Règlement général sur la protection des données

Sommaire

Introduction 2
1. Champ d'application territorial 3
2. Destinataires de la présente directive/responsabilités/sanctions 3

3. Principes de base du traitement des données à caractère personnel 4
3.1. Traitement loyal et licéité 4
3.2. Limitation des finalités 5
3.3. Transparence 5
3.4. Minimisation des données et abstention de collecte 5
3.5. Effacement 5
3.6. Exactitude factuelle et actualité des données 5
3.7. Confidentialité et sécurité des données 5
4. Licéité du traitement des données à caractère personnel 6
4.1. Principes du traitement des données 6
4.2. Consentement 7
4.3. Traitement des données à des fins publicitaires 7
4.4. Traitement des données pour une relation contractuelle 8
4.5. Traitement des données sur la base d'une autorisation légale 8
4.6. Intérêts légitimes prioritaires 8
4.7. Traitement de données nécessitant une protection particulière 9
4.8. Données des utilisateurs et Internet 9
4.9. Traitement en vue de l'établissement/de l'exécution d'une relation de travail 10
5. Transfert de données à caractère personnel 11
6. Obligations en cas de sous-traitance 11
7. Droits des personnes concernées 12
8. Confidentialité 13
9. Contrôle de la protection des données/rapport 13
10. Incidents de protection des données 14
11. Mesures de sécurité techniques et organisationnelles 15
12. Niveaux de protection 18
13. Définitions 18
Annexe 1 : Conformité PCI-DSS 21

Introduction

La présente directive règle la protection des données à caractère personnel dans le cadre de l'activité commerciale du CHROMOS Group.

La protection des données à caractère personnel est pour le CHROMOS Group une préoccupation essentielle. C'est pourquoi les entreprises du CHROMOS Group traitent les données à caractère personnel de leurs employés, de leurs clients et de leurs partenaires commerciaux conformément aux dispositions légales applicables en matière de protection des données à caractère personnel et de sécurité des données.

Le CHROMOS Group est dépendant des données et des informations ainsi que des processus commerciaux électroniques qui en découlent. L'exactitude, l'intégrité et la disponibilité des données et des informations sont d'une grande importance pour le CHROMOS Group.

1. Champ d'application territorial

La présente directive est applicable à tous les traitements (cf. point 13 m) de données à caractère personnel (cf. point 13 k) au sein du CHROMOS Group, quel que soit le lieu du traitement.

2. Destinataires de la présente directive/responsabilités/sanctions

La présente directive s'adresse à tous les employés des entreprises du CHROMOS Group afin de garantir de façon efficace un traitement des informations conforme à la protection des données, une sécurité des données et des réactions adaptées aux demandes de traitement des données des personnes concernées (cf. point 13 d).

Les **Directions** des entreprises du CHROMOS Group assument la responsabilité globale pour la protection des données et la mise en œuvre des dispositions du droit de la protection des données dans les entreprises correspondantes. Elles sont ainsi tenues de garantir par des mesures organisationnelles, personnelles et techniques un traitement des données en bonne et due forme effectué dans le respect des exigences légales de protection des données et des exigences de protection des données contenues dans la présente directive de protection des données. La mise en œuvre de ces dispositions est la responsabilité des employés compétents. Le délégué à la protection des données compétent doit être informé immédiatement de tout contrôle de la protection des données par les autorités. Sauf disposition contraire, tous les membres de la direction en question sont responsables conjointement (art. 26, par. 1 du RGPD).

Chaque employé est responsable dans son domaine de responsabilité du respect des dispositions du droit de la protection des données dans le cadre des prescriptions de l'entreprise et en particulier de la mise en œuvre continue de la présente directive. Par ailleurs, tous les employés du CHROMOS Group sont constamment formés concernant les dispositions du droit de la protection des données.

En plus du contrôle de leur propre domaine de responsabilité, les **responsables de département** doivent également veiller à ce que leurs employés (le cas échéant, également les employés temporaires) et/ou les personnes prenant part aux processus soient informés de la présente directive. En ce qui concerne la collecte/le traitement des données, ils ont également pour responsabilité dans leur département :

- de mettre à disposition les ressources matérielles et humaines nécessaires au respect des dispositions de la directive,
- de veiller à une surveillance adéquate du respect des dispositions de la directive,
- de veiller à la satisfaction des obligations d'information vis-à-vis des personnes concernées,
- de veiller à la réalisation des descriptions des processus prescrites,
- de veiller à la réalisation des analyses d'impact relatives à la protection des données prescrites et
- d'informer régulièrement le délégué à la protection des données compétent (cf. point 13 j) sur la collecte et le traitement des données à caractère personnel dans son département.

Les **délégués à la protection des données compétents** (cf. point 13 j) des entreprises du CHROMOS Group conseillent les directions et les autres employés des entreprises dans la mise en œuvre de la présente directive et vérifient qu'elle est respectée. Ils tiennent un registre des activités de traitement pour l'entreprise concernée du CHROMOS Group conformément à l'art. 30 du RGPD et traitent les demandes d'accès/de rectification ainsi que les oppositions des personnes concernées relevant du droit de la protection des données. Au moins une fois par an, ils soumettent les mesures de protection des données techniques et organisationnelles (cf. point 11) à un contrôle (cf. point 9) en collaboration avec les responsables de la sécurité informatique.

