Directive relative à la protection des données

Groupe-NITTEL®

Du: 21.03.2018

Sommaire

I. Objectif de la directive relative à la protection des données

Dans le cadre de sa responsabilité sociétale, le groupe NITTEL® s'engage à respecter les droits à la protection des données à l'échelle mondiale. Cette directive applicable à l'ensemble du groupe NITTEL® repose sur des principes de protection des données fondamentaux reconnus au niveau international. Le respect des règles de protection des données est l'une des conditions préalables à l'entretien de relations commerciales basées sur la confiance et à la réputation d'employeur de choix qui est celle de NITTEL®.

La présente directive crée par ailleurs l'une des conditions requises pour un échange global de données[1] entre les sociétés du groupe. Elle garantit en effet le niveau de protection adéquat exigé par la directive européenne relative à la protection des données[2] et les différentes législations nationales pour les échanges de données transfrontaliers, y compris dans les pays dépourvus d'une législation appropriée en la matière[3].

II. Champ d'application et modification de la directive relative à la protection des données

La présente directive relative à la protection des données s'applique à toutes les entreprises du groupe NITTEL® et toutes les sociétés qui en dépendent ou y sont rattachées, ainsi qu'à leurs collaborateurs. On entend par « dépendre » le fait que NITTEL® est en droit d'exiger, de manière directe ou indirecte, l'application de la présente directive, que ce soit sur la base d'une majorité des droits de vote, d'une majorité au sein de la direction de l'entreprise ou d'un accord. La directive relative à la protection des données couvre l'ensemble des formes de traitement de données à caractère personnel[4]. Elle s'applique également aux personnes morales dans les pays où le droit national englobe tant les personnes morales que les ersonnes physiques dans le champ de protection des données. Les données anonymisées[5], par exemple à des fins d'analyses statistiques ou d'enquêtes, n'entrent pas dans le cadre de la présente directive.

Toute modification de la présente directive doit être effectuée en concertation avec le délégué à la protection des données du groupe NITTEL® (délégué général) et ce, dans le cadre de la procédure prescrite pour la modification de directives. Les modifications sont notifiées sans délai aux entreprises du groupe NITTEL® dans le cadre de ladite procédure. Les modifications ayant des impacts majeurs sur le respect de la directive relative à la protection des données doivent être communiquées chaque année aux autorités chargées de valider la présente directive et de confirmer le caractère obligatoire de ses dispositions internes en matière de protection des données.

La toute dernière version de la directive relative à la protection des données peut être consultée sur le site Internet de groupe NITTEL® : www.nittel.eu.

[1] Cf. art. XV.

[2] Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données pouvant être consultée sous http://ec.europa.eu/justice_home/fsj/privacy/law/index_fr.htm#directive

[3] Cf. art. XV.

[4] Cf. art. XV.

[5] Cf. art. XV.

III. Validité du droit national

La présente directive relative à la protection des données reprend les principes reconnus universellement en la matière, sans se substituer au droit national en vigueur. Elle a pour but de compléter le droit national respectif en matière de protection des données. La législation nationale s'applique de manière prioritaire en cas de différences par rapport à la présente directive ou d'exigences dépassant le cadre de celle-ci. Les dispositions de la présente directive doivent être observées même en l'absence de règles de droit national correspondantes. Les obligations de déclaration existant en vertu du droit national pour le traitement des données doivent être impérativement respectées.

Chaque entreprise du groupe NITTEL® est responsable du respect de la présente directive ainsi que des obligations légales en matière de protection des données. S'il y a lieu de supposer que certaines obligations légales sont en contradiction avec les obligations résultant des présentes, il convient d'en informer immédiatement le délégué général à la protection des données. En cas d'opposition entre les dispositions légales nationales et la présente directive, recherchera, en concertation avec l'entreprise du groupe concernée, une solution acceptable conforme aux objectifs de ladite directive.

IV. Principes relatifs au traitement des données personnelles

1 Equité et légalité

Lors du traitement de données personnelles, les droits de la personnalité de l'intéressé[6] doivent être respectés. Les données à caractère personnel doivent être collectées et traitées conformément aux principes de droit et d'équité.

2 Limitation à une finalité spécifique

Le traitement de données à caractère personnel ne peut être effectué qu'aux fins spécifiées préalablement à leur collecte. Toute modification ultérieure des usages définis n'est possible que de manière restreinte et requiert justification.

[6] Cf. art. XV.

