NEWSLETTER #18 | Septembre 2017 • Monaco-UE / Données personnelles-IT

Le Règlement (UE) 2016/79 sur la protection des données personnelles (GDPR) : pourquoi les entreprises à Monaco doivent s'y préparer

À partir du 25/05/2018, le Règlement général sur la protection des données ou *General Data Protection Regulation* (GDPR)* de l'Union européenne remplacera la Directive 95/46/CE et les lois nationales de transposition des États-membres.

Il serait faux de déduire du fait que la Principauté de Monaco est un État-tiers à l'UE, que les entreprises monégasques ne sont pas concernées par le GDPR.

Le GDPR (ensemble 173 considérants et 99 articles) est applicable aux entreprises établies en dehors de l'UE qui traitent des données personnelles des personnes physiques dans l'UE pour leur offre de biens ou de services à ces personnes, ou pour le suivi du comportement de ces personnes au sein de l'UE.

Les professionnels concernés de la place doivent se familiariser avec le GDPR, qui introduit des principes et exigences inconnus de la Loi n° 1.165 du 23/12/1993 relative à la protection des informations nominatives.

La violation du GDPR est passible d'une amende administrative pouvant atteindre 20.000.000 € ou 4 % du chiffre d'affaires annuel mondial.

* Règlement (UE) 2016/79 du Parlement européen et du Conseil du 27/04/2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

Les entreprises concernées par le GDPR

Sont concernées par le GDPR les entreprises qui traitent (en qualité de responsable du traitement[1] ou de sous-traitant[2]) des données personnelles de personnes physiques[3] dans le cadre des activités d'un établissement[4] sur le territoire de l'UE, que le traitement lui-même ait ou non lieu dans l'UE.[5]

Sont également soumises au GDPR les entreprises établies hors du territoire de l'UE qui traitent (en qualité de responsable du traitement ou de sous-traitant) des **données à caractère personnel relatives à des personnes physiques qui se trouvent dans l'UE** lorsque :

- les activités de traitement sont liées à l'**offre de biens ou de services** à ces personnes, qu'un paiement soit ou non exigé ;
- le traitement est lié au **suivi du comportement** de ces personnes **qui a lieu au sein de l'UE**.[6]

Pour déterminer si le GDPR est applicable à une entreprise monégasque, il convient en particulier de se demander si elle :

- a un bureau, une succursale ou une filiale établie en UE ;
- réalise ses activités de traitement (en tout ou partie) dans un État membre de l'UE ;
- offre des biens ou services via un site Internet en ciblant le marché européen (possibilité de les commander dans des langues d'usage courant en UE, mention de clients ou d'utilisateurs qui se trouvent dans l'UE) ;
- suit sur Internet le comportement des personnes physiques qui se trouvent dans l'UE pour prendre des décisions les concernant, ou pour analyser ou prédire leurs dispositions d'esprit, comportements, préférences (profilage) ;
- traite des données personnelles pour le compte d'un tiers soumis au GDPR pour les activités concernées (envoi de bulletins de paie, services d'hébergement, services Cloud, maintenance informatique, etc.).

La (sous-)sous-traitance fortement impactée par le GDPR

Le GDPR organise un **régime de sous-traitance** distinct des devoirs de sécurité, y compris la **sous-traitance secondaire** (sous-traitance par le sous-traitant direct du responsable du traitement).

Le principe demeure celui d'une organisation contractuelle spécifique entre le responsable du traitement et le sous-traitant, mais le GDPR élargit le contenu du contrat écrit (y compris sous format électronique).[7]

1 La personne physique ou morale qui seule, ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (Article 4, 7).

2 La personne physique ou morale qui traite des données personnelles pour le compte du responsable du traitement (Article 4, 8).

3 Le traitement des données personnelles des personnes morales n'entre pas dans le champ d'application du GDPR. Celui-ci protège les personnes physiques (salariés, clients, etc.) indépendamment de leur nationalité.

4 *« L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable »* (Cons. 22). Voir CJUE, 3e ch., 01/10/2015, *Weltimmo s.r.o. c/ Nemzeti Adatvédelmi és Információszabadság Hatóság*, Aff. C-230/14.