Les **responsables de la sécurité informatique** organisent et assistent les délégués à la protection des données dans la création du registre des activités de traitement. Le responsable de la sécurité informatique propose des mesures techniques et organisationnelles afin de garantir le respect de la présente directive pour le CHROMOS Group. Les mesures sont documentées à la section 11. Toutes les mesures conformément à la présente directive sont contrôlées régulièrement par les responsables de la sécurité informatique et ces contrôles sont documentés.

Le **Département RH** satisfait les droits d'accès et d'information des employés.

Dans de nombreux États, tout traitement abusif des données à caractère personnel ou tout autre manquement au droit de la protection des données peut avoir des conséquences pénales et donner lieu à des dommages et intérêts. Les infractions dont les employés sont responsables individuellement peuvent entraîner des sanctions en matière de droit du travail.

3. Principes de base du traitement des données à caractère personnel

3.1. Traitement loyal et licéité

Les droits de la personnalité des personnes concernées (cf. point 13 d) sont garantis dans le cadre du traitement des données à caractère personnel au sein du CHROMOS Group. Les données à caractère personnel sont collectées et traitées de façon licite et loyale.

3.2. Limitation des finalités

Le traitement des données à caractère personnel peut uniquement avoir lieu pour les finalités ayant été définies avant la collecte des données. Les modifications ultérieures des finalités sont uniquement possibles de façon limitée et requièrent un motif légal.

3.3. Transparence

La personne concernée (cf. point 13 d) doit être informée du traitement de ses données. En principe, les données à caractère personnel doivent être collectées auprès de la personne concernée personnellement. En cas de collecte des données, la personne concernée doit pouvoir au minimum identifier les éléments suivants ou être informée de façon analogue :

- l'identité de l'organisme responsable (cf. point 13 n),
- la finalité du traitement des données,
- les tiers (cf. point 13 f) ou les catégories de tiers auxquels les données ont été transférées le cas échéant.

3.4. Minimisation des données et abstention de collecte

Il convient de vérifier avant tout traitement de données à caractère personnel si et dans quelle mesure un tel traitement est nécessaire pour atteindre la finalité visée avec le traitement. S'il est possible pour atteindre la finalité et si le coût est proportionnel à la finalité visée, des données anonymisées (cf. point 13 b) ou statistiques doivent être utilisées. Les données à caractère personnel ne peuvent pas être conservées en réserve en vue de futures finalités potentielles à moins qu'une telle conservation soit imposée ou autorisée par le droit de l'État concerné.

3.5. Effacement

Les données à caractère personnel n'étant plus nécessaires après l'expiration des délais de conservation légaux ou liés aux processus commerciaux (cf. point 13 h) doivent être effacées. Si, dans des cas individuels, il existe des présomptions d'intérêts légitimes, les données doivent être conservées jusqu'à ce que l'intérêt légitime ait été réglé d'un point de vue juridique.

3.6. Exactitude factuelle et actualité des données

Les données à caractère personnel doivent être enregistrées sous une forme exacte, complète et – si applicable – actuelle. Des mesures appropriées doivent être prises afin de veiller à ce que les données inexactes, incomplètes ou inactuelles soient effacées, rectifiées, complétées ou actualisées.

3.7. Confidentialité et sécurité des données

La confidentialité est assurée concernant les données à caractère personnel. Les données à caractère personnel sont par conséquent traitées de façon confidentielle dans le cadre du traitement individuel et protégées contre un accès non autorisé, un traitement illicite ou une transmission ainsi que contre toute perte, modification ou destruction par des mesures techniques et organisationnelles appropriées.

4. Licéité du traitement des données à caractère personnel

4.1. Principes du traitement des données

Le traitement des données à caractère personnel au sein du CHROMOS Group peut uniquement avoir lieu dans le cadre autorisé par la loi. En principe, seules les informations nécessaires à la réalisation des tâches opérationnelles (cf. point 13 h) et en relation directe avec la finalité du traitement peuvent être collectées et traitées.

Un traitement des données à caractère personnel est uniquement licite si l'une des conditions d'autorisation détaillées ci-après est satisfaite :

- en cas de consentement de la personne concernée (cf. point 4.2),
- afin de satisfaire à des demandes exprimées par le client et en cas de consentement à la publicité (cf. point 4.3),
- en cas de nécessité, afin d'établir/d'exécuter un contrat (cf. point 4.4),
- en cas d'autorisation légale (cf. point 4.5) ou
- en cas d'intérêt légitime, dans la mesure où les intérêts ou libertés et droits fondamentaux de la personne concernée ne prévalent pas (cf. point 4.6).

La finalité des données doit être documentée par écrit avant l'introduction de nouveaux types de traitements par le responsable de l'application. En principe, un changement de finalité est uniquement licite lorsque le traitement est compatible avec les finalités pour lesquelles les données avaient été initialement collectées. Les critères de pondération utilisés dans le cadre du changement de finalité doivent être contrôlés un à un. Par ailleurs, le contrôle doit être lui aussi documenté à des fins de preuve.

Avant l'introduction de nouveaux types de traitements de données à caractère personnel, il convient également de vérifier si la finalité du traitement peut être aussi bien atteinte en cas d'anonymisation (cf. par. 13 b) ou de pseudonymisation des données et si un tel traitement peut être privilégié le cas échéant.

Si d'autres organismes demandent des informations sur la personne concernée, celles-ci peuvent uniquement être fournies sans le consentement de la personne concernée lorsqu'il existe une obligation légale autorisant ce transfert ou lorsqu'il existe un intérêt légitime de l'entreprise procédant à la collecte/au traitement justifiant le transfert et que l'identité du demandeur est définie de manière incontestable. En cas de doute, le délégué à la protection des données compétent doit être consulté.

