HAKRO GmbH

Politique de confidentialité

État: 01.05.18

POLITIQUE DE CONFIDENTIALITÉ

Préface

Chers Messieurs,

À l'ère du numérique, nous, la société HAKRO GmbH, comme toute organisation et toute entreprise, dépendons de la collecte et du traitement de données pertinentes pour nos processus commerciaux.

Cela s'applique également à vos données si vous êtes un client, un client potentiel, un partenaire commercial ou un employé de notre société.

La protection de vos données personnelles est pour nous une priorité absolue. Nous considérons donc qu'il est de notre devoir de veiller à ce que la collecte et le traitement des données soient conformes aux différentes exigences légales.

Les droits personnels et la vie privée de chaque individu font partie des réalisations les plus importantes de notre société.

Nous avons fixé des conditions strictes pour le traitement des données personnelles dans nos lignes directrices sur la protection des données. Ceci est conforme aux exigences du règlement de base sur la protection des données et à d'autres lois de la République fédérale d'Allemagne et de l'Union européenne.

Nos employés sont tenus de respecter notre politique de confidentialité et d'observer les lois respectives sur la protection des données.

Carmen Kroll

Thomas Müller

Table des matières

1. Objectif

La société HAKRO GmbH s'engage à respecter les droits de protection des données dans le cadre de sa responsabilité sociale. Cette directive sur la protection des données s'applique à la société HAKRO GmbH et repose sur les principes de base de la protection des données acceptés dans l'Union européenne.

La politique de confidentialité crée l'une des conditions cadres nécessaires à la collecte, au traitement et, le cas échéant, à la transmission de données personnelles. Elle assure le niveau approprié de protection des données requis par la directive européenne sur la protection des données et les lois locales.

2. Champ d´application

Cette politique de confidentialité s'applique à la société HAKRO GmbH et nos employés. La politique de confidentialité couvre tous les traitements de données personnelles.

Les données anonymisées, par exemple pour des évaluations statistiques ou des enquêtes, ne sont pas soumises à cette politique de confidentialité.

Les employés n'ont pas le droit de prendre des dispositions qui s'écartent de cette politique de confidentialité. Les modifications de cette politique de confidentialité ne seront apportées qu'en consultation avec le délégué à la protection des données. Les changements seront annoncés immédiatement au sein de HAKRO GmbH.

3. Principes du traitement des données personnelles

3.1 Droit à l'autodétermination informationnelle

La base de la législation sur la protection des données est le droit de l'individu à l'autodétermination informationnelle.

3.2 Légalité

Les données personnelles doivent être collectées et traitées de manière licite. Lors du traitement de données personnelles, les droits de la personne concernée doivent être respectés.

3.3 Transparence

Les données doivent être collectées auprès de la personne concernée elle-même. La personne concernée doit être informée de la finalité du traitement des données, du responsable du traitement et de toute transmission à des tiers qui pourrait être nécessaire.

3.4 Limitation de l'objet

Les données personnelles ne peuvent être traitées qu'aux fins spécifiées au moment de leur collecte. Un changement ultérieur de finalité nécessite le consentement de la personne concernée ou une justification pertinente.

3.5 Évitement des données

Dans tout traitement de données personnelles, seules les données nécessaires à la finalité du traitement doivent être utilisées. Les données personnelles ne sont pas conservées pour une éventuelle finalité ultérieure.

3.6 Suppression

Après l'expiration des délais de conservation légaux ou liés au processus commercial, les données personnelles doivent être supprimées. Si, dans des cas individuels, il y a des indications que des intérêts légitimes sont sauvegardés, les données continuent à être stockées jusqu'à ce que l'intérêt légitime n'existe plus.

3.7 Exactitude des données

Les données personnelles doivent être sauvegardées de manière exacte et complète. Des mesures raisonnables sont prises pour garantir que les données incomplètes ou obsolètes soient supprimées ou rectifiées.

3.8 Confidentialité

Les données personnelles doivent être traitées de manière confidentielle. Cela est assuré par des mesures organisationnelles et techniques appropriées contre l'accès non autorisé, le traitement et la divulgation illicites, l'altération ou la destruction.