5 Article 3, § 1 GDPR.

6 Article 3, § 2 GDPR.

7 Article 28 GDPR.

Les contrats de prestation de services qui incluent de simples mentions générales (comme le fait pour le sous-traitant de ne pouvoir agir que sur les instructions du responsable du traitement) et un rappel des devoirs de sécurité s'imposant au sous-traitant, sont insuffisants au regard du GDPR.

Le sous-traitant ne peut plus fournir des services sans connaître les traitements auxquels il prend part, et ses obligations à l'égard du responsable du traitement sont alourdies.

Le contrat de sous-traitance doit prévoir (de manière non exhaustive) :

- des **informations sur le traitement** (finalité, objet et durée, etc.) ;
- le traitement des données sur la seule instruction du responsable du traitement qui doit être **documentée** (notamment en matière de sécurité et de confidentialité), y compris le **transfert des données vers des pays tiers**[8] ;
- la garantie que les personnes autorisées à traiter les données (salariés, consultants, etc.) respectent la **confidentialité** ;
- le respect des **conditions de recrutement d'un sous-traitant secondaire** ;
- la **collaboration avec le responsable du traitement** pour l'aider à donner suite à l'exercice des droits des personnes concernées (accès, effacement, portabilité, etc.), à garantir le respect de ses propres obligations de sécurité, à démontrer le respect des obligations de sous-traitance, pour permettre la réalisation d'audits, etc. ;
- les **obligations après l'exécution du service**, au choix du responsable du traitement, d'effacement ou de restitution des données, etc.[9]

La faculté du sous-traitant de lui-même sous-traiter doit faire l'objet d'une autorisation écrite préalable (spécifique ou générale[10]) du responsable du traitement. Le contrat de sous-traitance secondaire doit obéir aux règles de contenu applicables au contrat de sous-traitance directe. Le sous-traitant initial est responsable devant le responsable du traitement de la mauvaise exécution des obligations contractuelles de ses propres sous-traitants.

Lorsqu'en violation du contrat conclu avec le responsable du traitement, le sous-traitant réutilise les données personnelles qui lui sont confiées pour mettre en œuvre un traitement dont il est seul à définir la finalité et les moyens, il est considéré comme le responsable de ce traitement.[11]

Une logique de conformité fondée sur l'*accountability*

Les responsables du traitement et les sous-traitants monégasques soumis au GDPR doivent se familiariser avec une nouvelle logique de conformité fondée sur le principe d'*accountability*, et avec de nouveaux outils.

8 Si le sous-traitant est légalement tenu de procéder au transfert hors de l'UE, il en doit en informer le responsable du traitement sous réserve que cela ne soit pas interdit pour des motifs importants d'intérêt public.

9 Le GDPR prévoit la possibilité d'utiliser des clauses contractuelles types (fournies par la Commission européenne ou par les autorités de contrôle, ou incluses dans une procédure de certification).

10 Si générale, le sous-traitant doit donner au responsable du traitement la possibilité d'émettre des objections (information sur tout changement de sous-traitant secondaire).

11 Article 28, § 10 GDPR. Le sous-traitant encourt par ailleurs des sanctions pénales et administratives (Articles 82 à 84 GDPR).

Le GDPR équilibre la relation et les responsabilités entre le responsable du traitement et le sous-traitant.

Le sous-traitant n'est plus à l'abri des sanctions infligées par l'autorité de contrôle. Outre ses obligations contractuelles renforcées, le sous-traitant a des obligations directes à sa charge dont il doit lui-même répondre devant l'autorité de contrôle en cas de manquement.

Les responsables du traitement ainsi que les sous-traitants doivent être en mesure de démontrer l'efficacité des **mesures techniques et organisationnelles** (y compris des politiques) prises pour garantir un niveau de sécurité adapté au risque et la conformité du traitement au GDPR. L'application d'un code de conduite approuvé[12] ou de mécanismes de certification approuvés[13] par une autorité de contrôle constitue un élément de garantie (connaissance du domaine d'intervention, fiabilité, ressources, etc.) et de preuve du respect du GDPR.[14]

La protection des données personnelles doit être **proactive, préventive et automatique** : les mesures ne doivent pas être seulement mises en œuvre au moment du traitement, mais aussi dès la détermination des moyens du traitement (*data protection by design*), et doivent s'appliquer aux paramétrages par défaut (*data protection by default*). Le GDPR recommande la **pseudonymisation** (qui permet de ne plus pouvoir associer des données à une personne physique déterminée sans recourir à des informations supplémentaires) et la **minimisation** (qui permet de ne traiter que des données adéquates, pertinentes et limitées à la finalité du traitement).[15]

Le GDPR met fin aux déclarations ou autorisations préalables à la mise en œuvre du traitement[16], qu'il remplace par un régime d'autorégulation dont les mécanismes ciblent les traitements susceptibles de présenter des risques particuliers pour les droits et libertés[17] des personnes concernées.

