

Duro Đaković Termoelektrična postrojenja d.o.o.

Dr. Mile Budaka 1

Slavonski Brod

Slavonski Brod, 24.05.2018

Libellé du document:	Politique de gestion des données
Version:	01
Date de la version:	24.05.2018

Duro Đaković Termoeenergetska postrojenja d.o.o.

Dr. Mile Budaka 1 Slavonski Brod Slavonski Brod, 24/05/2018

POLITIQUE DE GESTION DES DONNÉES

Conformément au Règlement général sur la protection des données (RGPD UE 2016/679, ci-après : le Règlement), à la loi sur la mise en œuvre du Règlement général sur la protection des données (Narodne Novine n° 42/2018) et à d'autres règlements juridiques, L'administration de Đuro Đaković Termoeenergetska postrojenja d.o.o., Dr. Mile Budaka 1, Slavonski Brod (ci-après : la Société), détermine l'attitude de la Société à l'égard des données personnelles, définit les règles, attribue les responsabilités et apporte un soutien complet à la gestion des données et à la protection des données personnelles. Les données personnelles collectées et traitées par la Société sont considérées comme des informations confidentielles données à la Société par leurs sujets. Ces données doivent être traitées avec une attention particulière et ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été collectées.

COLLECTE ET TRAITEMENT

La collecte de données personnelles ne peut être effectuée qu'en conformité avec les réglementations légales et les principes éthiques. Les données personnelles ne peuvent être traitées que lorsqu'il existe une base légale clairement déterminée et documentée pour le traitement ou une base conforme à un accord contractuel, tandis que tous les autres types de traitement de données personnelles ne sont autorisés qu'avec le consentement clairement documenté de la personne concernée ou de son mandataire.

Lors de la collecte et du traitement des données personnelles, il est obligatoire de respecter le principe selon lequel seules les données indispensables à un traitement spécifique peuvent être collectées. Toute forme de collecte de données inutiles est interdite.

Avant la collecte de données à caractère personnel, les personnes concernées reçoivent des informations claires sur la finalité de la collecte, sur le type de collecte, le type de traitement dans lequel les informations en question seront utilisées ainsi que sur les éventuels tiers y ayant accès.

Toute forme de collecte et de traitement des informations concernant un mineur (16-18 ans) sera traitée avec le plus grand soin et en accord avec les principes éthiques les plus élevés.

DROITS DES PERSONNES CONCERNÉES

Les personnes concernées ont le droit d'accéder aux informations sur le type de données personnelles que la Société détient à leur sujet et le droit de savoir à quelles fins ces informations sont utilisées. La société donne aux personnes concernées la possibilité de corriger les données personnelles fausses et de compléter celles qui sont incomplètes, ainsi que la possibilité de refuser le droit au traitement de leurs données dans les cas où le traitement est conditionné par leur consentement. Lorsqu'une personne concernée refuse le droit de faire traiter ses informations, elle est informée des conséquences possibles de la rétention des informations, c'est-à-dire de la privation éventuelle d'un certain droit dans le cadre du contrat de travail si le droit en question est conditionné par le traitement de données à caractère personnel.

À la demande d'une personne concernée, les données personnelles obtenues avec son consentement doivent être supprimées (retirées) de tous les systèmes d'information de la société et des systèmes de données détenus par des tiers auxquels la société a autorisé l'accès.

Une personne concernée a le droit de faire transférer ses données. À la demande d'une personne concernée, ses données personnelles doivent être livrées sous forme électronique.

LA TENUE DES REGISTRES, LA CONSERVATION ET LA MANIPULATION

La Société est tenue de créer et de tenir un registre des types de données personnelles et des types de traitement effectués sur les données et doit désigner un responsable du traitement et du type de données personnelles collectées. Le responsable est tenu de garantir le traitement uniquement des données personnelles obtenues sur une base légale, par le biais d'une autorisation appropriée ou à des fins commerciales.

Lorsqu'il n'existe pas de base juridique pour conserver certaines données personnelles, celles-ci doivent être détruites sans délai. La société est tenue de sécuriser les données de manière adéquate.

Les données à caractère personnel ne peuvent être transmises à des pays tiers que dans le respect des dispositions légales et s'il est possible de garantir un certain niveau de sécurité par le biais d'une législation appropriée (clauses contractuelles types, règles d'entreprise contraignantes).

PROTECTION INTÉGRÉE DES DONNÉES

Lors de la conception des systèmes d'information et de l'organisation des processus d'entreprise qui peuvent influencer de quelque manière que ce soit la sécurité des données personnelles ou le droit à la vie privée des personnes concernées, la société évalue leur impact sur la sécurité des données et prend les mesures de protection appropriées. S'il est établi que les mesures de protection mises en œuvre ne sont pas suffisantes, la société consulte l'autorité compétente. Tous les nouveaux processus et systèmes d'information au sein de la société doivent être organisés de manière à répondre aux exigences de la présente politique.