3. Transparence

L'intéressé doit être informé du traitement de ses données. De manière générale, les données à caractère personnel doivent être recueillies auprès de la personne elle-même. Lors de la collecte des données, l'intéressé doit être en mesure d'identifier au minimum les éléments suivants ou disposer d'informations adéquates :

» Identité du service responsable[7]
» Finalité du traitement des données
» Tiers[8] ou catégories de tiers auxquels les données seront potentiellement transmises

4. Parcimonie des données

Il convient de vérifier préalablement au traitement de données à caractère personnel si et dans quelle mesure ce traitement s'impose pour atteindre l'objectif visé. Dans la mesure où la finalité définie le permet et où les moyens engagés sont proportionnels à l'objectif visé, il convient de recourir à des données anonymisées ou statistiques.
Les données à caractère personnel ne doivent en aucun cas être stockées en prévision de futures utilisations potentielles, à moins que cette mesure soit prescrite ou autorisée par la législation nationale.

5. Suppression

Les données à caractère personnel qui ne sont plus nécessaires à l'issue du délai de conservation légal ou commercial[9] doivent être impérativement supprimées. Si, dans des cas particuliers, il apparaît que ces données sont d'un intérêt sensible ou peuvent avoir une signification historique, il convient alors de les conserver jusqu'à ce que cet intérêt sensible ait été juridiquement clarifié ou que le service d'archives du groupe ait pu évaluer l'intérêt de leur archivage à des fins de documentation historique.

6. Exactitude et actualité des données

Les données à caractère personnel enregistrées doivent être exactes, exhaustives et – si nécessaire – à jour. Il convient de prendre toutes les mesures appropriées pour garantir que les données inexactes, incomplètes ou obsolètes sont supprimées, rectifiées, complétées ou mises à jour.

7. Confidentialité et sécurité des données

Les données à caractère personnel sont soumises au secret. Elles doivent être traitées par chaque intervenant avec la plus grande confidentialité et protégées contre tout accès, traitement ou transmission illicite, ainsi que contre toute perte, modification ou destruction accidentelle par des mesures techniques et organisationnelles appropriées.

[7] Cf. art. XV.
[8] Cf. art. XV.
[9] Cf. art. XV.

V. Fiabilité du traitement desdonnées

La collecte, le traitement et l'utilisation des données à caractère personnel ne sont autorisés qu'en liaison avec l'une des autorisations de fait mentionnées ci-après. Une telle autorisation de fait est également nécessaire en cas de modification de l'usage défini initialement pour la collecte, le traitement et l'utilisation des données à caractère personnel.

1. Données clients et partenaires

1.1 Traitement de données pour une relation contractuelle

Le traitement de données à caractère personnel de prospects, clients ou partenaires est autorisé aux fins d'établissement, d'exécution ou de cessation de contrat. Cela inclut également le suivi du partenaire contractuel dans la mesure où ce suivi est en relation avec la finalité du contrat. Durant la phase préalable à la conclusion d'un contrat, ou phase d'initialisation d'un contrat, le traitement de données à caractère personnel destinées à l'établissement d'offres, à la préparation de demandes d'achat ou à la satisfaction de souhaits d'autre nature exprimés par le prospect dans la perspective d'une conclusion de contrat, est autorisé.

1.2 Traitement de données à des fins publicitaires

Les prospects peuvent être contactés durant la phase d'initialisation du contrat par le biais des informations qu'ils ont communiquées. Les restrictions éventuelles formulées par le prospect doivent être respectées. Les mesures publicitaires dépassant le cadre défini ci-dessus doivent satisfaire aux conditions énoncées à l'art. V., al. 1.3.

1.3 Consentement au traitement des données

Le traitement de données à caractère personnel peut s'opérer sur la base du consentement donné par l'intéressé. Avant tout consentement, l'intéressé doit être informé conformément à l'art. IV., al. 3., de la présente directive relative à la protection des données. La déclaration de consentement doit être systématiquement établie sous forme écrite ou électronique afin de pouvoir être utilisée pour les nécessités de la preuve. Dans certaines circonstances, notamment dans le cadre d'une prestation de conseil téléphonique, le consentement peut également être accordé par oral. L'octroi du consentement doit être impérativement documenté.

1.4 Traitement de données du fait d'une autorisation légale

Le traitement de données à caractère personnel est également licite dans les cas où celui-ci est exigé, posé comme condition ou admis du fait de dispositions légales nationales. La nature et l'étendue du traitement des données doivent être nécessaires au traitement autorisé et définies en fonction de ces prescriptions légales.

[10] Cf. art. XV.

