FEDIL

Positionen - 15/04/2017

AVIS DE LA FEDIL – TRANSPOSITION EN DROIT NATIONAL DE CERTAINES DISPOSITIONS DU RGPD

Zusammenfassung / Inhalte

AVIS DE LA FEDIL EN VUE DE LA TRANSPOSITION EN DROIT NATIONAL DE CERTAINES DISPOSITIONS DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (EN ABRÉGÉ : RGPD)

1. Possibilités d'action offertes par le règlement
    a. Article 6 : Licéité du traitement
    b. Article 8 : Conditions applicables au consentement des enfants
    c. Article 23 : Limitation
    d. Article 58 : Pouvoirs des autorités de contrôle
    e. Article 80 : Représentation des personnes concernées
    f. Article 88 : Traitement des données dans le cadre de la relation de travail
    g. Article 90 : Obligation de secret
2. Les possibilités d'actions offertes par le règlement
    a. Article 28 : Sous-traitant
    b. Article 32 : Sécurité du traitement
    c. Article 37: Désignation du délégué à la protection des données (DPO)
    d. Article 62 : Opération conjointe des autorités de contrôle

RESUME DES PROPOSITIONS DE LA FEDIL

1. Possibilités d'action offertes par le règlement
    a. Article 6 : Licéité du traitement
    b. Article 8 : Conditions applicables au consentement des enfants

c. Article 23 : Limitations

d. Article 58 : Pouvoirs des autorités de contrôle

e. Article 80 : Représentation des personnes concernées

f. Article 88 : Traitement des données dans le cadre de la relation de travail

g. Article 90 : Obligation de secret

2. Les possibilités d'actions offertes par le règlement

a. Article 28 : Sous-traitant

b. Article 32 : Sécurité du traitement

c. Article 37 : Désignation du délégué à la protection des données (DPO)

d. Article 62 : Opération conjointe des autorités de contrôle

AVIS DE LA FEDIL EN VUE DE LA TRANSPOSITION EN DROIT NATIONAL DE CERTAINES DISPOSITIONS DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (EN ABRÉGÉ : RGPD)

Introduction

La FEDIL, en tant qu'acteur économique de poids représentant quelque 550 membres dans 35 secteurs d'activité au Luxembourg, entend ici porter les messages clés de ses membres afin de permettre au législateur de prendre conscience des besoins et inquiétudes des entreprises quant à ce règlement qui les impactera toutes, quelle que soit leur taille, à brève échéance. En effet, celui-ci, au regard des décisions stratégiques prises par le gouvernement, pourra avoir une incidence non négligeable, sur l'activité des entreprises.

Pour ce faire, la FEDIL a mené, avec ses membres, une réflexion sur le sujet et organisé un groupe de projet regroupant des entreprises de tous secteurs d'activités qui ont ainsi pu faire part de leurs préoccupations et de leurs besoins quant aux mesures à prendre par le Luxembourg dans le processus de transposition.

Commentaires généraux

Il est un fait que de nombreuses incertitudes demeurent quant à la mise en application de ce règlement. En effet, si ce règlement a été pensé pour corriger les travers de la Directive de 1995 et les transpositions parfois divergentes faites par les Etats membres (EM) créant ainsi trop de disparités et une fragmentation au niveau européen en terme de législation sur la protection des données, il n'en demeure pas moins qu'il laisse également aux EM une large autonomie de choix, qui fait craindre que le régime qui devait être uniformisé, ne le soit en définitive pas. De plus, la longueur des considérants ainsi que

leurs velléités normatives finissent de brouiller la compréhension de certaines règles figurant dans le corps du règlement.

Face au renforcement des pouvoirs des autorités de contrôle, les entreprises se montrent très attachées au *modus vivendi* existant au Luxembourg, à savoir une coopération et un support de la Commission Nationale pour la Protection des Données (CNPD) dans le cadre des questions de protection des données. Dans ce même ordre d'idée, il est important que le Luxembourg adopte des mesures lui permettant de garantir sa compétitivité sur le marché de la donnée en plein essor et d'en saisir les opportunités. Les mesures de transposition envisagées ne doivent également pas être trop restrictives et aller au-delà du texte.