La tenue d'un Registre des activités de traitement[18] sous forme écrite (y compris électronique) est généralisée. Elle s'impose aux responsables du traitement et aux sous-traitants (et leurs représentants le cas échéant) :

- qui emploient 250 personnes et plus ;
- quel que soit le nombre d'employés, lorsque le traitement est à risque pour les droits et les libertés des personnes concernées, s'il est récurrent ou s'il porte sur des données sensibles[19] ou relatives à des condamnations ou infractions pénales.

Une Analyse d'impact relative à la protection des données (DPIA)[20] est requise lorsque le traitement est susceptible d'engendrer un risque **élevé** pour les droits et libertés des personnes concernées (sauf si le traitement de ces données est protégé par le secret professionnel[21]), par exemple :

- traitement à grande échelle des données sensibles ou relatives à des condamnations et à des infractions pénales ;
- évaluation systématique et approfondie d'aspects personnels des personnes physiques fondée sur un traitement automatisé, y compris

12 Articles 40 et 41 GDPR. Le GDPR encourage leur élaboration en fonction de la spécificité des secteurs de traitement des données, et des besoins spécifiques des entreprises selon leur taille.

13 Articles 42 et 43 GDPR.

14 Articles 24 et 32 GDPR (procédures internes de garantie lors de la création ou la modification du traitement, inventaire des traitements, répartition des rôles et responsabilités, sensibilisation et formation du personnel, vérification de l'efficacité des mesures par des audits et contrôles, transparence sur les politiques de confidentialité et la gestion interne des plaintes, voire désignation d'un délégué à la protection des données).

15 Article 25 GDPR. La protection, **intégrale** (jusqu'à la conservation et la destruction des données), doit être **intégrée** dans la conception et l'architecture des systèmes informatiques et les pratiques de l'entreprise afin de prévoir et prévenir les incidents. Le GDPR vise les identifiants en ligne (adresses IP, cookies, étiquettes d'identification par radiofréquence) dont l'association aux identifiants uniques et à d'autres informations reçues par les serveurs (par les appareils, applications, outils et protocoles) peuvent servir à créer des profils et à identifier les personnes physiques (Cons. 30 GDPR).

16 Toutefois, un régime de consultation préalable s'applique aux **traitements soumis à une analyse d'impact** (Articles 35 et 36 GDPR). Voir *infra*.

17 Le Groupe de travail de l'article 29 (G29) a précisé qu'il s'agit du droit à la vie privée, de la liberté d'expression, de pensée, d'aller et venir, de conscience et de religion, de la non-discrimination. Voir *infra* note 20.

18 Article 30 GDPR.

19 Données qui révèlent l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données concernant la santé ou l'orientation sexuelle, les données génétiques ou biométriques (Article 9, § 1 GDPR). Le G29 inclut également les données de communication électronique, de géolocalisation, financières, d'activités personnelles dont la divulgation pourrait être considérée comme intrusive tels les agendas, documents, courriers électroniques hébergés par des services Cloud. Voir *infra* note 20.

20 Article 35 GDPR et Lignes directrices du G29 : Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is « likely to result in a high risk » for the purposes of Regulation 2016/679, 04/04/2017, WP 248.

21 Cons. 91 GDPR (données patients ou clients traitées par un médecin, professionnel de santé ou avocat exerçant à titre privé). D'autres exceptions s'appliquent (traitement régi par une base légale, etc.).

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 ;

– surveillance systématique à grande échelle d'une zone accessible au public (vidéosurveillance, etc.).[22]

La désignation d'un Délégué à la protection des données (DPO)[23] chargé de mettre en œuvre la conformité au GDPR (membre du personnel ou externe) est obligatoire pour les entreprises (responsable du traitement et sous-traitant) dont les activités de base[24] consistent en :

– des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;

– un traitement à grande échelle de données sensibles et relatives à des condamnations et infractions pénales.[25]

Un Groupe d'entreprises (entreprise qui exerce le contrôle et entreprises qu'elle contrôle[26]) peut désigner un Délégué unique.