1.5 Traitement de données du fait d'un intérêt légitime

Le traitement de données à caractère personnel est également possible lorsqu'il sert un intérêt légitime du groupe NITTEL®. Les intérêts légitimes sont généralement d'ordre juridique (recouvrement de dettes, par exemple) ou économique (prévention de défauts d'exécution de contrat, par exemple). Le traitement de données à caractère personnel du fait d'un intérêt légitime ne peut avoir lieu dès lors qu'il existe, dans un cas particulier, une raison de penser que les intérêts sensibles de l'intéressé prévalent sur l'intérêt à procéder au traitement. Avant tout traitement, il convient de vérifier s'il existe des intérêts sensibles.

1.6 Traitement de données particulièrement sensibles

Le traitement de données personnelles particulièrement sensibles[11] ne peut s'opérer que si ce traitement est requis par la loi ou si l'intéressé y a expressément consenti. Le traitement de ces données est également licite s'il est impérativement requis pour faire valoir, exercer ou défendre des droits à l'égard de l'intéressé. Le délégué général à la protection des données doit être informé en amont dès lors que le traitement de données sensibles est envisagé.

1.7 Décisions automatisées individuelles

Les procédures de traitement automatisé de données à caractère personnel s'accompagnant d'une évaluation de certains critères touchant à la personnalité (tels que la solvabilité) doivent satisfaire à des conditions particulières. Elles ne doivent pas constituer l'unique fondement de décisions susceptibles d'avoir des conséquences juridiques négatives pour l'intéressé ou de lui porter un préjudice majeur. En outre, l'intéressé doit être informé du fait qu'une décision automatisée a eu lieu et du résultat de cette décision ; il doit également avoir la possibilité de prendre position à ce sujet. Afin d'éviter toute décision erronée, une supervision et un contrôle de plausibilité doivent être assurés par un collaborateur.

1.8 Données utilisateurs et Internet

Lorsque des données à caractère personnel sont collectées, traitées et utilisées sur des sites Internet ou dans le cadre d'applications, les personnes concernées doivent en être informées dans des mentions relatives à la protection des données, voire à l'utilisation de cookies. Les mentions relatives à la protection des données ou aux cookies doivent être intégrées de manière à être facilement repérables, immédiatement accessibles et disponibles à tout moment pour les personnes concernées.
Si des profils utilisateurs sont générés aux fins d'analyse du comportement des utilisateurs de sites Internet et d'applications (« traçage »), les personnes concernées doivent dans tous les cas en être informées dans les mentions relatives à la protection des données. Le « traçage » d'un utilisateur ne peut avoir lieu que si la législation nationale l'autorise ou si la personne autorisée y a consenti. Si le « traçage » s'effectue sous un pseudonyme, l'intéressé doit se voir offrir une option de retrait (opt-out) qui figurera dans les mentions relatives à la protection des données. Si, dans le cadre de la visite de sites Internet ou de l'utilisation d'applications, il est donné la possibilité d'accéder à des données à caractère personnel via un espace réservé aux personnes inscrites, l'identification et l'authentification des personnes concernées doivent s'effectuer sous une forme offrant une protection appropriée pour le type d'accès considéré.

[11] Cf. art. XV.

2. Données collaborateurs

2.1 Traitement de données dans le cadre d'une relation de travail

Le traitement des données à caractère personnel nécessaires à l'établissement, à l'exécution ou à la cessation du contrat de travail est autorisé dans le cadre de la relation de travail. De même, le traitement des données personnelles des candidats est licite dans la phase initiale de la relation de travail. Les données d'un candidat non retenu doivent être supprimées dans le respect des délais requis pour l'apport de preuves, à moins que le candidat ait donné son consentement à une prolongation de l'enregistrement de ses données en prévision d'une procédure de recrutement ultérieure. Le consentement du candidat est également nécessaire pour permettre le recours aux données dans le cadre d'autres procédures de recrutement ou préalablement à leur communication à d'autres sociétés du groupe.

Dans le cadre d'une relation de travail existante, le traitement des données doit toujours être rattaché à la finalité du contrat de travail, dans la mesure où aucune des autorisations de fait ci-après n'intervient.

Si, dans la phase initiale de la relation de travail ou au cours de celle-ci, un complément d'information sur le candidat doit être obtenu auprès d'un tiers, il convient alors d'observer les dispositions légales nationales applicables. En cas de doute, il est nécessaire de solliciter le consentement du candidat.

Le traitement de données à caractère personnel effectué dans le contexte de la relation de travail, sans pour autant servir en premier lieu à l'exécution du contrat de travail, doit être justifié par un motif juridique légitime. Il pourra s'agir d'exigences légales, de réglementations collectives avec les organes de représentation des salariés, d'un consentement du collaborateur ou d'intérêts légitimes de l'entreprise.