La méthodologie employée pour le présent avis a été de prendre les points du règlement nécessitant une action des Etats membres dans un premier temps et dans un second temps, les points leur permettant d'adapter leur législation nationale.

Les points clefs de cet avis seront résumés en fin de texte.

1. POSSIBILITÉS D'ACTION OFFERTES PAR LE RÈGLEMENT

A. ARTICLE 6 : LICÉITÉ DU TRAITEMENT

Les conditions de licéité du traitement sont suffisamment explicitées par le RGPD et dès lors, aucune intervention du législateur n'est rendue nécessaire. **L'auto-évaluation et la responsabilisation du responsable du traitement doivent être privilégiées dans l'approche.**

Le RGPD apporte ici une précision par rapport à la Directive 95/46, notamment en excluant toute finalité exprimée de manière générale et donnant une véritable liberté de choix au sujet de droit. Il s'avère, cependant, que les conditions initiales liées à un traitement peuvent différer suivant l'avancée du traitement et du dossier apparenté de sorte que souvent, des questions opérationnelles liées se posent. Dans ce cas, il appartient au responsable de traitement d'évaluer le cadre et les conditions de cet élargissement notamment, la compatibilité des finalités nouvelles avec les finalités initiales au besoin avec le support de la CNPD. **C'est en ce sens que la formation et l'information des acteurs clefs du RGPD doivent absolument être mises en place.**

La FEDIL est d'avis qu'il ne faut aucunement rendre la licéité du traitement plus contraignante au Luxembourg.

Le concept d'intérêt public doit cependant s'entendre de manière plus large qu'actuellement et notamment inclure dans sa prise en compte, les notions de sécurité du public et des utilisateurs et/ou de danger immédiat. Pour être plus concret, il est parfois indispensable pour des raisons de sécurité évidentes (accident, fuite de gaz, etc.) que des conversations téléphoniques passées en dehors des numéros d'appel d'urgence soient enregistrées au-delà de tout lien contractuel ou que des géolocalisations soient possibles afin de permettre – dans des situations de stress élevé – de réécouter l'enregistrement et les informations qu'il contient et qui n'auraient peut-être pas été entièrement saisies par l'opérateur. Il est donc encore une fois important que, dans l'appréciation de la licéité du traitement, soit prise en compte la finalité de ce dernier et l'intérêt qu'elle protège.

Nous pensons, néanmoins, que cet article peut sérieusement nuire à l'harmonisation des règles au niveau européen et qu'il est dans l'intérêt du Luxembourg de se positionner afin d'attirer des acteurs économiques désireux d'être en présence de règles simples et efficaces.

B. ARTICLE 8 : CONDITIONS APPLICABLES AU CONSENTEMENT DES ENFANTS

Le point soulevé ici va au-delà de la licéité du traitement suivant l'âge des enfants avec ou sans autorisation parentale. Il nous semble nécessaire de mettre en perspective la situation au Luxembourg et d'envisager ce que le gouvernement souhaite faire sur ce sujet. Un enfant, à 13 ans, peut-il librement consentir au traitement de ses données qui serviront potentiellement à le « profiler » et lui faire recevoir des offres commerciales ? Quelle est sa compréhension des risques et surtout de la portée de son consentement ? Se pose également la question lors de l'utilisation des médias sociaux et de la possibilité d'y laisser des données qui pourront par la suite être utilisées.

La question du discernement est, selon notre lecture, la notion clef, cette dernière ne trouvant pas de réponse uniforme en droit luxembourgeois ni dans les pratiques existantes.

