'archive définitive en raison d'un intérêt historique.

FAQ. La FAQ précise comment encadrer les données relatives au suivi du contentieux.

12.1 Quelles sont les durées de conservation relatives à la gestion des fichiers de clients et de prospects ?

80. Chaque entité s'engage à ne pas conserver les *données à caractère personnel** relatives aux clients au-delà de la **durée strictement nécessaire à la gestion de la relation commerciale**.

81. Toutefois, pour les données permettant d'établir la preuve d'un droit ou d'un contrat, ou conservées au titre du respect d'une obligation légale, chaque entité pourra effectuer une politique **d'archivage intermédiaire pour une durée n'excédant pas la durée nécessaire aux *finalités** pour lesquelles elles sont conservées**, conformément aux dispositions en vigueur.

82. Pour pouvoir conserver, **au-delà de la *durée de conservation** fixée par la réglementation en vigueur**, chaque entité s'engage à **anonymiser les données de manière irréversible**, en procédant à la purge de toutes les *données à caractère personnel**, y compris les données indirectement identifiantes.

83. Chaque entité s'engage à ne conserver les données des clients utilisées à des fins de prospection commerciale que pendant un **délai de trois ans à compter de la fin de la relation commerciale**.

84. Chaque entité s'engage à ne conserver les *données à caractère personnel** relatives à un prospect non client que pendant un délai de trois ans à compter de leur *collecte** par le *responsable du traitement** ou du dernier contact émanant du prospect.

85. Au terme de ce délai de trois ans, le *responsable du traitement** de chaque entité pourra reprendre contact avec la *personne concernée** afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales.

86. En l'absence de réponse positive et explicite de la personne, chaque entité s'engage à supprimer les données ou les archiver conformément aux dispositions en vigueur.

12.2 Quelles sont les durées de conservation concernant les pièces d'identité ?

87. Lorsque les données relatives aux pièces d'identité sont conservées par le *responsable du traitement**, or **obligation de tenue du registre de police**, **en cas d'exercice du *droit d'accès** ou de *rectification**, chaque entité s'engage à ne conserver les données relatives aux pièces d'identité que pendant le délai prévu à l'article 9 du code de procédure pénale (**soit un an**). En cas d'exercice du droit d'opposition, ces données peuvent être archivées par chaque entité pendant le délai de prescription prévu à l'article 8 du code de procédure pénale (**soit trois ans**).

12.3 Quelles sont les durées de conservation concernant les données relatives aux cartes bancaires ?

88. Chaque entité s'engage à supprimer les données relatives aux cartes bancaires une fois la transaction réalisée, c'est-à-dire dès son paiement effectif, qui peut être différé à la réception du bien, augmenté, le cas échéant, du délai de rétractation prévu pour les contrats conclus à distance et hors établissement, conformément à l'article L. 221-18 du Code de la consommation.

89. Dans le cas d'un paiement par carte bancaire, le numéro de la carte et la date de validité de celle-ci pourra être conservés par chaque entité pour une *finalité** de preuve en cas d'éventuelle contestation de la transaction, en archives intermédiaires pour une durée de treize mois suivant la date de débit. Ce délai pourra être étendu à quinze mois afin de prendre en compte la possibilité d'utilisation de cartes de paiement à débit différé.

90. Chaque entité s'engage à ce que ces données soient utilisées uniquement en cas de contestation de la transaction et que la conservation de ces donnes à cette fin fasse l'objet de mesures de sécurité.

91. Les données relatives aux cartes bancaires pourront être conservées plus longtemps sous réserve d'obtenir le *consentement** exprès du client, préalablement informé de l'objectif poursuivi.

92. La *durée de conservation** ne saurait alors excéder la durée nécessaire à l'accomplissement de la *finalité** visée par le traitement.

93. Chaque entité s'engage à ce que le *consentement** prenne la forme d'un acte de volonté explicite et pouvant être recueilli par l'intermédiaire d'une case à cocher et non pré-cochée par défaut ni résulter de l'acceptation de conditions générales.

94. De manière générale, chaque entité s'engage à ce que les données relatives au cryptogramme visuel ne soient pas conservées au-delà du temps nécessaire à la réalisation de chaque transaction, y compris en cas de paiements successifs ou de conservation du numéro de la carte pour les achats ultérieurs.

95. Chaque entité s'engage lorsque la date d'expiration de la carte bancaire est atteinte, à supprimer les données relatives à celles-ci.

12.4 Quelles sont les durées de conservation concernant la gestion des listes d'opposition à recevoir de la prospection ?

96. Lorsqu'une personne exerce son droit d'opposition à recevoir de la prospection auprès d'un *responsable du traitement**, chaque entité s'engage à conserver au minimum trois ans à compter de l'exercice du droit d'opposition les informations permettant de prendre en compte son droit d'opposition.