2.2 Traitement de données du fait d'une autorisation légale

Le traitement de données à caractère personnel des collaborateurs est également licite dans les cas où celui-ci est exigé, posé comme condition ou admis du fait de dispositions légales nationales. La nature et l'étendue du traitement des données doivent être nécessaires au traite- ment autorisé et définies en fonction de ces prescriptions légales. En présence d'une marge de manœuvre légale, les intérêts sensibles du collaborateur doivent être pris en considération.

2.3 Réglementations collectives relatives au traitement des données

Si le traitement dépasse le cadre de la simple exécution d'un contrat, il est licite pour autant qu'il soit légitimé par une réglementation collective. Les réglementations collectives englobent les conventions collectives ou les conventions passées entre l'employeur et les organes de re- présentation des salariés, dans le cadre des possibilités offertes par le droit du travail applicable. Les réglementations, qui doivent couvrir la finalité concrète du traitement souhaité, peuvent être formulées dans le cadre des dispositions prévues par la législation nationale relative à la protection des données.

2.4 Consentement au traitement des données

Le traitement de données de collaborateurs peut avoir lieu sur la base du consentement donné par le collaborateur intéressé. Les déclarations de consentement doivent être formulées selon le principe de la libre volonté. Tout consentement donné sur une base non volontaire est réputé sans effet. La déclaration de consentement doit être systématiquement établie sous forme écrite ou électronique afin de pouvoir être utilisée pour les nécessités de la preuve.

Si, à titre exceptionnel, les circonstances ne le permettent pas, le consentement peut être accordé par oral. L'octroi du consentement doit dans tous les cas être correctement documenté. Le consentement peut également être accordé de manière implicite par la communication volontaire de données par l'intéressé, dès lors que le droit national ne prescrit pas de consentement explicite. Avant toute demande de consentement, l'intéressé doit être informé conformément à l'art. IV., al. 3., de la présente directive relative à la protection des données.

2.5 Traitement de données du fait d'un intérêt légitime

Le traitement de données à caractère personnel de collaborateurs est également possible lorsqu'il sert un intérêt légitime. Les intérêts légitimes sont généralement d'ordre juridique (par exemple le fait de faire valoir, d'exercer ou de défendre des droits, par exemple) ou économique (évaluations d'entreprises, par exemple).

Le traitement de données à caractère personnel du fait d'un intérêt légitime ne peut avoir lieu dès lors qu'il existe, dans un cas particulier, une raison de penser que les intérêts sensibles du collaborateur prévalent sur l'intérêt à procéder au traitement. Avant tout traitement, il convient de vérifier s'il existe des intérêts sensibles.

Les mesures de contrôle requérant le traitement de données de collaborateurs ne peuvent être appliquées qu'en présence d'une obligation légale ou d'un motif fondé. Même en cas de motif fondé, il convient de vérifier que le principe de proportionnalité est respecté. A cet effet, il convient de pondérer les intérêts légitimes de l'entreprise à l'exécution de la mesure de contrôle (respect des dispositions légales et des règlements internes à l'entreprise, par exemple) et les éventuels intérêts sensibles du collaborateur concerné à l'exclusion de cette mesure. Les contrôles ne devront être effectués que s'ils sont proportionnés. L'intérêt légitime de l'entreprise et les éventuels intérêts sensibles des collaborateurs doivent être déterminés et documentés avant toute mesure. Par ailleurs, il convient, le cas échéant, de prendre en considération les exigences complémentaires découlant de la législation nationale (droits de cogestion des organes de représentation des salariés, droits à l'information des intéressés, par exemple).

2.6 Traitement de données particulièrement sensibles

Les données personnelles particulièrement sensibles ne doivent être traitées que dans certaines conditions définies. Par données sensibles, on entend des données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la santé ou à la vie sexuelle de l'intéressé. Selon la législation nationale, d'autres catégories de données peuvent également être considérées comme particulièrement sensibles ; le contenu des catégories peut également être défini différemment. De même, le traitement de données relatives aux délits est souvent soumis à des conditions définies par la législation nationale.
Le traitement des données doit être expressément autorisé ou prescrit par la législation nationale. Par ailleurs, un traitement des données peut être autorisé lorsqu'il s'avère nécessaire pour permettre au service responsable d'exercer ses droits et d'assumer ses devoirs dans le domaine du droit du travail. Le collaborateur a également la possibilité de donner son consentement exprès au traitement des données le concernant.

Le délégué général à la protection des données doit être informé en amont dès lors que le traite- ment de données sensibles est envisagé.