Le G29 recommande de documenter l'analyse interne visant à déterminer si un Délégué doit être ou non désigné, et encourage la désignation volontaire.

En cas d'**application extraterritoriale du GDPR**, les responsables du traitement et les sous-traitants établis hors UE ont l'obligation de désigner par convention écrite un représentant (personne physique ou morale) établi dans l'UE[27] lorsque le traitement est :

– récurrent ;

– occasionnel s'il implique de traiter à grande échelle des données sensibles ou relatives à des condamnations et infractions pénales, et est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, compte tenu de la nature, du contexte, de la portée et des finalités du traitement.

Le GDPR prévoit l'obligation du **responsable du traitement** de notification à l'autorité de contrôle d'une violation de données personnelles[28] (violation de la sécurité qui entraîne de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée des données transmises, conservées ou autrement traitées, ou l'accès non autorisé aux données)[29] dans les meilleurs délais et si possible au plus tard 72 h après en avoir eu connaissance[30], sauf si elle ne paraît pas faire courir de risque pour les droits et libertés des personnes physiques.

Le **sous-traitant** doit quant à lui notifier toute violation au responsable du traitement, dans les meilleurs délais après en avoir eu connaissance.

Une trace documentée de chaque violation indiquant son contexte, ses effets et les mesures prises pour y remédier doit être conservée, qu'elle donne ou non lieu à notification.

22 Le G29 y ajoute les cas de transfert de données personnelles hors de l'UE, et des personnes concernées vulnérables (enfants, mais aussi salariés ce qui soulève la question des conditions de mise en œuvre d'une SIRH).

23 Articles 37 à 39 GDPR, et Lignes directrices du G29 : Guidelines on Data Protection Officers (DPO's), révisées le 05/04/2017, 16/EN, WP 243 rev.01. Le GDPR précise les compétences professionnelles requises, le statut et la fonction du DPO.

24 Dans le secteur privé, les activités de base correspondent aux activités principales. Le traitement des données en tant qu'activité auxiliaire n'est pas concerné (Cons. 97 GDPR). Le G29 précise que la notion d'activité de base ne devrait pas être exclue si l'activité consiste intrinsèquement à traiter des données à caractère personnel (comme par exemple une société de surveillance chargée d'assurer la sécurité d'un centre commercial ou d'un lieu ouvert au public).

25 Le droit de l'UE ou des États-membres peut exiger la désignation d'un DPO dans d'autres cas. Les opérations de traitement à grande échelle s'évaluent au regard du volume considérable de données traitées, de l'étendue géographique (régionale, nationale, supranationale), du nombre de personnes concernées susceptibles d'être affectées, etc. (Cons. 91 GDPR). Le traitement de données personnelles de patients, clients par un médecin, professionnel de santé ou avocat exerçant à titre privé n'est pas considéré à grande échelle.

26 Article 4, 19) GDPR.

27 Article 27 GDPR. Le représentant mandaté doit être établi dans un des États membres où se trouvent les personnes physiques concernées (dont les données font l'objet d'un traitement lié à l'offre de biens ou services, ou dont le comportement est suivi). La tenue d'un Registre des activités de traitement lui incombe également. Interlocuteur de l'Autorité de contrôle, il peut faire l'objet de mesures coercitives en cas de non-respect du GDPR par le responsable du traitement ou le sous-traitant (Cons. 80 GDPR).

28 Article 33 GDPR.

29 Article 4, 12) GDPR.

30 Il est tenu compte de la nature et de la gravité de la violation, de ses conséquences et effets négatifs pour la personne concernée (Cons. 87).