97. Chaque entité s'engage à ce que ces données ne puissent en aucun cas être utilisées à d'autres fins que la gestion du droit d'opposition et seules les données nécessaires à la prise en compte du droit d'opposition seront conservées.

12.5 Quelles sont les durées de conservation concernant les statistiques de mesure d'audience ?

98. Chaque entité s'engage à ne conserver pas les informations stockées dans le terminal des utilisateurs (ex : cookies), ou tout autre élément utilisé pour identifier les utilisateurs et permettant leur traçabilité, au-delà de treize mois. Les nouvelles visites ne doivent pas prolonger la durée de vie de ces informations.

99. Chaque entité s'engage à ne pas conserver les données de fréquentation brutes associant un identifiant plus de treize mois. Au-delà de ce délai, chaque entité s'engage à supprimer les données ou les anonymiser.

13 Quelles sont les mesures techniques et organisationnelles de sécurité appropriées ?

Article 25 et 32 du RGPD

100. Chaque entité s'engage à mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque.

101. Chaque entité doit protéger ses fichiers et sécurisez les données.

102. Les *données à caractère personnel** traiter par chaque entité doivent rester confidentielles. Chaque entité doit prendre soin de ne pas divulguer ces informations auprès d'autres services ou auprès de *tiers** qui ne seraient pas habilités à en prendre connaissance.

103. Chaque entité s'engage à mettre en place des moyens pour garantir la confidentialité, l'intégrité, la disponibilité et la solidité constantes des systèmes et des services de traitement.

104. Si une entité a besoin de sous-traiter une partie ou la totalité de la mise en œuvre d'un traitement, il doit imposer contractuellement au sous-traitant des obligations fortes de sécurité et de confidentialité des données.

105. Chaque entité s'engage à ce que les responsables du traitement prennent toutes précautions utiles pour préserver la sécurité des données et empêcher qu'elles soient déformées ou endommagées ou que des *tiers** non autorisés y aient accès.

13.1 Comment adopter une démarche de protection des données dès la conception ?

106. La démarche intégrale de *protection des données dès la conception** est présentée dans le kit de mise en conformité étape par étape.

13.2 Quels sont vos obligations de notification des violations de données à caractère personnel ?

Article 33 du RGPD

107. Dès lors qu'un incident menaçant la sécurité des données entraîne la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés aux données, la violation de *données à caractère personnel** est constituée. Peu importe notamment que la violation soit accidentelle ou illicite.

108. Chaque entité s'engage à notifier la violation de données :

- la notification des violations à *l'autorité de contrôle** sous 72 heures au plus tard après en avoir pris connaissance ;
- la communication des violations aux personnes concernées dans les meilleurs délais.

109. Une très grande réactivité est nécessaire en cas de violation de *données à caractère personnel**, qu'il s'agisse de résoudre l'incident ou de notifier et communiquer sur la violation.

14 Etes-vous en présence de flux de données hors de l'Union européenne ?

Article 44 et 46 du RGPD

110. Chaque entité s'engage à maîtriser les flux de *données à caractère personnel**.

111. Chaque entité s'engage à ne transférer des *données à caractère personnel** vers un autre pays qu'après avoir vérifié auprès de son référent protection des données dans quelles conditions il est autorisé à le faire.

FAQ. Une liste des pays offrant une protection adéquate aux *données à caractère personnel** transférés est disponible dans la FAQ.

15 Quelles sont vos obligations lorsque vous êtes responsable du traitement ?

15.1 Disposez-vous d'un registre à jour des activités de traitement ?

Article 30 du RGPD

112. Chaque entité s'engage à tenir un registre :

- si l'entreprise fait moins de 250 salariés et que le traitement qui n'est pas occasionnel comporte un risque pour les droits et libertés des personnes concernées ;
- si l'entreprise fait moins de 250 salariés et que le traitement porte sur les *donnée particulières** ;
- si l'entreprise fait moins de 250 salariés et porte notamment sur des données relatives à des condamnations pénales et des infractions.

113. Lorsque l'entité doit tenir un registre, il doit comprendre les informations suivantes :

- le nom et les coordonnées du *responsable du traitement** pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du *délégué à la protection des données**;
- les catégories de traitements effectués pour le compte du responsable du traitement ;
- le cas échéant, les transferts de *données à caractère personnel** vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
- la *pseudonymisation** et le chiffrement des *données à caractère personnel**;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des *données à caractère personnel** et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

FAQ. Un modèle de registre est disponible dans la FAQ.