2.7 Décisions automatisées

Dans le cadre de la relation de travail, les procédures de traitement automatisé de données à caractère personnel s'accompagnant d'une évaluation de certains critères touchant à la personnalité (par exemple dans le cadre du recrutement de candidats ou de l'évaluation de profils de compétence) doivent satisfaire à des conditions particulières. Elles ne doivent pas constituer l'unique fondement de décisions susceptibles d'avoir des conséquences négatives pour le collaborateur concerné ou de lui porter un préjudice majeur. Afin d'éviter toute décision erronée, il convient, dans le cadre d'une procédure automatisée, de garantir que les faits sont évalués par une personne physique et que la décision est prise sur la base de cette évaluation. En outre, le collaborateur concerné doit être informé du fait qu'une décision automatisée a eu lieu et du résultat de cette décision ; il doit également avoir la possibilité de prendre position à ce sujet.

2.8 Télécommunications et Internet

Les installations téléphoniques, adresses électroniques, sites Intranet et Internet ainsi que les réseaux sociaux internes sont en premier lieu mis à disposition par l'entreprise dans le cadre d'une mission professionnelle. Ce sont à la fois des moyens de travail et des ressources pour l'entreprise. Ces moyens peuvent être utilisés dans le cadre de la réglementation en vigueur et des directives internes à l'entreprise. Dès lors que l'usage à titre privé de ces moyens est autorisé, il convient de respecter le secret des télécommunications ainsi que la législation nationale en vigueur en la matière, dans la mesure où ces dispositions s'appliquent.

Aucune surveillance générale n'est mise en place pour les communications par téléphone ou par mail, ni pour l'utilisation d'Intranet et d'Internet. Afin de lutter contre d'éventuelles menaces visant l'infrastructure informatique ou des utilisateurs individuels, des mesures de protection peuvent être mises en œuvre au niveau des interfaces avec le réseau du groupe NITTEL®. Il pourra s'agir de dispositifs assurant le verrouillage de contenus pouvant causer des dommages techniques ou de mesures servant à analyser les schémas d'attaque informatique. Pour des raisons de sécurité, l'utilisation des installations téléphoniques, des adresses électroniques, de l'Intranet, de l'Internet ainsi que des réseaux sociaux internes peuvent donner lieu à l'établissement d'un compte rendu détaillé sur une période limitée. Toute analyse de données de ce type s'intéressant à une personne donnée doit être fondée sur des soupçons fondés d'infraction aux lois ou aux directives du groupe NITTEL®. Ces contrôles ne peuvent être effectués que par des services enquêteurs et ce, dans le respect du principe de proportionnalité. Il convient alors de respecter la législation nationale applicable ainsi que les dispositions du groupe existant en la matière.

VI. Transmission de données à caractère personnel

La transmission de données à caractère personnel à des destinataires externes ou internes de la société est soumise aux mêmes conditions d'autorisation que le traitement des données à caractère personnel (cf. art. V). Le destinataire des données doit en outre s'engager à n'utiliser ces données qu'aux fins définies.

En cas de transmission de données à un destinataire externe au groupe NITTEL® se trouvant dans un Etat tiers[12], celui-ci est tenu de garantir un niveau de protection des données équivalent à celui exigé par la présente directive.

[12] Cf. art. XV.

[13] Cf. art. XV.

VII. Traitement de données dans le cadre d'un mandat

Le traitement de données dans le cadre d'un mandat consiste à confier le traitement de données à caractère personnel à un prestataire de services, sans que la responsabilité du processus opérationnel considérée soit reportée sur celui-ci. En tel cas, il convient de conclure un accord relatif au traitement de données dans le cadre d'un mandat et ce, tant avec des prestataires externes qu'entre entreprises du groupe NITTEL®. Dans ce contexte, le donneur d'ordre reste responsable de l'exécution correcte du traitement des données. Le preneur d'ordre n'est autorisé à traiter les données à caractère personnel que dans le cadre des instructions qui lui ont été données par le donneur d'ordre. Lors de l'octroi du mandat, il convient d'observer les règles suivantes, le service donneur d'ordre devant pour sa part garantir la mise en œuvre des mesures spécifiées.