La mise à jour des transferts (y compris ultérieurs) hors de l'UE

Le GDPR instaure un droit de suite inédit : les transferts des données personnelles vers les pays tiers à l'UE ne peuvent avoir lieu que si le responsable du traitement et le sous-traitant qui tombent sous son champ d'application respectent les règles du chapitre V[31] pour les **traitements en cours ou prévus, mais aussi les transferts ultérieurs au départ du pays tiers vers un autre pays tiers**.[32]

Les transferts vers les pays tiers ayant fait l'objet d'une décision de la Commission européenne constatant un **niveau adéquat de protection** des données personnelles (dont elle publie la liste) peuvent avoir lieu sans autorisation spécifique.[33]

En l'absence de décision d'adéquation, les transferts hors UE doivent être automatiquement couverts par des garanties appropriées en faveur de la personne concernée pour compenser l'insuffisance de la protection. Le GDPR étoffe le choix des outils, tout en confortant ceux existants.[34]

La mise en place des garanties suivantes s'opère **sans autorisation particulière de l'autorité de contrôle** :

- Règles d'entreprises contraignantes approuvées par l'autorité de contrôle et répondant aux exigences de l'article 47 GDPR (transferts intra-groupes) ;[35]
- Clauses contractuelles types de protection des données adoptées par la Commission européenne, ou par une autorité de contrôle et approuvées par la Commission européenne ;
- Code de conduite approuvé ;
- Mécanisme de certification approuvé attestant de la conformité aux règles de l'UE.

Les garanties peuvent être également fournies **sous réserve de l'autorisation de l'autorité de contrôle** par d'autres clauses contractuelles (non types) entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données dans le pays tiers.

En l'absence de garanties visées ci-dessus, des **dérogations particulières** peuvent s'appliquer.[36]

Celles-ci sont classiques mais adaptées (consentement explicite au transfert – transfert nécessaire à la conclusion ou l'exécution d'un contrat, mesures précontractuelles – motifs importants d'intérêt publics – constatation, exercice ou défense d'un droit en justice – sauvegarde de l'intérêt vital – transfert au départ d'un registre public), avec une nouvelle dérogation dont le recours est strictement encadré (nécessité du transfert aux fins des intérêts légitimes impérieux du responsable du traitement).

31 Articles 44 à 50 GDPR.

32 Article 44 GDPR.

33 Article 45 GDPR.

34 Article 46 GDPR.

35 Les *Binding Corporate Rules* (BCR) déjà adoptées doivent être revues, étant donné le contenu obligatoire élargi par l'Article 47 BCR : caractère juridiquement contraignant pour les entités du groupe et leurs employés ; droits opposables des personnes concernées concernant le traitement de leurs données ; structure et coordonnées ; application des principes généraux de protection des données ; droit des personnes concernées et manière de les exercer ; acceptation par le responsable ou le sous-traitant établi sur le territoire de l'UE de voir sa responsabilité engagée pour toute violation des BCR par toute entité concernée non établie dans l'UE à moins qu'il ne prouve que le fait générateur du dommage n'est pas imputable à l'entité en cause ; missions du DPO ou de toute personne chargée de la surveillance du respect des BCR.

36 Article 49 GDPR.

La responsabilité renforcée à l'égard des personnes physiques

S'agissant des traitements fondés sur le consentement de la personne physique concernée, le responsable du traitement a la **charge de la preuve du consentement**, qui doit être donné par un **acte positif clair** (déclaration écrite y compris par voie électronique, ou orale) par lequel la personne concernée manifeste son accord de façon **libre, spécifique, éclairée et univoque**. Il ne peut y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité.[37]

Le GDPR instaure une nouvelle règle lorsque le consentement au traitement des données personnelles est requis dans le contexte d'une **déclaration écrite qui concerne également d'autres questions**. La demande relative au consentement doit être présentée sous une forme qui la distingue clairement de ces autres questions, d'une façon compréhensible et aisément accessible, en des termes clairs et simples. Le consentement à des conditions générales contenant une acceptation de traitement serait ainsi insuffisant au sens du GDPR.

La personne concernée doit pouvoir **retirer son consentement** à tout moment pour un traitement futur, de manière aussi simple que celle de donner son consentement.

Le GDPR innove en posant des conditions spécifiques au **consentement des enfants** (moins de 16 ou 13 ans, selon le droit de l'Etat membre de l'UE) **dans le cadre de l'offre directe de services de la société de l'information**. Le responsable du traitement doit obtenir le consentement du titulaire de la responsabilité parentale.[38]

Le responsable du traitement doit donc :

- prévoir un archivage dans son processus de traitement pour ménager la preuve du consentement ;
- exclure les consentements tacites ou passifs ;
- considérer le consentement au traitement des données personnelles indépendamment du consentement contractuel ;
- informer et faciliter l'exercice du droit de retirer son consentement ;
- pour les traitements des données relatives aux enfants, faire des efforts raisonnables compte tenu des moyens technologiques disponibles, pour vérifier que le consentement est donnée ou autorisé par le titulaire de la responsabilité parentale.