Les dispositions de la section 4.8 sont applicables aux données à caractère personnel traitées via le site Internet.

Le traitement des données des employés est effectué conformément aux dispositions de la section 4.9.

4.2. Consentement

Un traitement des données peut être effectué sur la base d'un consentement de la personne concernée.

L'acceptation des consentements a toujours lieu en ayant conscience que le consentement de la personne concernée au traitement des données à caractère personnel est donné volontairement. Avant le consentement, la personne concernée doit être informée conformément au point 3.3. Pour cela, une manifestation d'intention fournie sans équivoque par la personne concernée sous la forme d'une déclaration ou d'une autre action de confirmation incontestable, avec laquelle la personne concernée donne son accord au traitement des données vous concernant est nécessaire.

Il doit être possible de justifier de ce consentement (art. 7, par. 1 du RGPD). Dans ce contexte, les déclarations de consentement doivent être obtenues par écrit ou sous forme électronique et enregistrées et/ou conservées. Si, dans des cas convenus avec les délégués à la protection des données compétents, le consentement devait être obtenu à l'oral, par exemple par téléphone, ce consentement doit être documenté précisément et la documentation doit être enregistrée et/ou conservée.

Les consentements accordés avant le 25 mai 2018 sont maintenus dans la mesure où ils satisfont aux exigences de base du RGPD.

4.3. Traitement des données à des fins publicitaires

Les mesures de fidélisation de la clientèle ou publicitaires nécessitent d'autres conditions légales. Le traitement de données à caractère personnel à des fins de prospection ou d'études de marché et de sondages d'opinion est licite dans la mesure où il est compatible avec la finalité pour laquelle les données ont été collectées initialement. Si des données sont collectées exclusivement à des fins publicitaires, la personne concernée les fournit sur une base volontaire. La personne concernée est informée du fait que les données collectées à cette fin sont fournies volontairement. Il convient d'obtenir de la personne concernée un consentement (cf. point 4.2) au traitement de ses données à des fins de prospection. Dans le cadre du consentement, la personne concernée doit pouvoir choisir entre différents moyens de contact disponibles tels que par voie postale, électronique ou par téléphone.

Si une personne concernée s'adresse à une entreprise du CHROMOS Group avec une demande d'informations (par exemple une demande d'envoi de documents d'information concernant une prestation ou un produit), le traitement des données est licite pour l'exécution de cette demande.

Si la personne concernée s'oppose à l'utilisation de ses données à des fins de prospection, une utilisation ultérieure de ses données à cette fin est illicite et les données doivent être bloquées pour cette finalité.

4.4. Traitement des données pour une relation contractuelle

Le traitement des données à caractère personnel pour établir, exécuter et mettre fin à un contrat est licite (art. 6, par. 1, lettre b du RGPD). Ceci inclut également l'accompagnement du partenaire contractuel dans la mesure où un tel accompagnement entre dans le cadre de la finalité du contrat.

Dans le cadre de contrats existants, il est par conséquent possible que des données contractuelles, de base et de facturation du partenaire contractuel, telles que son nom et son adresse soient traitées afin de lui faire parvenir la facture ou la livraison par exemple.

Lors de la phase d'établissement du contrat, le traitement des données à caractère personnel est autorisé afin de créer des offres, de préparer des documents contractuels ou de satisfaire d'autres souhaits de l'intéressé en ce qui concerne la conclusion d'un contrat. En font également partie les processus de traitement des données nécessaires à l'établissement ou à l'exécution de relations de travail.

Les intéressés peuvent être contactés pendant l'établissement du contrat en utilisant les données que vous avez communiquées. Les restrictions éventuellement exprimées par les intéressés doivent être observées.

Pour d'autres mesures publicitaires, les conditions mentionnées au point 4.3 doivent être satisfaites.

4.5. Traitement des données sur la base d'une autorisation légale

Les traitements de données sont également licites s'ils sont nécessaires en raison de dispositions légales. Le fondement juridique pour un tel traitement peut être des dispositions nationales ou communautaires auxquelles nous sommes soumis ou auxquelles les personnes intervenant sont soumises (art. 6, par. 1, lettre c du RGPD).

La nature et l'étendue du traitement des données doivent être nécessaires au traitement licite des données et sont fonction de ces dispositions légales.

C'est par exemple le cas des dispositions du droit commercial et fiscal qui nous imposent pour partie des obligations importantes en matière de documentation et de conservation.

4.6. Intérêts légitimes prioritaires

Le traitement des données à caractère personnel peut uniquement avoir lieu s'il est nécessaire à la défense de nos intérêts légitimes ou des intérêts légitimes d'un tiers (cf. point 13 f). On entend principalement par « intérêt légitime » les intérêts juridiques (notamment le recouvrement de créances) et économiques (par exemple la prévention de défauts d'exécution du contrat).

Un traitement de données à caractère personnel sur la base d'un intérêt légitime ne saurait toutefois avoir lieu lorsqu'il existe au cas par cas des raisons de penser que les intérêts de la personne concernée dignes d'être protégés prévalent sur l'intérêt au traitement (art. 6, par. 1, lettre f du RGPD).

Dans un tel cas, il convient par conséquent de vérifier les intérêts dignes d'être protégés de la personne concernée par le traitement des données. Il convient donc de déterminer dans le cadre d'une pondération globale des intérêts, quels intérêts prévalent – les nôtres ou ceux de la personne concernée. En cas de doute, le délégué à la protection des données compétent doit être consulté.