1. Le preneur d'ordre doit être sélectionné en fonction de son aptitude à garantir la mise en œuvre des mesures de protection d'ordre technique et organisationnel indispensables.
2. Le contrat doit être formulé par écrit. Les instructions à respecter dans le cadre du traitement des données et la répartition des responsabilités entre le donneur d'ordre et le preneur d'ordre doivent être stipulées dans des documents dûment archivés.
3. Les normes contractuelles mises à disposition par le délégué général à la protection des données doivent être respectées.
4. Avant tout traitement de données, le donneur d'ordre doit s'assurer que le preneur d'ordre respecte ses obligations. Le preneur d'ordre peut notamment prouver qu'il respecte les exigences applicables en matière de sécurité des données par le biais d'une certification appropriée. Selon le niveau de risque inhérent au traitement des données, le contrôle pourra, le cas échéant, être répété à intervalles réguliers pendant toute la durée du contrat.
5. En cas de traitement de données transfrontalier, il convient de satisfaire aux exigences nationales définies pour le traitement de données à caractère personnel à l'étranger. Le traitement de données à caractère personnel en provenance de l'EEE ne peut en particulier avoir lieu dans un Etat tiers que si le preneur d'ordre fournit la preuve qu'il offre un niveau de sécurité de données équivalent à celui défini par la présente directive. Voici quelques moyens de preuve appropriés :
    a. Convention de clauses contractuelles types de l'UE relatives au traitement de données à caractère personnel dans des Etats tiers avec le preneur d'ordre et d'éventuels sous-traitants.
    b. Participation du preneur d'ordre à un système de certification reconnu par l'UE visant à garantir un niveau de sécurité des données approprié.
    c. Reconnaissance, par les autorités de surveillance compétentes en matière de protection des données, des règlements internes du preneur d'ordre visant à garantir un niveau de sécurité des données approprié.

VIII. Droits de l'intéressé

Tout intéressé peut faire valoir les droits exposés ci-après. L'examen, par le service responsable, des droits revendiqués doit avoir lieu sans délai, et ne doit causer aucun préjudice à l'intéressé.

1. L'intéressé peut exiger des renseignements sur la nature des données personnelles enregistrées le concernant, leur origine et l'usage auquel elles sont destinées. Si, dans le cadre d'une relation de travail, la législation du travail respective prévoit un droit de

regard sur les informations conservées par l'employeur (dossiers personnels des collaborateurs), ce droit est intégralement préservé.

2. En cas de transmission de données à caractère personnel à des tiers, il convient également d'indiquer l'identité du destinataire ou les catégories de destinataires.
3. S'il s'avère que des données à caractère personnel sont inexactes ou incomplètes, l'intéressé est en droit d'exiger qu'elles soient rectifiées ou complétées.
4. L'intéressé peut s'opposer au traitement de ses données à caractère personnel à des fins de publicité, d'études de marché et de sondages d'opinion. Les données doivent alors être verrouillées pour ces usages.
5. L'intéressé est en droit d'exiger la suppression de ses données s'il s'avère que le traitement des données n'a pas ou plus de fondement juridique. Il en va de même si la finalité du traitement des données est caduque ou n'a plus lieu d'être pour d'autres raisons. Il convient dans ce contexte de tenir compte des obligations légales de conservation des données et des intérêts sensibles s'opposant à la suppression des données.
6. L'intéressé dispose d'un droit d'opposition fondamental au traitement de ses données qu'il convient de respecter dès lors que son intérêt légitime prévaut, en raison d'une situation personnelle particulière, sur l'intérêt du traitement. Cette disposition ne s'applique pas si le traitement des données est prescrit par la loi.

L'intéressé peut en outre faire valoir les droits qui lui sont concédés au titre des arts. III. al. 2, IV., V., VI., IX., X et XIV. al. 3 en tant que tiers bénéficiaire lorsqu'une entreprise qui s'était engagée à observer la directive relative à la protection des données n'en a pas respecté les dispositions et que ses droits ont été violés de ce fait.

IX. Confidentialité du traitement

Les données à caractère personnel sont soumises au secret. Toute collecte, traitement ou utilisation illicites sont interdits aux collaborateurs. Est considéré comme illicite tout traitement entrepris par un collaborateur sans y avoir été initié ni dûment autorisé dans le cadre de l'exercice de ses fonctions. Il convient d'appliquer le principe de la connaissance sélective (« need to know ») : les collaborateurs ne sont autorisés à accéder à des données à caractère personnel que dans les cas et dans la mesure où cela est nécessaire dans le cadre de leurs fonctions respectives. Cela implique une répartition et une séparation minutieuses des rôles et des compétences ainsi qu'un suivi de leur mise en œuvre et de leur mise à jour dans le cadre de schémas d'habilitation.

