Đuro Đaković Termoenergetska postrojenja d.o.o.
Dr. Mile Budaka 1
Slavonski Brod
Slavonski Brod, 24.05.2018

Name des Dokuments:	Richtlinie des Verwaltungssystems für personenbezogene Daten
Version:	01
Datum der Version:	24.05.2018

RICHTLINIE DES VERWALTUNGSSYSTEMS FÜR PERSONENBEZOGENE DATEN

Geschäftsführung der Gesellschaft Đuro Đaković Termoenergetska postrojenja d.o.o., Dr. Mile Budaka 1, Slavonski Brod (im Folgenden: das Unternehmen), in Übereinstimmung mit der Allgemeinen Datenschutzverordnung (DSGVO EU 2016/679, im Folgenden: die Verordnung), dem Gesetz zur Umsetzung der Allgemeinen Datenschutzverordnung (Amtsblatt Nr. . 42/2018.) und andere gesetzliche Vorschriften, bestimmt die Einstellung des Unternehmens zu personenbezogenen Daten, definiert Regeln, weist Verantwortlichkeiten zu und unterstützt das System der Verwaltung und des Schutzes personenbezogener Daten. Personenbezogene Daten, die das Unternehmen bei seiner Arbeit sammelt und verarbeitet, gelten als vertrauliche Informationswerte, die dem Unternehmen von ihren Eigentümern zur Verfügung gestellt werden. Diese Informationen müssen mit besonderer Sorgfalt behandelt werden und dürfen nur in Übereinstimmung mit dem Zweck verwendet werden, für den sie erhoben wurden.

ERHEBUNG UND VERARBEITUNG

Die Erhebung personenbezogener Daten darf nur im Einklang mit gesetzlichen Vorschriften und ethischen Grundsätzen erfolgen. Personenbezogene Daten dürfen nur verarbeitet werden, wenn es eine klar definierte und dokumentierte Rechtsgrundlage oder Grundlage eines Vertragsverhältnisses gibt, während jede andere Verarbeitung personenbezogener Daten nur mit der eindeutig dokumentierten Zustimmung ihres Eigentümers oder seines Bevollmächtigten zulässig ist.
Bei der Erhebung und Verarbeitung personenbezogener Daten ist zwingend der Grundsatz anzuwenden, wonach nur diejenigen Daten erhoben werden dürfen, die für die jeweilige Verarbeitung wirklich erforderlich sind. Jede Sammlung redundanter Daten ist untersagt.
Vor der Erhebung personenbezogener Daten werden den Eigentümern klare Informationen über den Grund der Erhebung, die Art der Verarbeitung, bei der die Informationen verwendet werden, und alle Dritten, die auf die Informationen zugreifen, zur Verfügung gestellt.
Jede Erfassung und Verarbeitung von Informationen durch Minderjährige (Personen im Alter von 16 bis 18 Jahren) wird mit besonderer Sorgfalt angegangen und von den höchsten ethischen Grundsätzen geleitet.

RECHTE DER EIGENTÜMER PERSONENBEZOGENER DATEN

Eigentümer personenbezogener Daten erhalten das Recht auf Auskunft darüber, welche personenbezogenen Daten das Unternehmen über sie hat und zu welchem Zweck sie verwendet werden. Das Unternehmen wird dem Eigentümer personenbezogener Daten die Berichtigung ungenauer und unvollständiger personenbezogener Daten sowie die Möglichkeit ermöglichen, das Recht auf Verarbeitung seiner Daten zu verweigern, wenn die Verarbeitung auf der Zustimmung des Eigentümers beruht. Im Falle der Verweigerung des Rechts auf Datenverarbeitung durch den Eigentümer wird er zuvor über die möglichen Folgen einer solchen Verweigerung oder des möglichen Verlusts eines der Rechte aus dem Beschäftigungsverhältnis informiert, wenn die Verwirklichung derselben durch die Verweigerung der Verarbeitung bedingt ist.
Auf Verlangen des Eigentümers müssen personenbezogene Daten, die auf der Grundlage einer Einwilligung bereitgestellt wurden, aus allen Informationssystemen des

Unternehmens und Informationssystemen Dritter, denen das Unternehmen Zugriff auf diese Daten gewährt hat, gelöscht (entfernt) werden.
Der Eigentümer hat das Recht auf Übertragbarkeit seiner personenbezogenen Daten. Auf Verlangen des Eigentümers müssen seine personenbezogenen Daten in elektronischer Form bereitgestellt werden.