Le GDPR repose sur le principe de transparence, qui implique que le responsable du traitement prenne des mesures appropriées pour mettre à disposition une information concise, facile à comprendre, aisément accessible, formulée en des termes clairs et simples, voire illustrée à l'aide d'éléments visuels s'il y a lieu[39]. Celui-ci s'applique :

- aux **informations à fournir** à la personne physique concernée[40] ;

37 Article 7 GDPR et Considérant 32.

38 Article 8 GDPR et Considérant 38. Sont en particulier visées : l'utilisation de données à des fins de marketing ou de création de profils d'utilisateur ou de personnalité, la collecte de données lors de l'ouverture de comptes Facebook, Instagram Snapchat, etc. Les législations nationales en matière contractuelle qui comprendraient des règles spécifiques concernant notamment la validité, la formation ou les effets d'un contrat à l'égard d'un enfant, ne sont pas affectées.

39 Article 12 et Cons. 58 GDPR.

40 Articles 13 et 14 GDPR.

– à l'**exercice des droits** d'accès[41], de rectification[42], à l'effacement (droit à l'oubli)[43], à la limitation du traitement[44], à la portabilité des données[45], d'opposition[46], de ne pas être soumis à une décision individuelle automatisée y compris le profilage[47] ;

– à l'**obligation de notification** en ce qui concerne la rectification ou l'effacement des données ou la limitation du traitement[48] ;

– à la **communication d'une violation des données personnelles** à la personne concernée[49].

Les professionnels doivent se familiariser avec les obligations renforcées ou nouvelles à l'égard des personnes physiques.

Les éléments d'information à fournir à la personne concernée sont plus nombreux, que les données soient ou non collectées auprès d'elle[50]. Le GDPR distingue les informations **obligatoires**[51], diversifiées, des informations **complémentaires nécessaires pour garantir un traitement équitable et transparent** à l'égard de la personne concernée[52].

Un apport majeur du GDPR est de conforter le droit à l'oubli numérique et à l'effacement, et d'en fixer les **conditions d'exercice**. Le responsable du traitement ayant rendu publiques des données personnelles qui est tenu de les effacer doit, compte tenu des technologies disponibles et des coûts de mise en œuvre, informer les autres responsables qui traitent ces données de la demande de la personne concernée d'effacer tout lien vers ces données ou les copies ou reproductions qui en ont été faites. Le GDPR liste les motifs[53] obligeant le responsable du traitement à effacer les données personnelles, dans les meilleurs délais.

Le GDPR introduit le droit à la limitation du traitement (marquage des données personnelles conservées, en vue de limiter leur traitement futur) dans des **cas de figure limitativement énumérés**. Comme méthodes, le responsable du traitement peut par exemple déplacer temporairement les données sélectionnées vers un autre système de traitement, les rendre inaccessibles aux utilisateurs, ou retirer temporairement celles publiées sur un site Internet.[54]

L'obligation du responsable du traitement de **notifier à chaque destinataire des données personnelles leur rectification, effacement ou la limitation du traitement** requiert une parfaite gestion de la procédure de suivi des transmissions des données, et dépend fortement de la pérennité des tiers (tranformation, faillite, etc.). Le responsable du traitement peut se soustraire à cette obligation s'il démontre qu'une telle communication se révèle impossible ou suppose un effort disproportionné.[55]

Le nouveau droit à la portabilité des données (transmission des données d'un système de traitement automatisé à un autre), qui s'applique lorsque la personne concernée a fourni les données personnelles sur la base de son **consentement** ou lorsque le traitement est nécessaire pour l'**exécution d'un contrat,** implique que la personne concernée puisse récupérer les données qu'elle a fournies sous une forme aisément réutilisable et que les responsables du traitement mettent au point des formats interopérables.