4.7. Traitement de données nécessitant une protection particulière

Le traitement de données à caractère personnel nécessitant une protection particulière (cf. point 13 c) peut uniquement avoir lieu lorsqu'il est imposé par la loi ou lorsque la personne concernée a donné son consentement explicite. Le traitement de ces données est également licite lorsqu'il est impérativement nécessaire afin de faire valoir, exercer ou défendre des prétentions légales vis-à-vis de la personne concernée.

Si un traitement de données nécessitant une protection particulière est prévu, le délégué à la protection des données compétent (cf. point 13 j) doit en être informé.

Le traitement des données de cartes de crédit est effectué dans le respect des dispositions de conformité PCI-DSS conformément aux mesures décrites à l'Annexe 1 de la présente directive.

4.8. Données des utilisateurs et Internet

Si des données à caractère personnel du CHROMOS Group sont traitées sur des sites Internet ou dans des applications, les personnes concernées doivent en être informées dans les informations sur la protection des données ou dans les informations sur les cookies. Les informations sur la protection des données et, le cas échéant, les informations sur les cookies doivent être intégrées de façon à ce qu'elles soient facilement identifiables, directement accessibles et toujours disponibles pour les personnes concernées.

Si des profils d'utilisation sont créés afin d'évaluer le comportement d'utilisation des sites Internet et des applications (suivi), les personnes concernées en sont toujours informées dans les informations sur la protection des données. Un suivi lié à la personne peut uniquement avoir lieu lorsque la personne concernée y a consenti. Si le suivi est effectué sous un pseudonyme, une possibilité d'opposition doit être donnée à la personne concernée dans les informations sur la protection des données (opt-out).

Si un accès à des données à caractère personnel est rendu possible dans le cadre de sites Internet ou d'applications avec un espace nécessitant une inscription, l'identification et l'authentification de la personne concernée doivent être conçues de façon à ce qu'une protection adaptée soit assurée pour l'accès concerné.

4.9. Traitement en vue de l'établissement/de l'exécution d'une relation de travail

Dans le cadre de l'établissement et de l'exécution de relations de travail, les données à caractère personnel nécessaires à l'établissement, à l'exécution et à la résiliation du contrat de travail sont traitées.

Des données à caractère personnel des candidats peuvent être traitées lors de l'établissement d'une relation de travail. En cas de refus, les données du candidat sont effacées en tenant compte des délais de preuve légaux, à moins que le candidat ait consenti à une conservation ultérieure en vue d'une future procédure de sélection. Un consentement est également nécessaire pour une utilisation des données en vue de procédures de sélection futures ou avant la transmission de la candidature à d'autres entreprises du CHROMOS Group.

Dans le cadre de relations de travail existantes, le traitement des données doit toujours être lié à la finalité du contrat de travail dans la mesure où aucun autre motif de légitimation mentionné précédemment dans la présente section 4 n'est présent.

Si lors de l'établissement de la relation de travail ou dans le cadre d'une relation de travail existante, la collecte d'autres informations sur le candidat est nécessaire auprès d'un tiers (cf. point 13 f), le consentement de la personne concernée doit être obtenu en cas de doute.

Pour les traitements de données à caractère personnel ayant lieu dans un contexte de relation de travail mais ne servant pas initialement à l'exécution du contrat de travail, un motif juridique légitime est nécessaire. Il peut s'agir d'exigences légales, de dispositions collectives à convenir avec les représentants du personnel dans le cadre des dispositions légales, d'un consentement de l'employé ou de nos intérêts légitimes prioritaires (cf. point 4.6). S'il existe une marge de manœuvre légale ou convenue, il doit toujours être tenu compte des intérêts de l'employé dignes d'être protégés.

Les mesures de contrôle nécessitant un traitement des données des employés peuvent uniquement être effectuées sur la base d'une obligation légale ou s'il existe un motif légitime. Même s'il existe un motif légitime, la proportionnalité des mesures de contrôle doit être vérifiée. Les intérêts légitimes de l'entreprise à l'exécution des mesures de contrôle (par exemple le respect des dispositions légales et des règles internes de l'entreprise) doivent être mis en balance avec un éventuel intérêt digne d'être protégé de l'employé concerné par la mesure à l'exclusion de la mesure et peuvent uniquement être effectués s'ils sont raisonnables. L'intérêt légitime de l'entreprise et les éventuels intérêts dignes d'être protégés de l'employé doivent être déterminés et documentés avant chaque mesure. Il doit être tenu compte dans ce cadre des éventuels droits de participation des représentants du personnel et droits d'information des personnes concernées.

Les installations téléphoniques, les comptes de messagerie, l'Intranet et Internet ainsi que les réseaux sociaux internes sont mis à disposition des employés par l'entreprise pour exécuter leurs tâches professionnelles. Ce sont des outils de travail et des ressources de l'entreprise. Ils peuvent être utilisés dans le cadre des dispositions légales applicables et des dispositions internes de

l'entreprise. En cas d'utilisation autorisée à des fins privées, le secret et le droit des télécommunications doivent être observés dans la mesure où il est applicable.