4. Licéité du traitement des données

4.1 Données sur les clients, les clients potentiels et les partenaires

4.1.1 Traitement des données pour l'exécution de la relation contractuelle

Les données personnelles de le client potentiels, du client ou du partenaire peuvent être traitées à l'établissement, à l'exécution et à la résiliation de la relation contractuelle. Cela inclut également le soutien du partenaire contractuel, dans la mesure où il est lié à l'objet du contrat. Dans la perspective d'un contrat, le traitement de données personnelles est autorisé pour la préparation d'offres, pour l'élaboration de demandes d'achat ou pour la réalisation d'autres souhaits de l'intéressé visant à la conclusion d'un contrat. Les parties intéressées peuvent être contactées pendant la phase de préparation du contrat en utilisant les données qu'elles ont fournies. Toute restriction exprimée par l'intéressé doit être respectée.

Si la personne concernée contacte la société HAKRO GmbH pour une demande d´informations, le traitement des données est autorisé pour l'exécution de cette demande. Si la personne concernée s'oppose à l'utilisation de ses données à des fins publicitaires, l'utilisation ultérieure de ses données à ces fins n'est pas autorisée et elle doit être bloquée ou supprimée à ces fins.

4.1.2 Consentement au traitement des données

Si la personne concernée consent au traitement des données, celui-ci peut avoir lieu. Avant de donner son consentement, la personne concernée doit être informée de la nature et de la portée de ses droits.

La déclaration de consentement doit toujours être obtenue par écrit ou par voie électronique. Dans le cas d'une consultation téléphonique, le consentement peut également être donné verbalement. Cela doit être documenté.

4.1.3 Traitement des données sur la base juridique

Le traitement des données personnelles est autorisé s'il est requis, présupposé ou autorisé par des dispositions légales gouvernementales. Le type et l'étendue du traitement de données autorisé sont déterminés par ces dispositions légales.

4.1.4 Traitement des données sur la base d'un intérêt légitime

Les données personnelles peuvent être traitées si cela est nécessaire pour la réalisation d'un intérêt légitime de la société HAKRO GmbH.

Généralement légitimé sont les intérêts juridique (par exemple, l'exécution des créances en souffrance) ou économique (par exemple, la prévention des ruptures de contrat). À cet égard, les intérêts de la personne concernée qui sont dignes de protection ne doivent pas être ignorés. Cela doit être vérifié avant tout traitement.

4.1.5 Traitements de données dignes de protection particulière

Les données personnelles dignes de protection particulière ne peuvent être traitées que si la loi l'exige ou si la personne concernée y a expressément consenti.

Le traitement de ces données est également autorisé s'il est absolument nécessaire pour faire valoir, exercer ou défendre des droits légaux à l'encontre de la personne concernée.

Le délégué à la protection des données doit être informé avant le traitement des données dignes de protection.

4.1.6 Données sur les utilisateurs sur l'Internet

Si des données personnelles sont collectées, traitées et utilisées sur des sites web ou dans des programmes, la personne concernée doit en être informée dans les avis de protection des données. Ces avis doivent être facilement reconnaissables et compréhensibles pour la personne concernée.

Si des profils d'utilisation sont créés pour analyser le comportement d'utilisation des sites web et des programmes, la personne concernée doit en être informée de manière compréhensible dans les avis de protection des données.

Si des sites web ou des programmes permettent d'accéder à des données personnelles dans un espace personnel, l'identification et l'authentification de la personne concernée doivent être conçues de manière à assurer une protection adéquate de l'accès respectif.

4.2 Données relatives aux employés et aux candidats

4.2.1 Traitement des données pour la relation de travail

Pour la relation de travail, il est possible de traiter des données personnelles qui sont nécessaires à l'établissement, à l'exécution et à la résiliation du contrat de travail. Lors de l'initiation d'une relation de travail, les données personnelles des candidats peuvent être traitées. Après le rejet, les données du candidat doivent être supprimées, en tenant compte des délais prévus par le droit de la preuve, à moins que le candidat n'ait consenti à un stockage supplémentaire pour un processus de sélection ultérieur.

Dans une relation de travail existante, le traitement des données doit toujours être lié à la finalité du contrat de travail.