Au Luxembourg, en matière pénale, la jurisprudence fixe généralement l'âge du discernement à 6 ans. Dès 12 ans, l'enfant peut ouvrir un compte bancaire avec l'accord de ses parents et à 15 ans disposer d'une carte de paiement. La majorité sexuelle est, quant à elle, fixée à 16 ans. En France, on estime que l'âge de discernement se situe aux alentours de 12 ans sans que cette règle ne trouve une base légale.

Ramener l'âge du consentement des enfants à 13 ans pourrait être un avantage concurrentiel pour le Luxembourg mais à l'instar des autres EM, la question du recueil de l'autorité parentale pose question. Comment s'assurer que l'autorisation a bien été donnée ? Comment le responsable du traitement peut-il s'en assurer ?

La FEDIL est en faveur d'une uniformisation de l'âge avec ce qui se pratique dans les autres cas cités précédemment au Luxembourg. L'âge de 15 ans ressort dans différents éléments de la vie quotidienne (Compte bancaire, signature, etc.). **La FEDIL propose de retenir cet âge comme âge de référence en matière de consentement.**

C. ARTICLE 23 : LIMITATION

Cet article, déjà présent dans la directive, voit cependant son champ d'application s'étendre en permettant de limiter le droit de la personne concernée quant à l'accès à ses données personnelles, à leur gestion ou à leur effacement ou limiter les cas de communication d'une violation. Les conditions se font cependant sous couvert du respect des droits fondamentaux et qu'il s'agisse d'une mesure nécessaire et proportionnée dans une société démocratique.

La FEDIL demande l'application stricte par les autorités luxembourgeoises des limitations énumérées par le règlement. Nous estimons, en effet, qu'il n'est nulle nécessité d'élargir les possibilités de limitation des droits. Celles-ci ne doivent en aucun cas devenir un moyen détourné pour limiter les droits de la personne concernée quant à la protection de ses données à caractère personnel.

La FEDIL convie le législateur à établir, par voie règlementaire ou législative, une liste des autorités pouvant bénéficier de ces dérogations. Cette liste doit être publiquement accessible afin de permettre au responsable du traitement de pouvoir identifier l'autorité de contrôle requérante, au besoin à l'aide de demande de documents « d'accréditation », et sa légitimité à limiter les droits de la personne concernée.

Il est essentiel que la limitation des droits ne se fasse que sur base d'indices graves et concordants rentrant dans les cas d'ouverture précisés par le RGPD et non pas dans le cadre d'une simple recherche ou demande d'information.

D. ARTICLE 58 : POUVOIRS DES AUTORITÉS DE CONTRÔLE

Le règlement impose, d'une part, aux EM de prévoir par voie législative, le pouvoir de l'autorité de contrôle pour agir en justice contre les violations du RGPD et d'autre part, permet aux EM de donner des pouvoirs additionnels à l'autorité de contrôle.

Le RGPD, en privilégiant le contrôle à posteriori du traitement, oblige les différents acteurs et notamment les responsables du traitement, à assumer leurs responsabilités. La sanction en cas de non-respect étant le pouvoir pour la CNPD de prononcer des amendes ou d'agir en justice et ne nécessite pas dans ce cas d'élargir les pouvoirs lui dévolus.

La FEDIL plaide, dès lors, en faveur d'un maintien strict des dispositions du règlement sans élargir encore la palette dévolue aux autorités de contrôle.

La question qui est par ailleurs soulevée, est l'interconnexion forte entre différentes autorités nationales intervenant sur des dossiers identiques, connexes ou similaires, comme la CNPD, la CSSF, l'ILR ou encore le Commissariat aux assurances sans que cette liste ne soit exhaustive. La CSSF va, en effet, réguler les données clients alors qu'elle ne sera plus compétente pour les données entre fournisseurs et clients. Il risque dès lors d'y avoir en pratique quelques heurts. **Il nous semble important, notamment pour les professions réglementées d'avoir un guichet unique (one stop shop), respectivement un point de contact unique permettant de renseigner les entreprises, de faciliter et coordonner les relations entre les différentes autorités et les entreprises.**

Le système luxembourgeois repose sur la collaboration et la coopération avec la CNPD. C'est un modèle que les entreprises souhaitent voir perdurer malgré les nouveaux pouvoirs conférés à la CNPD. Il s'agit véritablement d'un avantage par rapport à d'autres pays qui seront nécessairement concurrents dans le développement de business relatifs à la protection des données ou qui se montreront plus immédiatement répressifs.