41 Article 15 GDPR.

42 Article 16 GDPR.

43 Article 17 GDPR. Voir *infra*.

44 Article 18 GDPR. Voir *infra*.

45 Article 20 GDPR. Voir *infra*.

46 Article 21 GDPR.

47 Article 22 GDPR. Voir *infra*.

48 Article 19 GDPR.

49 Article 34 GDPR. Voir *infra*.

50 Articles 13 et 14 GDPR.

51 Informations obligatoires : - identification du responsable du traitement et de son représentant ; - identification du **délégué à la protection des données** ; - finalités et **base juridique** du traitement ; - **intérêts légitimes** fondant le traitement ; - (catégories de) destinataires des données ; - **intention d'effectuer un transfert de données hors de l'UE**, et existence ou absence d'une décision d'adéquation de la Commission européenne ou la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir copie ou l'endroit où elles ont été mises à disposition.

52 Informations complémentaires : - **durée de conservation** des données personnelles ou critères utilisés pour déterminer cette durée ; - **existence de l'ensemble des droits** pouvant être exercés auprès du responsable du traitement ; - **droit d'introduire une réclamation** auprès d'une autorité de contrôle ; - **caractère réglementaire ou contractuel de l'exigence de fourniture des données** ou si cette fourniture **conditionne la conclusion d'un contrat** avec les conséquences éventuelles de leur non-fourniture ; - **existence d'une prise de décision automatisée, y compris un profilage** et la logique sous-jacente, l'importance et les conséquences prévues pour la personne concernée ; - **intention d'effectuer un traitement ultérieur pour une finalité autre** que la finalité initiale, accompagnée des éléments d'information préalable.

53 Motifs d'effacement : - les données ne sont plus nécessaires au regard des finalités présidant le traitement ; - la personne physique a retiré son consentement et il n'existe aucun autre fondement juridique au traitement ; - traitement illicite des données ; - respect d'une obligation légale.

54 Articles 4 (3) et 18, Cons. 67 GDPR. Cas de figure : - contestation de l'exactitude des données ; - traitement illicite ; - données qui ne sont plus nécessaires au traitement, mais à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ; - opposition au traitement pendant la vérification de ce que les motifs légitimes poursuivis par le responsable prévalent sur ceux de la personne concernée.

55 Article 12 GDPR.

Lorsque cela est techniquement possible, le responsable du traitement peut être amené à transmettre directement les données à un autre responsable du traitement.[56]

Le GDPR précise le droit de la personne concernée de ne pas faire l'objet d'une décision impliquant l'évaluation de certains aspects personnels la concernant, prise sur le seul fondement d'un traitement automatisé et produisant des effets juridiques la concernant ou l'affectant de manière significative (recrutement en ligne sans aucune intervention humaine, rejet automatique d'une demande de crédit en ligne, etc.), y inclus le **profilage**[57] (utilisation des données pour analyser ou prédire des aspects concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt, la fiabilité, le comportement, la localisation, les déplacements de la personne concernée, etc.). Dans les **cas où ce droit ne s'applique pas**[58], le responsable du traitement est tenu d'assortir le traitement automatisé de **garanties** pour la personne concernée (information spécifique, droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de l'évaluation, et de contester la décision).[59]

Le GDPR introduit l'obligation du responsable du traitement, soumise à exceptions[60], de notifier dans les meilleurs délais à la personne physique concernée les violations de données personnelles susceptibles de l'exposer à un risque élevé pour ses droits et libertés, afin qu'elle puisse prendre les précautions qui s'imposent (dommages physiques, matériels, préjudice moral : perte de contrôle sur ses données, limitation de ses droits, discrimination, vol ou usurpation d'identité, perte financière, renversement non autorisé de la procédure de pseudonymisation, atteinte à la réputation, perte de confidentialité de données protégées par le secret professionnel, ou tout autre dommage économique ou social important).[61]

Toute personne physique ayant subi un **dommage matériel ou moral** du fait d'une violation du GDPR a droit d'obtenir réparation du responsable du traitement ou du sous-traitant devant les juridictions de l'Etat membre soit dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement, soit dans lequel la personne concernée a sa résidence habituelle[62]. Le GDPR indique les faits générateurs de responsabilité propres à chacun de ces acteurs[63], à charge pour eux de prouver que le fait qui a provoqué le dommage ne leur est nullement imputable pour être exonérés de toute responsabilité. Le GDPR innove en prévoyant à certaines conditions une responsabilité solidaire des responsables du traitement et sous-traitants participant au même traitement.[64]

Il est rare que la personne concernée recoure aux procédures judiciaires disponibles du fait en particulier des frais à engager. Le GDPR introduit ainsi le principe des actions collectives. Les États membres ont la faculté de prévoir que les organismes, organisations ou associations à but non lucratif valablement constitués conformément à leur droit, dont les objectifs statutaires sont d'intérêt public et qui sont actifs dans le domaine de la protection des droits et libertés des personnes en matière de données personnelles, puissent obtenir réparation en son nom.[65]

56 Article 20 et Cons. 68 GDPR, lignes directrices du G29 : Guidelines on the right to data portability, 16/EN, WP 242 rev.01, 05/04/2017.