4.2.2 Traitement des données sur la base d´une autorisation légale

Le traitement des données personnelles est autorisé s'il est requis, présupposé ou autorisé par des dispositions légales gouvernementales. Le type et l'étendue du traitement de données autorisé sont régis par ces dispositions légales.

4.2.3 Consentement au traitement des données

Les données relatives aux employés peuvent être traitées sur la base du consentement de la personne concernée. Les déclarations de consentement doivent être données volontairement.

La déclaration de consentement doit généralement être obtenue par écrit ou par voie électronique. Si les circonstances ne le permettent pas dans des cas exceptionnels, le consentement peut être donné verbalement. Dans tous les cas, l'octroi du consentement doit être documenté.

4.2.4 Traitement des données sur la base d'un intérêt légitime

Le traitement des données relatives aux employés peut avoir lieu si cela est nécessaire pour la réalisation d'un intérêt légitime de la société HAKRO GmbH.

Généralement légitimé sont les intérêts juridique (par exemple, l'exécution des créances en souffrance) ou économique (par exemple, la prévention des ruptures de contrat). À cet égard, les intérêts de la personne concernée qui sont dignes de protection ne doivent pas être ignorés. Cela doit être vérifié avant tout traitement.

Les mesures de contrôle qui nécessitent le traitement des données relatives aux employés ne peuvent être exécutées que s'il existe une obligation légale de le faire ou s'il y a une raison justifiée de le faire. À cet égard, les intérêts de la personne concernée qui sont dignes de protection ne doivent pas être ignorés. Cela doit être vérifié avant tout traitement.

4.2.5 Télécommunications et Internet

Les systèmes téléphoniques, les adresses électroniques, les intranets et l'Internet sont principalement fournis par l'entreprise dans le cadre de ses tâches opérationnelles. Ce sont des équipements de travail et des ressources de l'entreprise. Ils peuvent être utilisés dans le cadre des réglementations légales applicables et des directives internes de l'entreprise.

Il n'y a pas de surveillance générale des communications téléphoniques ou électroniques ou de l'utilisation d'Internet. Afin de se défendre contre les attaques visant l'infrastructure informatique ou les utilisateurs individuels, des mesures de protection peuvent être implémentées au niveau des passerelles du réseau de l'entreprise qui bloquent les contenus techniquement préjudiciables ou analysent les motifs d'attaques.

Pour des raisons de sécurité, l'utilisation du téléphone, de la communication par courrier électronique ou de l'Internet peut être enregistrée pendant une période limitée.

Les évaluations personnelles de ces données ne peuvent être effectuées qu'en cas de suspicion concrète et justifiée d'une violation des lois ou des directives de la société HAKRO GmbH. Le délégué à la protection des données doit être consulté dans ce cas.

5. Transfert des données personnelles

En cas de transmission de données personnelles à des tiers, le traitement des données doit être licite. Le destinataire des données doit être obligé de les utiliser uniquement aux fins spécifiées.

6. Traitement des commandes

Il y a traitement de données commandées si un contractant est chargé de traiter des données personnelles sans être responsable du processus commercial associé.

Dans ces cas, un contrat pour le traitement des données commandées doit être conclu. Dans ce cas, la société mandataire conserve l'entière responsabilité de la bonne exécution du traitement des données. Le contractant ne peut traiter les données personnelles que dans le cadre des instructions du client. Les exigences suivantes doivent être respectées lors de l'attribution de la commande :

a) Le contractant est choisi en fonction de son aptitude à assurer les mesures de protection techniques et organisationnelles nécessaires.

b) La commande doit être passée sous forme de texte. Les instructions relatives au traitement des données et les responsabilités du client et du contractant doivent être documentées.

c) Le client doit s'assurer que le contractant respecte ses obligations avant le début du traitement des données. Un contractant peut prouver qu'il respecte les exigences en matière de sécurité des données, notamment en présentant une attestation appropriée. L'inspection doit être répétée régulièrement pendant la durée du contrat, si nécessaire.