Une surveillance généralisée des communications par téléphone et par e-mail ou de l'utilisation de l'Intranet et d'Internet n'a pas lieu. Afin d'empêcher des attaques sur l'infrastructure informatique ou sur des utilisateurs individuels, des mesures de protection peuvent être mises en place aux points d'accès dans le réseau du CHROMOS Group afin de bloquer les contenus nuisibles d'un point de vue technique ou d'analyser les modèles d'attaques. Pour des raisons de sécurité, l'utilisation des installations téléphoniques, des comptes de messagerie, de l'Intranet et d'Internet ainsi que des réseaux sociaux internes est archivée pendant une durée limitée. Des analyses de ces données liées à des personnes peuvent uniquement être effectuées en cas de soupçon concret justifié de manquement aux lois ou aux dispositions du CHROMOS Group et de ses entreprises. Ces contrôles peuvent uniquement être effectués par des départements d'investigation en respectant le principe de proportionnalité. Les lois applicables et les dispositions existantes de l'entreprise doivent être observées.

5. Transfert de données à caractère personnel

Un transfert des données à caractère personnel à des destinataires en dehors ou au sein du CHROMOS Group est soumis aux conditions de licéité du traitement des données à caractère personnel conformément à la section 4. Le destinataire des données doit être tenu d'utiliser uniquement les données pour les finalités fixées.

En cas de transfert de données à des destinataires en dehors du CHROMOS Group dans un État tiers (cf. point 13 g), ce dernier doit garantir un niveau de protection des données équivalent à celui de la présente directe de protection des données. Ceci ne s'applique pas lorsque le transfert est effectué en raison d'une obligation légale. Une telle obligation légale peut découler du droit national ou le droit national reconnaît l'objectif de traitement des données poursuivi avec l'obligation légale d'un État tiers.

En cas de transfert de données de tiers à des entreprises du CHROMOS Group, il doit être veillé à ce que les données puissent être utilisées aux fins prévues.

6. Obligations en cas de sous-traitance

Il y a sous-traitance lorsqu'un mandataire est chargé du traitement des données à caractère personnel sans que la responsabilité pour le processus commercial correspondant lui soit transférée. Dans de tels cas, un accord de sous-traitance doit être conclu, qu'il s'agisse de mandataires externes ou d'entreprises du CHROMOS Group. Ce faisant, l'entreprise mandante conserve l'entière responsabilité pour l'exécution correcte du traitement des données. Le mandataire peut uniquement traiter des données à caractère personnel dans le cadre des instructions du donneur d'ordre. Les dispositions suivantes doivent être observées lors du mandatement ; le département à l'origine du mandatement doit garantir leur mise en œuvre.

a) Le mandataire est sélectionné en fonction de son aptitude à assurer les mesures de protection techniques et organisationnelles nécessaires.
b) Le mandat doit être confié sous forme écrite. Les instructions concernant le traitement des données et les responsabilités du mandataire et du donneur d'ordre doivent être documentées dans ce cadre.
c) Les normes contractuelles mises à disposition par les délégués à la protection des données compétents doivent être observées.
d) Avant le traitement des données, le donneur d'ordre doit s'assurer du respect des obligations du mandataire. Un mandataire peut notamment prouver qu'il respecte les exigences en matière de sécurité des données en présentant un certificat approprié ou toute autre preuve de sécurité des données adaptée. En fonction du risque auquel est soumis le traitement des données, le contrôle peut le cas échéant être renouvelé pendant la durée du contrat.
e) En cas de sous-traitance transfrontalière, les exigences légales concernant un transfert des données à caractère personnel à l'étranger doivent être satisfaites. En particulier, le traitement des données à caractère personnel provenant de l'Espace économique européen peut uniquement avoir lieu dans un État tiers lorsque le mandataire justifie d'un niveau de protection des données équivalent à celui de la présente directive de protection des données. Des outils adaptés peuvent être :
    (1) la conclusion avec le mandataire et d'éventuels sous-traitants supplémentaires de clauses contractuelles types de l'UE concernant la sous-traitance dans des États tiers,
    (2) la participation du mandataire à un système de certification reconnu par l'UE visant à établir un niveau de protection des données adapté,
    (3) la reconnaissance par les autorités de contrôle de la protection des données compétentes de règles d'entreprise contraignantes du mandataire visant à établir un niveau de protection des données adapté.

7. Droits des personnes concernées

Chaque personne concernée peut exercer les droits suivants. L'exercice de ces droits doit être traité sans délai par le département responsable et ne peut en aucun cas entraîner un préjudice pour les personnes concernées.

a) La personne concernée peut exiger des informations sur les données à caractère personnel enregistrées la concernant et sur la finalité de l'enregistrement. Si, dans le cadre d'une relation de travail, d'autres droits de consultation plus larges en matière de droit du travail sont prévus dans les documents de l'employeur (par exemple dans les dossiers du personnel), ces droits ne sont pas affectés.
b) Si des données à caractère personnel sont transférées à des tiers, des informations sur l'identité du destinataire et sur les catégories de destinataires doivent également être fournies.
c) Si des données à caractère personnel s'avèrent inexactes ou incomplètes, la personne concernée peut exiger qu'elles soient rectifiées ou complétées.

d) La personne concernée peut s'opposer au traitement de ses données à caractère personnel à des fins de prospection ou de réalisation d'études de marché et de sondages d'opinion. En cas d'opposition à ces finalités, ses données doivent être bloquées.
e) La personne concernée est autorisée à exiger l'effacement de ses données lorsqu'il n'y a pas de fondement juridique au traitement des données ou que le fondement juridique a disparu. Il en va de même lorsque la finalité du traitement des données disparaît en raison du temps ou pour d'autres raisons. Les obligations de conservation existantes et les intérêts dignes d'être protégés s'opposant à un effacement doivent être observés.
f) La personne concernée dispose d'un droit fondamental d'opposition au traitement de ses données dont il convient de tenir compte lorsque son intérêt légitime découlant de sa situation personnelle particulière prévaut sur l'intérêt au traitement des données. Ceci ne s'applique pas lorsqu'une disposition légale impose la réalisation du traitement.