AUFZEICHNUNGEN, AUFBEWAHRUNG UND VERFAHREN

Das Unternehmen ist verpflichtet, ein Verzeichnis der Arten personenbezogener Daten und der damit durchgeführten Verarbeitungen zu erstellen und zu führen und für jede Verarbeitung und Art personenbezogener Daten eine verantwortliche Person zu ernennen. Der Verantwortliche ist verpflichtet sicherzustellen, dass nur personenbezogene Daten in die Verarbeitung einbezogen werden, für deren Verarbeitung eine gesetzliche Grundlage, eine entsprechende Einwilligung oder eine geschäftliche Notwendigkeit besteht.
Alle personenbezogenen Daten, für die keine Grundlage für die Speicherung besteht, sind unverzüglich zu vernichten. Das Unternehmen ist verpflichtet, personenbezogene Daten angemessen bereitzustellen.
Eine Übermittlung personenbezogener Daten an Drittländer darf nur im Einklang mit den gesetzlichen Bestimmungen erfolgen, sofern dies durch Verordnungen (Standardvertragsklauseln, verbindliche Unternehmensregeln) möglich ist und ein gewisses Maß an Sicherheit bietet.

TECHNISCHER UND INTEGRIERTER DATENSCHUTZ

Beim Aufbau von Informationssystemen und der Regulierung von Geschäftsprozessen, die in irgendeiner Weise die Sicherheit personenbezogener Daten beeinträchtigen oder das Recht auf Privatsphäre ihrer Eigentümer ausüben können, führt das Unternehmen eine Sicherheitsfolgenabschätzung durch und stellt geeignete Schutzmaßnahmen bereit. Stellt sie fest, dass die von ihr umzusetzenden Garantien nicht ausreichen, konsultiert sie vor der Verarbeitung die zuständige Behörde. Alle neuen Prozesse und Informationssysteme im Unternehmen werden so eingerichtet, dass sie die Anforderungen dieser Richtlinie erfüllen.

MINIMIERUNG UND SCHUTZ PERSONENBEZOGENER DATEN

Das Unternehmen wird personenbezogene Daten nur erheben und speichern, soweit dies zur Erbringung der Leistung, Begründung eines Beschäftigungsverhältnisses, Entsendung von Mitarbeitern und Ausübung aller Rechte der Mitarbeiter aus dem Beschäftigungsverhältnis erforderlich ist.
Bei der Speicherung von Daten werden personenbezogene Daten an möglichst wenigen Orten gespeichert, an denen sie angemessen geschützt werden müssen. Der Zugriff auf personenbezogene Daten darf ausschließlich auf der Grundlage geschäftlicher Anforderungen gewährt werden.
Es ist untersagt, personenbezogene Daten zu Zwecken der Entwicklung oder Erprobung von informationstechnischen Systemen zu verwenden. Personenbezogene Daten sind nach Möglichkeit durch Verschlüsselung, Pseudonymisierung oder Anonymisierung zu schützen.