Il est interdit aux collaborateurs d'utiliser des données à caractère personnel à des fins privées ou commerciales, de les transmettre à des personnes non autorisées ou de leur en concéder l'accès d'une toute autre façon. Avant l'embauche, les supérieurs hiérarchiques doivent informer leurs collaborateurs de l'obligation d'observer la confidentialité des données. Cette obligation se poursuit également au-delà de la période d'emploi.

X. Sécurité du traitement

Les données à caractère personnel doivent être protégées à tout moment contre tout accès non autorisé, traitement ou transmission illicite, ainsi que contre toute perte, falsification ou destruction. Ceci s'applique tant au traitement des données sous forme électronique que sur papier. Avant l'introduction de nouvelles méthodes de traitement des données, et notamment de nouveaux systèmes informatiques, il convient de définir et de mettre en œuvre des mesures techniques et organisationnelles appropriées afin d'assurer la

protection des données à caractère personnel. Ces mesures doivent être conformes aux évolutions techniques, aux risques inhérents au traitement des informations et au degré de protection requis pour les données considérées (résultant du processus de classification des informations). Le service responsable peut à cet effet demander conseil à son délégué à la sécurité de l'information (ISO) ainsi qu'au coordinateur chargé des questions de protection des données. Les mesures de protection des données à caractère personnel d'ordre technique et organisationnel font partie d'un système de gestion de la sécurité de l'information mis en place à l'échelle du groupe. Elles doivent donc sans cesse être adaptées aux évolutions techniques et changements structurels.

XI. Contrôle en matière de protection des données

Le respect des directives de protection des données ainsi que de la législation applicable en la matière est vérifié à intervalles réguliers par le biais d'audits et autres contrôles de sécurité des données. L'exécution de ces contrôles est du ressort du délégué général à la protection des données, des coordinateurs en charge des questions de protection des données, d'autres services dotés de droits d'audit ou d'auditeurs externes mandatés à cet effet. Les résultats des contrôles doivent être communiqués au délégué général à la protection des données. La direction doit être informée des principaux résultats dans le cadre des obligations de rapport respectivement définies. Sur requête, les résultats des contrôles de protection des données doivent être mis à la disposition des autorités de surveillance compétentes en matière de protection des données. Dans le cadre des attributions qui leur sont octroyées en vertu du droit national, ces autorités peuvent également procéder à leurs propres contrôles afin de vérifier le respect des dispositions de la présente directive.

XII. Incidents de sécurité des données

Chaque collaborateur est tenu de signaler sans délai à son supérieur hiérarchique, au coordinateur chargé des questions de protection des données ou au délégué général à la protection des données, tous cas d'infraction à la présente directive ou à d'autres dispositions en matière de protection des données à caractère personnel (incidents de sécurité des données[14]). Le cadre responsable du service ou de l'unité a l'obligation d'informer immédiatement le coordinateur compétent chargé des questions de protection des données ou le délégué général à la protection des données des incidents de sécurité des données.
En cas
» de transmission illicite de données à caractère personnel à des tiers,
» d'accès illicite à des données à caractère personnel par des tiers, ou
» de pertes de données à caractère personnel, les signalements prévus au sein de l'entreprise (Information Security Incident Management) doivent être effectués sans délai afin de satisfaire aux obligations légales de déclaration d'incidents de sécurité des données du pays respectif.

XIII. Responsabilités et sanctions

La direction est responsable du traitement des données dans leur domaine de responsabilité respectif. Il est ainsi tenu de garantir le respect des dispositions légales et des exigences de sécurité des données formulées dans la directive relative à la protection des données (obligations de déclaration nationales). Il appartient aux cadres, dans le cadre de leur mission de management, de garantir, par la mise en place de mesures techniques et organisationnelles, un traitement des données en bonne et due forme respectant les impératifs

de protection des données. La mise en œuvre de ces prescriptions est de la responsabilité du collaborateur compétent. En cas de contrôles de sécurité des données par une autorité publique, le délégué général à la protection des données doit être informé immédiatement.

La direction doit nommer un coordinateur chargé des questions de protection des données.

Les experts responsables de processus commerciaux et de projets doivent informer en temps utile les coordinateurs chargés des questions de protection des données des nouvelles procédures de traitement de données à caractère personnel. Dans le cadre de projets de traitement de données susceptibles de présenter des risques spécifiques quant aux droits de la personnalité des personnes concernées, il convient d'impliquer le délégué général à la protection des données avant le début du traitement. Cette disposition s'applique de manière spécifique aux données à caractère personnel particulièrement sensibles.

Les cadres doivent s'assurer que leurs collaborateurs sont formés dans toute la mesure requise à la protection des données.