8. Confidentialité

Les données à caractère personnel sont soumises à la confidentialité des données. Un traitement non autorisé est interdit à l'ensemble des employés du CHROMOS Group. Est considéré comme non autorisé tout traitement effectué par un employé sans que ce traitement lui ait été demandé dans le cadre de l'exécution de ses tâches et sans autorisation.

Les employés peuvent uniquement avoir accès aux données à caractère personnel lorsque et dans la mesure où un tel accès est nécessaire pour l'exécution de leurs tâches. Ceci implique une répartition et une séparation consciencieuses des rôles et des compétences ainsi que leur mise en œuvre et leur maintien dans le cadre des concepts d'autorisation.

Les employés ne sont pas autorisés à utiliser les données à caractère personnel à des fins privées ou économiques personnelles, à les transmettre à des personnes non autorisées ou à les rendre accessibles de toute autre façon.

Tous les employés sont informés au début de la relation de travail de l'obligation de confidentialité et y sont soumis. Cette obligation persiste également après la fin de la relation de travail.

9. Contrôle de la protection des données/rapport

Le respect des directives relatives à la protection des données et des lois applicables sur la protection des données est contrôlé régulièrement, au moins une fois par an, dans le cadre de contrôles de la protection des données. Leur exécution est la responsabilité du délégué à la protection des données compétent, le cas échéant, avec l'aide des responsables de la sécurité informatique ainsi que, le cas échéant, avec l'aide d'autres départements de l'entreprise ou auditeurs externes mandatés disposant de droits d'audit.

Le délégué à la protection des données compétent résume les résultats une fois par an dans un rapport qui doit comporter au minimum les points suivants :

- la description des nouveaux processus,
- les incidents de protection des données,
- les demandes liées à des personnes,

D'autre part, une liste des demandes d'effacement et de rectification des données à caractère personnel à documenter par le délégué à la protection des données doit être jointe au rapport en tant qu'annexe.

Les directions des entreprises du CHROMOS Group doivent être informées des principaux résultats des contrôles de la protection des données. Sur demande, les résultats des contrôles de la protection des données sont mis à disposition des autorités de contrôle de la protection des données. L'autorité de contrôle de la protection des données compétente peut également effectuer ses propres contrôles du respect des dispositions de la présente directive dans le cadre des pouvoirs dont elle dispose en vertu de la loi de l'État.

10. Incidents de protection des données

Chaque employé doit signaler sans délai à son supérieur et au délégué à la protection des données compétent les manquements à la présente directive de protection des données ou à d'autres dispositions de protection des données à caractère personnel (incidents de protection des données, cf. point 13 e).

En cas

- de transmission illicite de données à caractère personnel à des tiers,
- d'accès aux données à caractère personnel par des tiers ou
- de perte de données à caractère personnel,

dans la mesure où l'incident de protection des données entraîne un risque pour la personne concernée, le délégué à la protection des données compétent procède à la notification à l'autorité de contrôle imposée par l'art. 33 du RGPD.

Dans la mesure où

- l'incident de protection des données présente un risque élevé pour les droits et libertés des personnes concernées,
- aucune mesure technique ou organisationnelle adaptée – empêchant l'accès non autorisé aux données à caractère personnel (par exemple un chiffrement) – n'existe et où
- aucune mesure efficace de limitation du dommage – ayant éliminé le risque élevé existant au moment de l'incident de protection des données – n'a été prise,

le délégué à la protection des données compétent procède à la notification de la personne concernée conformément à l'art. 34 du RGPD.

11. Mesures de sécurité techniques et organisationnelles

Les données à caractère personnel doivent être à tout moment protégées contre un accès non autorisé, un traitement ou une transmission illicite ainsi que contre une perte, une falsification ou une destruction. Ceci s'applique que le traitement des données ait lieu par voie électronique ou sur papier. Avant d'introduire de nouvelles procédures de traitement des données, en particulier de nouveaux systèmes informatiques, des mesures techniques et organisationnelles doivent être fixées et mises en œuvre afin de protéger les données à caractère personnel. Ces mesures doivent être axées sur l'état de la technique, les risques découlant du traitement et la nécessité de la protection des données (cf. niveaux de protection conformément à la section 12).

Les mesures sont révisées chaque année et ajustées si nécessaire. La révision et les ajustements sont documentés.