15.2 Comment analyser l'impact sur la vie privée des données collectées ? (Analyse d'impact)

Article 35 du RGPD

114. Chaque entité s'engage à consulter la liste de *l'autorité de contrôle** indiquant les traitements pour lesquels une analyse d'impact doit être menée.

Exemple.
L'analyse d'impact est en particulier requise dans les cas suivants :

- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le *profilage**, et sur la base

de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- le traitement à grande échelle de *catégories particulières de données** visées à ou de *données à caractère personnel** relatives à des condamnations pénales et à des infractions,
- la surveillance systématique à grande échelle d'une zone accessible au public c'est-à-dire la vidéosurveillance d'un lieu public.

D'autres exemples complètent cette liste :
- évaluation d'aspects personnels ou de comportements relatifs aux individus (par exemple *profilage** et l'étude de marché) ;
- traitement des données personnelles en masse (en termes de volume de données, de nombre de personnes concernées, de durée et de permanence ou d'étendue géographique) ? ;
- utilisation de nouvelles technologies (par exemple certaines application associés à des objets connectés) pouvant être perçue comme intrusives ;
- fichiers de données ayant été jumelés ou combinés ;
- données de personnes concernées vulnérables ;
- transfert de données avec des pays en dehors de l'Union Européenne ;
- le traitement lui-même empêche les individus concernés d'exercer un droit.

115. Chaque entité s'engage à effectuer une analyse d'impact des opérations de traitement envisagées avant le traitement, quand elle est requise, et que le traitement peut engendrer un risque élevé pour les droits et libertés.

FAQ. Un outil d'analyse d'impact est présenté dans la FAQ.

16 A quelles sanctions vous exposez-vous en cas de non-respect des exigences de la réglementation sur les données à caractère personnel ?

116. Tout manquement à l'une des obligations prévues par la réglementation en vigueur est susceptible non seulement d'engager votre responsabilité, celle du groupe auquel votre société appartient, mais également d'altérer gravement votre image et/ou celle du groupe.

117. Chaque membre s'engage en conséquence à respecter le présent code qui a pour vocation de permettre le respect de l'ensemble des obligations issues de la réglementation en vigueur, sans en créer de nouvelles.

16.1 Quelles sont les sanctions prévues dans le règlement ?

118. La sanction pour la violation des dispositions du Règlement n°2016/679 (RGPD) est un paiement d'une amende qui peut s'élever à :

- un montant de 10 000 000 euros ou 2% du chiffre d'affaire annuel mondial en cas de :
  - absence de *protection des données dès la conception** et *protection des données par défaut** ;
  - absence de représentant établi dans l'Union ;
  - absence de registre des activités de traitement ;
  - absence de coopération avec *l'autorité de contrôle** ;
  - absence de notification à *l'autorité de contrôle*(Cnil*)*
  - ou à la *personne concernée** d'une *violation des données** ;
  - absence d'analyse d'impact.

- un montant de 20 000 000 euros ou 4% du chiffre d'affaire annuel mondial en cas de :
  - non-respect des principes de base d'un traitement (licéité, loyauté, légitimité adéquation, et pertinence des données, *consentement**, *données sensibles**…) ;

- non-respect du droit des personnes ;
- non-respect des règles relatives aux transferts de *données à caractère personnel**.

16.2 La Cnil peut-elle effectuer des contrôles ?

119.. La *Cnil** dispose, de par la loi, d'un pouvoir de contrôle sur place, par audition et en ligne, d'injonction et de sanctions administratives.

120. **Toute entrave** à l'exercice par la *Cnil** de sa mission constitue un délit sanctionné pénalement.

121. Toute violation du règlement est pénalement sanctionnée.

122. L'action de groupe en matière de protection des données personnelles est désormais possible en droit français.

123. Le projet de loi français relatif à la protection des données personnelles[4], précise en son article 43 que l'action de groupe peut être exercé en vue de :

- la cessation du manquement, tel que l'arrêt d'un traitement illicite ;
- l'engagement de la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation du préjudice des personnes concernées.

17 Gouvernance

124. Le code a été adopté par Gitec Human Resources.

125. Le code de conduite se substitue à tout autre *code de conduite** existant préalablement.

126. Le groupe de travail permettra d'encadrer la gestion du *code de conduite**. Un membre de chaque fédération composera le groupe de travail. Au moins 10% des participants du groupe de travail peuvent réaliser et adopter des modifications du code de conduite.

18 Quels sont les textes applicables ?

127. Des textes légaux et réglementaires sont applicables aux activités de Gitec Human Resources dont notamment :

- la loi dite « Informatique et Libertés » n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

- le RGPD : Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques.

[4] Projet de loi relatif à la protection des données personnelles, adopté en 1ère lecture par l'Assemblée nationale le 13 février 2018.