Il est, pour ce faire, également indispensable que la CNPD voit ses effectifs renforcés mais surtout, que les entreprises puissent y trouver des officiers dédiés en mesure de répondre à leurs besoins.

E. ARTICLE 80 : REPRÉSENTATION DES PERSONNES CONCERNÉES

Cet article prévoit la possibilité de mandater une organisation pour représenter les intérêts de la personne concernée mais également de prévoir la possibilité d'agir sans mandat.

La FEDIL se montre, de ce fait, fermement opposée à toute action de Tiers sans mandat en la matière. Les risques sont, par ailleurs, plus importants que le bénéfice attendu. En effet, la CNPD disposera d'un contrôle efficace et surtout d'un panel de sanctions dissuasives en matière de violation de protection des données. Le sujet de droit redevient maitre de ses données et des voies de droit s'ouvrent également à lui de sorte qu'une protection juridique efficace et efficiente existera sans avoir besoin de l'intervention de Tiers.

Il s'avère qu'un principe élémentaire du droit est celui de ne pas pouvoir disposer de droit pour autrui, ce qui exclut toute action sans mandat.

Par conséquent, **nous estimons qu'il n'y a pas lieu de l'introduire via ce règlement**. Au surplus, les conséquences ne sont pas évaluables et risquent d'être préjudiciables aux entreprises.

En effet, les entreprises se retrouveront sous investigation; obligées de fournir des documents, les actions pouvant se multiplier entrainant de potentiels blocages, mobilisant des ressources qui ne devraient pas l'être, etc.

Il n'est pas exclu non plus que certaines actions se veuillent malveillantes et ne constituent un moyen détourné pour avoir accès – au moins partiellement – à certains documents de l'entreprise.

Par ailleurs, le plaignant sera informé, ce qui peut aussi nuire à l'entreprise visée par la plainte et violer ainsi la confidentialité nécessaire à toute activité surtout si cette dernière est sensible.

F. ARTICLE 88 : TRAITEMENT DES DONNÉES DANS LE CADRE DE LA RELATION DE TRAVAIL

Il est manifeste que la législation actuelle figurant dans le code du travail n'est plus adaptée aux réalités de l'entreprise et des avancées technologiques.

La FEDIL propose de réviser et d'adapter les articles L. 261-1 et suivants du code du travail, ces derniers étant devenus obsolètes.

De plus, l'usage de la vidéo doit être permis dans un cadre plus large et se généraliser. Se pose en premier lieu le problème de la formation. Beaucoup d'entreprises veulent tourner des vidéos pour expliquer les bons gestes ou les gestes à proscrire. La vidéo est un excellent moyen didacticiel pour former des équipes même éloignées ou donner des formations récurrentes pour les salariés intérimaires par exemple ou encore permettre de visionner certaines techniques à plusieurs reprises. Or, à ce jour, la législation ne le prévoit pas, représentant un vrai manque pour les entreprises et pour les salariés.

Pareillement, pour les entreprises ayant des métiers à risques ou sur des installations à risques, des métiers exercés de manière isolée et dont les salariés peuvent intervenir seul sur une zone potentiellement dangereuse, il n'est à l'heure actuelle, pas possible de les localiser alors qu'il en va de leur sécurité, la mesure rencontrant systématiquement l'objection de la CNPD. Si les droits de la personne doivent naturellement être protégés, il n'en demeure pas moins que les mesures de surveillance se font aussi dans l'intérêt du salarié qui les réclame : poste autonome, isolé, risqué, déplacements fréquents, …

Une autorisation plus générale devrait être possible pour des questions spécifiques. Ces questions devraient être du ressort du responsable du traitement, au besoin avec la collaboration de la délégation du personnel.