Les mesures techniques et organisationnelles suivantes sont prises dans les entreprises du CHROMOS Group :

Contrôle des accès	Limitation de l'accès des personnes aux locaux afin d'empêcher des personnes non autorisées d'accéder à des installations de traitement des données avec lesquelles des données à caractère personnel sont traitées ou utilisées.	• Données du niveau de protection A : Système de verrouillage du bâtiment ou gardien ; pièces dans des bâtiments non verrouillables, postes de travail normaux • Postes de travail avec accès aux données des niveaux de protection C et D ; portes supplémentaires verrouillables, • salles de serveurs ; système anti-intrusion, accès sécurisé par un protocole, pas de fenêtres, pour les données de tous les niveaux de protection
Contrôle de l'accès	Restriction de l'accès aux données et aux appareils de traitement des données afin d'empêcher que les systèmes de traitement des données ne puissent être utilisés par des personnes non autorisées	• Données des niveaux de protection A à C ; poste de travail normal (incl. un environnement virtuel) avec contrôle AD sans accès externe. • Données des niveaux de protection A et B ; poste de travail normal avec accès externe via Internet. Couche de sécurité supplémentaire séparée (Netscaler) • Accès au serveur ; pour les données de tous les niveaux de protection, authentification séparée (soit AD plus Admin-AD soit AD pour PC plus connexion locale au serveur)

Contrôle de l'accès	Restriction de l'accès aux données au sein d'une application afin de garantir que les personnes autorisées à utiliser un système de traitement des données puissent uniquement accéder aux données concernées par leur autorisation d'accès, et que les données à caractère personnel ne soient pas lues, copiées, modifiées ou effacées de façon illicite lors du traitement, de l'utilisation et après leur enregistrement	• Application pour les données du niveau de protection A : aucun droit ni aucune attribution de rôles • Application pour les données du niveau de protection B : connexion simple à l'application • Application pour les données du niveau de protection C : droits et concept de rôles • Application pour les données du niveau de protection D : droits et concept de rôles, deux facteurs authentification • Pour le traitement de données à caractère personnel de tous les niveaux de protection ayant un caractère public/juridique (assurance sociale, agence pour l'emploi, tribunal, etc.), les contrôles d'accès prescrits par l'unité fiscale publique/juridique doivent être utilisés.
Contrôle du transfert	Il convient d'empêcher que des données à caractère personnel soient lues, copiées, modifiées ou effacées sans autorisation lors du transfert électronique ou du transport ou lors de l'enregistrement sur des supports de données et d'empêcher qu'il soit possible de déterminer où de telles données doivent être transmises dans le système informatique.	• Données des classes de protection A et B : aucune restriction supplémentaire, en cas de transfert en ligne chiffrement du transfert (https) • Données du niveau de protection C : archivage supplémentaire de la transmission (archivé dans Microsoft Navision) • Données du niveau de protection D : chiffrement supplémentaire du contenu • Pour le traitement de données à caractère personnel de tous les niveaux de protection ayant un caractère public/juridique (assurance sociale, agence pour l'emploi, tribunal, etc.), les contrôles du transfert prescrits par l'unité fiscale publique/juridique doivent être utilisés.

Contrôle de la saisie	Il convient de veiller à ce qu'il soit possible de vérifier a posteriori si et par qui des données à caractère personnel ont été saisies, modifiées ou effacées.	• Données du niveau de protection A : un contrôle de la saisie n'est pas nécessaire • Données des niveaux de protection B et supérieurs : Archivage du traitement • Pour le traitement de données à caractère personnel de tous les niveaux de protection ayant un caractère public/juridique (assurance sociale, agence pour l'emploi, tribunal, etc.), les contrôles de saisie prescrits par l'unité fiscale publique/juridique doivent être utilisés.
Contrôle de la sous-traitance	Il convient de veiller à ce que les données à caractère personnel traitées en sous-traitance soient traitées conformément aux instructions du donneur d'ordre.	• Création d'un concept de sécurité des données (TOM) en fonction du niveau de protection selon ce modèle
Contrôle de la disponibilité	Il convient de veiller à ce que les données à caractère personnel soient protégées contre une destruction ou une perte accidentelle.	• Données du niveau de protection A : Protection contre les virus • À partir des données du niveau de protection B : instantanés supplémentaires, concept de sauvegarde • À partir des données du niveau de protection C : climatisation supplémentaire, ASI • À partir des données du niveau de protection D : conservation supplémentaire dans des endroits séparés • Pour le traitement de données à caractère personnel de tous les niveaux de protection ayant un caractère public/juridique (assurance sociale, agence pour l'emploi, tribunal, etc.), les contrôles de disponibilité prescrits par l'unité fiscale publique/juridique doivent être utilisés.
Règle de séparation	Il convient de veiller à ce que les données à caractère personnel collectées à des fins différentes puissent être traitées séparément.	• Pour les données de tous les niveaux de protection ; séparation des donneurs d'ordre, sociétés

12. Niveaux de protection

Afin de pouvoir évaluer les mesures de sécurité techniques et organisationnelles (cf. point 11) quant à leur adéquation, les données à caractère personnel doivent être subdivisées en fonction du préjudice potentiel (degré de dommage possible pour les intérêts dignes d'être protégés) dans les niveaux de préjudice/protection suivants :

Niveau A :
Les données accessibles librement pouvant être consultées sans que la personne les consultant ait besoin de faire valoir un intérêt légitime, par exemple les répertoires, les registres de membres, les annuaires papier et en ligne.

Niveau B :
Les données à caractère personnel dont une utilisation abusive n'entraînerait pas d'atteinte particulière mais liées à un intérêt légitime de la personne les consultant, par exemple les dossiers publics à accès limité, les commandes de clients, les contrats avec des partenaires commerciaux.

Niveau C :
Les données à caractère personnel dont une utilisation abusive pourrait nuire à la personne concernée dans sa position au sein de la société ou dans ses relations économiques (« réputation ») par exemple les revenus, les prestations sociales, les impôts fonciers, les infractions, les contrats de travail (sans les données de santé).

Niveau D :
Les données à caractère personnel dont une utilisation abusive pourrait considérablement nuire à la position au sein de la société ou aux relations économiques de la personne concernée (« existence »), par exemple les infractions lourdes, les évaluations professionnelles, les résultats d'examens médicaux ou psychologiques, les dettes, les saisies, les insolvabilités.