MINIMISER ET PROTÉGER LES DONNÉES PERSONNELLES

La société ne collecte et ne conserve les données personnelles que dans la mesure où elles sont nécessaires au service rendu, au contrat de travail, à l'envoi de travailleurs et à l'exercice des droits fondés sur le contrat de travail.

Les données sont stockées dans le plus petit nombre d'endroits possible et sont protégées de manière adéquate. L'accès aux données personnelles peut être autorisé à des fins exclusivement professionnelles.

Il est interdit d'utiliser des données personnelles pour le développement ou le test de systèmes informatiques. Chaque fois que cela est possible, les données personnelles doivent être protégées par cryptage, pseudonymisation ou anonymisation.

GESTION DES INCIDENTS

La société établit et maintient les procédures d'action en cas d'incident lié à la violation de la sécurité des données personnelles, tant au sein de la société qu'avec les tiers qui ont été autorisés à accéder aux données personnelles par la société ou qui ont permis à la société d'y accéder.

La société établit et maintient la structure de responsabilité pour la remise de rapports sur les incidents liés à la sécurité des données personnelles.

La société conçoit et maintient les mesures destinées à détecter l'accès non autorisé aux données personnelles ou la divulgation non autorisée de données personnelles conservées dans le système d'information.

En cas de violation de la sécurité des données personnelles, la Société informera sans délai, au plus tard dans les 72 heures suivant la constatation de l'incident, l'autorité compétente. En cas de divulgation non autorisée de données personnelles, la Société informera également les sujets dont les données ont été compromises, si cela s'avère possible.

CERTIFICATION

La société crée et maintient un système de gestion des bases de données conforme aux normes applicables en matière de protection de la vie privée et de sécurité des informations, telles que la norme ISO 27001, dont la conformité est prouvée par une certification appropriée lorsque cela est possible.

EXCEPTIONS

Dans des cas exceptionnels concernant des données personnelles, le délégué à la protection des données peut approuver une action temporaire qui n'est pas conforme à la présente politique. Le responsable de la sécurité des données est tenu de conserver des traces de ces approbations, des responsabilités et des délais pour l'ajustement des données et d'en informer l'administration.

RESPONSABILITÉS

Tous les employés de la société sont tenus de suivre les mesures définies par la présente politique, de même que tous les tiers qui peuvent accéder aux données dans le cadre de la coopération avec la société.

La personne responsable de la création et de la maintenance des données et de la coordination de toutes les activités relatives à la gestion des données est le délégué à la protection des données. Le délégué est nommé par l'administration de l'entreprise à laquelle il est directement rattaché. Le délégué à la protection des données est notamment responsable de ce qui suit :

- informer et conseiller le détenteur des données ou le responsable du traitement des données ainsi que les employés qui traitent des données à caractère personnel sur les obligations qui leur incombent en vertu du règlement,
- contrôler le respect du règlement, des politiques internes et des autres législations liées à la protection des données,
- la création et la tenue d'un registre de données personnelles,
- l'attribution de responsabilités en matière de protection des données aux employés et aux tiers impliqués dans le processus de gestion des données personnelles.
- la sensibilisation et la formation des employés à la protection des données,
- la mise en œuvre de la protection de la vie privée dans les processus commerciaux et les systèmes d'information,
- la mise en œuvre de la protection de la vie privée dans les procédures d'audit,
- le soutien pendant les évaluations des impacts possibles sur la protection des données,

- la coopération avec les autorités de contrôle,
- le suivi du processus de gestion des risques lors du traitement des données personnelles,
- la communication de rapports à l'administration sur l'efficacité des systèmes de gestion des bases de données.

Le département informatique est responsable de la formation et de l'exécution des contrôles techniques nécessaires à l'adaptation aux exigences de la présente politique, notamment en ce qui concerne les points suivants :

- l'identification et la protection des données personnelles,
- les mécanismes destinés à la protection des droits des personnes concernées.

Le département juridique est responsable du suivi et de l'interprétation des règlements liés à la protection des données et de la fourniture d'un soutien juridique au système de gestion des données.

Le département de la sécurité est chargé de superviser l'application des mesures de protection des données et d'apporter un soutien professionnel au système de gestion des données.

La présente politique est révisée au moins une fois par an ou après chaque modification de l'environnement juridique ou de risque susceptible d'avoir un impact sur son efficacité ou son application.

Le suivi de l'application des règles énoncées dans la présente politique ainsi que les suggestions concernant l'amélioration et la promotion du système de protection des données au sein de l'entreprise sont les tâches du délégué à la protection des données.

Slavonski Brod, 24/05/2018

Au nom de l'administration

Ivica Marić, PDG