Il est impératif de revoir les législations devenues obsolètes et de ne plus voir le pouvoir de surveillance de l'employeur comme un élément néfaste visant uniquement à „traquer" le salarié.

Nous recommandons la révision des dispositions légales mais également qu'une certaine souplesse soit laissée au responsable du traitement afin justement de permettre au principe de proportionnalité de jouer. Principe qui, s'il n'est pas respecté, fera l'objet d'un avertissement de la CNPD et de sanctions si ce dernier n'est pas pris en compte, rendant dès lors inutile le maintien de dispositions légales ayant les mêmes conséquences tout en rigidifiant des mécanismes qui ont besoin d'évoluer.

Les représentants des salariés auront largement la possibilité de jouer le rôle de lanceur d'alerte.

G. ARTICLE 90 : OBLIGATION DE SECRET

Cet article laisse la possibilité aux EM d'adopter des règles spécifiques afin de déterminer les pouvoirs des autorités de contrôle quant aux responsables de traitement ou sous-traitant soumis à une obligation de secret.

La FEDIL suggère la plus grande prudence quant à la notion de traitement de données personnelles dans le cadre du secret professionnel. Il est important que le pouvoir des autorités de contrôle tienne compte de ces facteurs et qu'il soit de ce fait limité.

Il parait à ce stade, adéquat qu'une ordonnance judiciaire, sans préjudice de tout autre acte, soit au minimum délivrée pour accéder aux données et qu'un juge puisse faire la balance des intérêts en présence, et garantir la proportionnalité de la mesure tout en permettant une célérité du traitement de la demande.

2. LES POSSIBILITÉS D'ACTIONS OFFERTES PAR LE RÈGLEMENT

Divers articles confrontent le RGPD à la règlementation nationale. S'il n'est plus question pour les Etats d'agir quant à la mise en place du RGPD dans leurs droits nationaux, il s'agit ici d'espaces laissés par le RGPD pour les lois nationales et une certaine application des textes.

A. ARTICLE 28 : SOUS-TRAITANT

Cet article amplifie les obligations du sous-traitant et les dispositions contractuelles du contrat de sous-traitance. La question qui se pose immédiatement aux entreprises est le lien avec les entreprises étrangères et les chaînes de sous-traitance.

Beaucoup de questions y relatives se posent : jusqu'où va la responsabilité du sous-traitant et quelles sont ses obligations en la matière ? Quelle responsabilité pour le DPO ? Comment peut-on avoir la certitude que le sous-traitant répondra à ses obligations contractuelles, notamment lorsque les données sont stockées ou hébergées hors de l'Union Européenne ?etc.

L'audit des sous-traitants ?

L'audit des sous-traitants pourrait être une solution pour permettre de

s'assurer de la conformité des sous-traitants comme cela est pratiqué par certaines grandes entreprises. Le cas des entreprises de taille plus modeste est ici soulevé alors que ces dernières ne disposent pas de suffisamment de ressources leurs permettant de contrôler les agissements du sous-traitant. La question peut être financière, avec la recherche du prix le plus concurrentiel ; humaine, le personnel n'étant pas formé à ces questions ou encore intellectuelle avec l'absence de notion juridique les rendant dépendantes du contrat proposé.

Nous sommes d'avis que le Luxembourg devrait très clairement se diriger vers une obligation de moyen renforcée quant à la conformité des sous-traitants.

En effet, devant la complexité de la matière, le responsable du traitement ou le DPO devrait pouvoir s'exonérer de toute responsabilité en démontrant avoir fait les recherches nécessaires sur le sous-traitant, au besoin en lui ayant fait remplir une fiche déclarative et en apportant la preuve des engagements contractuels pris.