Niveau E :
Les données dont une utilisation abusive peut nuire à la santé, à la vie ou à la liberté de la personne concernée, par exemple les données sur des personnes pouvant être les victimes potentielles d'une infraction pénale.

13. Définitions

a) Un **niveau de protection des données adéquat** des États tiers est un niveau de protection des données reconnu par la Commission européenne à un État non membre de l'UE, selon lequel les principaux éléments de la vie privée – tels qu'ils sont entendus de façon unanime dans les États membres de l'UE – sont protégés dans l'ensemble. Lors de sa décision, la Commission européenne tient compte de toutes les circonstances jouant un rôle dans le cadre d'un transfert de données ou d'une catégorie de transferts de données. Ceci inclut une évaluation du droit dans l'État ainsi que des codes de conduite et des mesures de sécurité applicables.

b) Les **données anonymisées** sont les données pour lesquelles il n'est plus possible d'établir un lien avec la personne de façon durable et par personne ou pour lesquelles un lien avec la personne peut uniquement être établi avec un effort démesuré en termes de temps, de coûts et de travail.

c) Les **données nécessitant une protection particulière** sont des données sur l'origine raciale ou ethnique, sur les opinions politiques, sur la confession religieuse ou les convictions philosophiques, sur l'appartenance à des syndicats ou sur la santé ou la vie sexuelle de la personne concernée. Selon le droit de l'État, d'autres catégories de données peuvent être classées comme nécessitant une protection particulière ou le contenu des catégories de données peut être différent. De la même façon, les données concernant des délits peuvent souvent être traitées uniquement dans des conditions particulières imposées par la loi de l'État.

d) Une **personne concernée** au sens de la présente directive de protection des données est toute personne physique sur laquelle des données sont traitées.

e) Les **incidents de protection des données** sont tous les événements pour lesquels il existe un soupçon justifié sur le fait que des données à caractère personnel sont espionnées, collectées, modifiées, copiées, transmises ou utilisées de façon illicite. Ils peuvent aussi bien concerner des actes de tiers que d'employés.

f) Un **tiers** est toute personne en dehors de la personne concernée et de l'organisme responsable du traitement des données. Au sein de l'UE, les sous-traitants ne sont pas des tiers au sens du droit de la protection des données étant donné qu'ils sont rattachés légalement à l'organisme responsable du traitement.

g) Les **États tiers** au sens de la directive sur la protection des données sont tous les États en dehors de l'Union européenne et de l'EEE. Font exception les États dont le niveau de protection des données a été reconnu comme adéquat par la Commission européenne.

h) Le traitement de données à caractère personnel est **nécessaire** lorsque la finalité licite ou l'intérêt légitime ne peut pas être atteint sans les données à caractère personnel ou uniquement avec un effort démesuré.

i) L'**Espace économique européen (EEE)** est un espace économique associé à l'UE, dont font partie la Norvège, l'Islande et le Liechtenstein.

j) Le **délégué à la protection des données compétent** est le délégué à la protection des données nommé pour l'entreprise correspondante du CHROMOS Group.

k) Les **données à caractère personnel** sont toutes les informations sur une personne physique déterminée ou déterminable. Une personne est par exemple déterminable lorsqu'un lien

avec la personne peut être établi par une combinaison d'informations et de connaissances complémentaires disponibles de façon aléatoire.

l) **Transfert** désigne toute divulgation par l'organisme responsable de données protégées du traitement à des tiers.

m) **Traitement de données à caractère personnel** désigne tout procédé de collecte, d'enregistrement, d'organisation, de conservation, de modification, d'interrogation, d'utilisation, de transfert, de diffusion ou de combinaison et de comparaison des données exécuté avec ou sans l'aide de processus automatisés. L'élimination, l'effacement et le blocage des données et des supports de données en font également partie.

n) L'**organisme responsable** est la société indépendante juridiquement du CHROMOS Group dont l'activité commerciale donne lieu à la mesure de traitement.

Annexe 1 : Conformité PCI-DSS

Le traitement des données de cartes de crédit est effectué au sein du CHROMOS Group dans le respect des dispositions de conformité PCI-DSS ci-après :

- SAQ 12.8.1 :
  Une liste des prestataires doit être tenue. La liste doit comporter une description des prestations fournies. La liste doit être tenue par le département sécurité informatique. Tous les responsables de départements sont tenus de signaler immédiatement les modifications concernant les prestataires au département sécurité informatique.

- SAQ 12.8.2
  Chaque prestataire doit conclure avec l'entreprise correspondante du CHROMOS Group un accord écrit relatif à la protection des données des titulaires des cartes de crédit. Le département sécurité informatique doit contrôler l'accord et la directive afin d'exécuter l'accord.

- SAQ 12.8.3 :
  Le département sécurité informatique doit établir une procédure devant impérativement être observée lors de la sélection des prestataires.

- SAQ 12.8.4 :
  Le département sécurité informatique vérifie une fois par an la conformité PCI-DSS des prestataires et la documente.

- SAQ 12.8.5 :
  Le département sécurité informatique documente toutes les exigences PCI-DSS et note dans ce cadre la responsabilité (la sienne ou celle du prestataire).

- SAQ 12.10.1 :
  Le département sécurité informatique veille à ce que les perturbations soient mises en œuvres dans la procédure de réponse aux incidents.