Dans de nombreux pays, le traitement abusif de données à caractère personnel ou autres violations de la législation font l'objet de poursuites judiciaires et peuvent donner lieu au versement de dommages et intérêts. Toute infraction imputable à des collaborateurs peut entraîner des sanctions en vertu du droit du travail.

[14] Cf. art. XV.

XIV. Délégué à la protection des données

En tant qu'organe interne indépendant, le commissaire à la protection des données agit en faveur du respect des réglementations nationales et internationales en matière de protection des données. Il est responsable des directives relatives à la protection des données et en contrôle le respect.
Le commissaire à la protection des données est nommé par la direction.

Tout intéressé peut s'adresser au commissaire à la protection des données en charge des questions de protection des données qui lui a été désigné pour lui soumettre des suggestions, des questions, des demandes de renseignements ou des réclamations en rapport avec la protection ou la sécurité des données. A sa demande, ses requêtes et réclamations seront traitées dans le respect des règles de confidentialité.

Le délégué du groupe et ses collaborateurs peuvent être contactés à l'adresse suivante :

Beatrix Lippke
Nittel GmbH & Co KG, Frankfurter Straße 85, 65479 Raunheim
E-mail : beatrix.lippke@nittel.com
Téléphone: +49 (0)6142-946785

XV. Définitions

» La commission européenne reconnaît à un pays tiers un niveau de protection des données approprié lorsque les principes fondamentaux de respect de la vie privée, tels qu'ils sont unanimement entendus par les Etats membres de l'Union européenne, sont préservés pour l'essentiel. Lors de sa décision, la Commission européenne prend en considération l'ensemble des circonstances intervenant lors d'une transmission de données ou jouant un rôle pour une catégorie de transferts de données. Ce processus inclut l'appréciation du droit national ainsi que des règles professionnelles et des mesures de sécurité applicables.

» Les données sont réputées anonymisées lorsque personne ne peut plus durablement établir de lien avec une personne précise ou que le lien avec la personne ne pourrait être restauré qu'au prix d'efforts démesurés en termes de temps, de coûts et de ressources humaines.

» Par données particulièrement sensibles, on entend des données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, à la santé ou à la vie sexuelle de l'intéressé. En vertu de la législation nationale, d'autres catégories de données peuvent être qualifiées de sensibles. Le contenu des catégories de données peut également être défini différemment. De même, le traitement de données relatives aux délits est souvent soumis à des conditions particulières définies par la législation nationale.

» Par intéressé, au sens de la présente directive relative à la protection des données, on entend toute personne physique dont les données font l'objet d'un traitement. Dans certains pays, des personnes morales peuvent également être assimilées aux intéressés.

» Par incident de sécurité des données, on entend l'ensemble des événements pour lesquels il existe des présomptions fondées d'espionnage, de prélèvement, de modification, de copie, de transfert ou d'utilisation illégaux de données à caractère personnel. Ce terme peut se rapporter à des actes commis par tant par des tiers que par des collaborateurs.

» Le tiers désigne toute personne à l'exception de l'intéressé et du service responsable du traitement des données. Au sein de l'Union européenne, les personnes chargées du traitement ne sont pas considérées comme des tiers, étant donné qu'elles sont rattachées au service responsable du traitement.

» Par Etat tiers au sens de la directive relative à la protection des données, on entend tout Etat situé hors de l'Union européenne/EEE. Sont exceptés les Etats dont le niveau de protection des données a été jugé adéquat par la Commission européenne.

» Le consentement est une déclaration volontaire et juridiquement contraignante indiquant que l'on accepte le traitement de données.

» Le traitement de données à caractère personnel est nécessaire lorsque la finalité légale ou l'intérêt légitime ne peut être assuré sans les données à caractère personnel considérées ou alors seulement moyennant un effort démesuré.

» L'Espace économique européen (EEE) est un espace économique associé à l'Union européenne auquel appartiennent la Norvège, l'Islande et le Liechtenstein.

» Les données à caractère personnel désignent toutes les informations concernant une personne physique déterminée ou déterminable. Une personne est déterminable lorsque, notamment, le lien avec la personne peut être établi grâce à une combinaison d'informations et de quelques connaissances supplémentaires, même obtenues de manière fortuite.

» Par transmission, on entend toute communication, par le service responsable, de données protégées à des tiers.

» Le traitement de données à caractère personnel désigne toute opération effectuée avec ou sans l'aide de procédés automatisés, et notamment la collecte, l'enregistrement, l'organisation, la conservation, la modification, la consultation, l'utilisation, la transmission, la diffusion, la combinaison et le rapprochement de données. Cela comprend également la destruction, la suppression et le verrouillage de données et de supports de données.