Cette approche est fondamentale et doit ressortir du projet de loi alors que l'incertitude quant aux responsabilités risque à terme de paralyser un certain nombre d'échanges. La stratégie numérique du Luxembourg passe par la captation d'acteurs numériques et il convient de leur offrir un cadre juridique sain et clair.

Il est important que les entreprises soient conscientes des efforts à fournir en la matière en cas de sous-traitance mais il est indubitable que l'obligation de résultat est impossible à exiger au regard de la multiplicité potentielle des intervenants partout dans le monde.

Les entreprises doivent dès lors être raisonnablement tenues que du possible et de ce qui peut être en leur pouvoir pour garantir le respect du règlement de la part de leurs sous-traitants.

La révision des contrats de sous-traitance ?

Il est important de faire la promotion des règles relatives aux contrats de sous-traitance notamment les clauses proposées par la Commission européenne dans le cadre de la sous-traitance en matière de transfert de données. Des règles *sui generis* peuvent également être proposées au niveau national et diffusées auprès des entreprises afin de leur permettre de sécuriser au maximum leur traitement de données.

Il ne faut cependant pas devenir trop spécifique ce qui obligerait à une révision globale de tous les contrats et d'engendrer trop de contraintes, mais il faut permettre aux contrats de sous-traitance de s'enrichir afin de protéger les responsables de traitement et DPO et au final les données personnelles traitées. L'équilibre doit être maintenu.

B. ARTICLE 32 : SÉCURITÉ DU TRAITEMENT

A la lecture du texte, le droit d'un EM pourrait obliger le responsable du traitement ou le sous-traitant à communiquer certaines données. Cela pourrait être le cas d'autorités judiciaires ou administratives.

Nous jugeons ici important une nouvelle fois, de limiter les cas de recours respectivement de ne le permettre que sur base d'une autorisation officielle, idéalement établie par une autorité judiciaire afin d'éviter tout abus de droit dans le présent cadre.

La notion de devoir de sécurité est également à aborder dans ce cadre. En effet, c'est la finalité du traitement qui déterminera le niveau de sécurité à mettre en œuvre. Les règles de sécurité sont donc amenées à évoluer constamment afin de tenir compte de l'état des menaces. Cela implique, dès lors, une politique de gestion des risques pour les entreprises et un classement des données en fonction de leur sensibilité.

C. ARTICLE 37: DÉSIGNATION DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

Afin d'éviter la prolifération de formations quant au DPO, **nous recommandons expressément de mettre en place une formation officielle, respectivement, d'accréditer des formations de DPO alors qu'actuellement sont proposées sur le marché un ensemble de formation avec des contenus plus ou moins aboutis.**

Le label pourrait s'inscrire dans cette démarche alors qu'il permettrait de garantir les connaissances de ce professionnel et son „agréation" par l'autorité de contrôle. (Connaissances théoriques, pratique du métier, etc.)

Nous jugeons important que le législateur se positionne sur une définition d' « activités de base consistant en un traitement à grande échelle de catégorie particulières de données ». En effet, cette terminologie reste absconde pour beaucoup d'entreprises et les définitions respectivement, les approches se dessinant dans les différents Etat Membres sont loin d'être concordantes. Dès lors, le Luxembourg gagnerait à définir un cadre clair pour les entreprises en adoptant naturellement une approche restrictive quant aux cas d'ouvertures, le DPO étant une charge pour les entreprises.

D. ARTICLE 62 : OPÉRATION CONJOINTE DES AUTORITÉS DE CONTRÔLE

La FEDIL estime que les pouvoirs d'une autorité étrangère agissant sur le sol luxembourgeois ne doivent pas excéder les pouvoirs dévolus à la CNPD. Afin d'éviter tout abus ou toute méconnaissance de tels droits, la FEDIL s'oppose à toute délégation de pouvoir de la part de la CNPD dans le cadre d'enquête à une autorité étrangère.