57 Aux fins du **profilage**, le responsable du traitement doit utiliser des procédures mathématiques ou statistiques adéquates, faire en sorte que les facteurs qui entraînent des erreurs soient corrigés, que le risque d'erreurs soit réduit au minimum, prévenir en particulier les effets discriminatoires.

58 Ce droit ne s'applique pas lorsque la décision est : - expressément autorisée par le droit de l'UE ou le droit d'un Etat membre (aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale, etc.) ; - nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ; - fondée sur le consentement explicite de la personne concernée.

59 Articles 4, 4), 22 et Cons. 71, 72 GDPR.

60 Exceptions lorsque le responsable du traitement : - a mis en oeuvre les mesures de protection techniques et organisationnelles appropriées rendant les données incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès (chiffrement, etc.) ; *ou* - a pris des mesures ultérieures garantissant que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ; *ou* – devrait fournir des efforts disproportionnés (il est dans ce cas procédé à une communication publique).

61 Article 34, Cons. 85, 86 GDPR.

62 Article 79, § 2 GDPR.

63 La responsabilité du responsable du traitement ayant causé un dommage qui constitue une violation du GDPR est engagée du fait de sa participation au traitement. Le sous-traitant est responsable de la violation des obligations du GDPR qui lui incombent spécifiquement, ou s'il a agi en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

64 Article 82 GDPR. Afin d'assurer une compensation effective de la personne concernée, chacun est tenu responsable du dommage dans sa totalité. Une action récursoire est ouverte à celui qui aurait réparé l'intégralité du dommage, lui permettant de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part propre de responsabilité qui leur incombe.

65 Article 80 GDPR.

Il ne faut pas négliger l'impact pour les entreprises monégasques soumises au GDPR du futur cadre UE de la protection des données personnelles, très protecteur des droits des personnes physiques et inversement très contraignant pour les responsables du traitement et les sous-traitants, d'autant que la Loi n° 1.165 du 23/12/1993 relative à la protection des informations nominatives n'offre pas en l'état un niveau de protection équivalent et adéquat.

En particulier les secteurs informatique - Cloud, biens de consommation, banque, tourisme vont devoir mettre en place rapidement de nouveaux outils et pratiques de gouvernance pour être prêts en mai 2018. Les amendes administratives[66] susceptibles d'être infligées en cas de violation du GDPR sont loin d'être symboliques.

La Loi n° 1.165 est appelée à évoluer pour au minimum se conformer au standard international du Conseil de l'Europe. Le processus de modernisation de la Convention N°108 pour la protection des personnes à l'égard du traitement automatisé des données et de son Protocole (en vigueur à Monaco depuis le 01/04/2009) est en phase finale. Cette mise à jour a été synchronisée avec la réforme de l'UE afin d'assurer la cohérence entre la Convention modernisée N°108 et le GDPR.[67]

66 Article 83 GDPR. Deux paliers d'amendes administratives sont prévues : 1/ jusqu'à 10 millions € ou 2% du CA annuel mondial de l'exercice précédent (consentement des mineurs - traitements qui ne nécessitent pas d'identification - protection des données à la conception et par défaut - missions du délégué à la protection des données - violation des Code de conduite, certificat) ; 2/ jusqu'à 20 millions € ou 4% du CA annuel mondial de l'exercice précédent (principes de base dont les conditions au consentement - droits des personnes concernées - transferts de données hors UE - non conformité aux ordres des autorités de contrôle).

67 Le Comité ad hoc sur la protection des données (CAHDATA), créé par le Conseil des ministres (art. 17 Statut Conseil de l'Europe, et Résolution CM/Res(2011)24), a produit la Version consolidée de la Convention modernisée 108 (09/2016). La mise à jour traite les problématiques liées au respect de la vie privée résultant de l'utilisation des nouvelles technologies de l'information et de la communication (NTIC), et renforce le mécanisme de suivi.