7. Droits de la personne concernée

Si les droits suivants sont revendiqués, ils doivent être traités immédiatement et ne doivent pas entraîner de désavantages pour la personne concernée.

a) La personne concernée peut demander des informations sur quelles données personnelles sont stockées à quel sujet et quelle origine sur quelle raison.

b) Si des données personnelles sont transférées à des tiers, des informations doivent également être fournies sur l'identité du destinataire ou sur les catégories de destinataires.

c) Si les données personnelles sont incorrectes ou incomplètes, la personne concernée peut demander qu'elles soient corrigées ou complétées.

d) La personne concernée peut s'opposer au traitement de ses données personnelles à des fins de publicité ou d'études de marché et d'opinion. À ces fins, les données doivent être bloquées ou supprimées.

e) La personne concernée a le droit d'exiger la suppression de ses données si la base juridique du traitement des données est manquante ou a cessé d'exister. Il en va de même lorsque la finalité du traitement des données a cessé d'exister en raison de l'écoulement du temps ou pour d'autres raisons. Les obligations de conservation existantes et les intérêts dignes de protection qui sont en conflit avec la suppression doivent être respectés.

f) La personne concernée a un droit fondamental de s'opposer au traitement de ses données, qui doit être respecté si son intérêt digne de protection en raison d'une situation personnelle particulière l'emporte sur l'intérêt du traitement.

Cette disposition ne s'applique pas si une disposition légale oblige à effectuer le traitement.

8. Confidentialité du traitement

Les données personnelles sont soumises au secret des données. Il est interdit aux employés de collecter, de traiter ou d'utiliser des données sans autorisation.

Le traitement non autorisé est tout traitement effectué par un employé sans qu'il en soit chargé dans le cadre de l'exercice de ses fonctions et sans y être autorisé.

Cela nécessite une division et une séparation minutieuses des rôles et des responsabilités ainsi que leur mise en œuvre et leur maintien dans le cadre des concepts d'autorisation.

Les employés ne peuvent pas utiliser les données personnelles à leurs propres fins privées ou commerciales, les transmettre à des personnes non autorisées ou les leur rendre accessibles de toute autre manière.

Cette obligation continue à s'appliquer même après la fin de la relation de travail.

9. Sécurité du traitement

Les données personnelles doivent être protégées à tout moment contre l'accès non autorisé, le traitement ou la transmission illicite, ainsi que contre la perte, la corruption ou la destruction. Cela s'applique indépendamment du fait que les données soient traitées électroniquement ou sur papier. Avant l'introduction de nouvelles procédures de traitement des données, en particulier de nouveaux systèmes informatiques, des mesures techniques et organisationnelles de protection des données personnelles sont définies et appliquées. Ces mesures doivent être fondées sur l'état de la technique, les risques découlant du traitement et la nécessité de protéger les données.

10. Contrôle de la protection des données

Le respect de la politique de confidentialité et des lois applicables de protection des données est régulièrement vérifié au moyen de contrôles appropriés.

11. Incidents liés à la protection des données

Les employés doivent signaler immédiatement les incidents de protection des données à la direction ou au délégué à la protection des données.

En particulier, dans les cas de

- la transmission illicite de données personnelles à des tiers

- l'accès illégal à des données personnelles par des tiers

- la perte de données personnelles

le rapport doit être fait sans délai afin que les obligations existantes en matière de rapport aux autorités de contrôle puissent être remplies sans délai.

12. Responsabilités et sanctions

La direction est responsable du bon traitement des données.

Elle est donc tenue d'assurer que les exigences légales en matière de protection des données et celles contenues dans la politique de confidentialité soient prises en compte.

La réalisation de ces exigences relève de la responsabilité des employés responsables.

En cas de contrôle par les autorités de contrôle, le délégué à la protection des données doit être immédiatement informé.

13. Délégué à la protection des données

Chaque personne concernée peut contacter le délégué à la protection des données avec des suggestions, des demandes de renseignements, des demandes d'informations ou des plaintes en rapport avec des questions de protection ou de sécurité des données.

Les demandes et les plaintes seront traitées confidentiellement sur demande.

Vous pouvez contacter votre délégué à la protection des données comme suit :

Guido Petermann
Hildebrandtstr. 24C
40215 Düsseldorf

Téléphone: +49 211 72139550
E-mail: datenschutz@planitas.de
Site web: www.planitas.de