RESUME DES PROPOSITIONS DE LA FEDIL

1. POSSIBILITÉS D'ACTION OFFERTES PAR LE RÈGLEMENT

A. ARTICLE 6 : LICÉITÉ DU TRAITEMENT

- Ne pas rendre la licéité du traitement plus contraignante au Luxembourg,
- Privilégier dans l'approche, l'auto-évaluation et la responsabilisation du responsable du traitement,
- Mettre en place la formation et l'information des acteurs clefs du RGPD.

B. ARTICLE 8 : CONDITIONS APPLICABLES AU CONSENTEMENT DES ENFANTS

- Uniformiser l'âge du consentement avec ce qui se pratique dans d'autres cas au Luxembourg,
- Retenir l'âge de 15 ans comme âge de référence en matière de consentement.

C. ARTICLE 23 : LIMITATIONS

- Appliquer strictement les limitations énumérées par le règlement,
- Etablir par voie réglementaire ou législative, une liste des autorités pouvant bénéficier de dérogations quant aux limitations établies et rendre celle-ci publique.

D. ARTICLE 58 : POUVOIRS DES AUTORITÉS DE CONTRÔLE

- Maintenir strictement les dispositions du règlement sans élargir la palette de pouvoirs dévolus aux autorités de contrôle,
- Créer un guichet unique permettant de renseigner les entreprises, de faciliter et de coordonner les relations entre les différentes autorités et les entreprises,
- Renforcer les effectifs de la CNPD pour répondre aux besoins des entreprises,
- Faire perdurer le modèle luxembourgeois basé sur la collaboration et la coopération entre la CNPD et les entreprises.

E. ARTICLE 80 : REPRÉSENTATION DES PERSONNES CONCERNÉES

- Interdire toute action de tiers sans mandat de la personne concernée.

F. ARTICLE 88 : TRAITEMENT DES DONNÉES DANS LE CADRE DE LA RELATION DE TRAVAIL

- Adapter les articles L. 261-1 et suivant du code du travail,
- Réviser les dispositions légales,
- Laisser au responsable du traitement l'évaluation de la proportionnalité du traitement à mettre en œuvre en ce qui concerne les données dans le cadre de la relation de travail au besoin en informant la délégation du personnel.

G. ARTICLE 90 : OBLIGATION DE SECRET

- Demander au minimum la délivrance d'une ordonnance judiciaire, sans préjudice de tout autre acte, pour accéder aux données,
- Demander à ce qu'un juge fasse la balance des intérêts en présence,
- Garantir la proportionnalité de la mesure tout en permettant la célérité du traitement de la demande.

2. LES POSSIBILITÉS D'ACTIONS OFFERTES PAR LE RÈGLEMENT

A. ARTICLE 28 : SOUS-TRAITANT

- Fournir une obligation de moyen à l'égard du responsable de traitement ou DPO quand à l'évaluation de la conformité du sous-traitant dès lors qu'il peut démontrer avoir fait le nécessaire pour s'informer et notamment par une fiche déclarative remplie par le sous-traitant,
- Proposer des règles types à insérer dans les contrats de sous-traitance.

B. ARTICLE 32 : SÉCURITÉ DU TRAITEMENT

- Limiter les cas de recours respectivement, ne les permettre que sur base d'une autorisation officielle, idéalement établie par une autorité judiciaire afin d'éviter tout abus dans le présent cadre.

C. ARTICLE 37 : DÉSIGNATION DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

- Mettre en place une formation officielle, respectivement, accréditer les formations de DPO déjà existantes sur le marché,
- Définir les « Activités de base consistant en un traitement à grande échelle de catégorie particulières de données ».

D. ARTICLE 62 : OPÉRATION CONJOINTE DES AUTORITÉS DE CONTRÔLE

- Ne pas autoriser la délégation de pouvoirs de la part de la CNPD dans le cadre d'enquête à une autorité étrangère.