VORFALLMANAGEMENT

Das Unternehmen wird Verfahren für den Fall eines Vorfalls im Zusammenhang mit der Verletzung der Sicherheit personenbezogener Daten innerhalb des Unternehmens und mit Dritten einrichten und aufrechterhalten, denen das Unternehmen personenbezogene Daten zur Verfügung gestellt hat oder die dem Unternehmen personenbezogene Daten zur Verfügung gestellt haben.
Das Unternehmen wird eine Verantwortungsstruktur für die Meldung von Vorfällen im Zusammenhang mit der Sicherheit personenbezogener Daten einrichten und aufrechterhalten.
Das Unternehmen wird Maßnahmen zur Erkennung des unbefugten Zugriffs auf personenbezogene Daten und der unbefugten Offenlegung personenbezogener Daten aus dem Informationssystem einführen und aufrechterhalten.
Im Falle einer Verletzung der Sicherheit personenbezogener Daten benachrichtigt das Unternehmen unverzüglich und spätestens 72 Stunden nach Entdeckung des Vorfalls die zuständige Behörde. Im Falle einer unbefugten Offenlegung personenbezogener Daten wird das Unternehmen auch die Eigentümer benachrichtigen, deren Daten kompromittiert wurden, wenn dies vernünftigerweise praktikabel ist.

ZERTIFIZIERUNG

Das Unternehmen wird ein Verwaltungssystem für personenbezogene Daten in Übereinstimmung mit den geltenden Standards im Bereich Datenschutz und Informationssicherheit, wie z. B. ISO 27001, einrichten und aufrechterhalten und nach Möglichkeit die Einhaltung einer entsprechenden Zertifizierung nachweisen.

AUSNAHMEN

Wenn es einen berechtigten Grund gibt, kann der Sicherheitsbeauftragte für personenbezogene Daten ausnahmsweise die vorübergehende Handhabung personenbezogener Daten genehmigen, die nicht dieser Richtlinie entspricht. Der Datenschutzbeauftragte ist verpflichtet, Aufzeichnungen über solche Genehmigungen, Verantwortlichkeiten und Fristen für die Einhaltung zu führen und dies dem Vorstand zu melden..

VERANTWORTLICHKEITEN

Alle Mitarbeiter des Unternehmens sind verpflichtet, die in dieser Richtlinie festgelegten Maßnahmen einzuhalten, sowie Dritte, die im Rahmen ihrer Zusammenarbeit mit dem Unternehmen Zugang zu personenbezogenen Daten erhalten.
Der Datenschutzbeauftragte ist verantwortlich für die Einrichtung und Pflege des Systems zur Verwaltung personenbezogener Daten und die Koordinierung aller Aktivitäten im Zusammenhang mit der Verwaltung personenbezogener Daten. Der Datenschutzbeauftragte wird vom Vorstand der Gesellschaft ernannt, dem er für seine Arbeit direkt verantwortlich ist. Der Datenschutzbeauftragte ist insbesondere verantwortlich für:

- Unterrichtung und Beratung des für die Verarbeitung Verantwortlichen oder Ausführenden und der Arbeitnehmer, die personenbezogene Daten

verarbeiten, über ihre Pflichten gemäß der Verordnung,

- Überwachung der Einhaltung der Verordnung und interner Richtlinien und anderer Vorschriften zum Schutz personenbezogener Daten,
- Einrichtung und Führung eines Registers personenbezogener Daten,
- Zuweisung der Verantwortung für den Schutz personenbezogener Daten an Mitarbeiter und Dritte, die an der Erhebung und Verarbeitung personenbezogener Daten beteiligt sind,
- Sensibilisierung und Schulung von Arbeitnehmern im Bereich des Schutzes personenbezogener Daten,
- Integrieren des Datenschutzes in Geschäftsprozesse und Informationssysteme,
- Integrieren von Datenschutzmaßnahmen in Audit-Prozesse,
- Beratung bei der Durchführung von Datenschutz-Folgenabschätzungen,
- Zusammenarbeit mit Aufsichtsbehörden,
- Überwachung des Risikomanagementprozesses bei der Verarbeitung personenbezogener Daten,
- Berichterstattung an den Vorstand über die Wirksamkeit des Systems zur Verwaltung personenbezogener Daten.

Die IT-Abteilung ist verantwortlich für die betriebliche Einrichtung und Aufrechterhaltung der technischen Kontrollen, die zur Einhaltung der Anforderungen dieser Richtlinie erforderlich sind, insbesondere der Maßnahmen zur:

- Identifizierung und Schutz personenbezogener Daten,
- Mechanismen zur Erfüllung der Rechte der Eigentümer personenbezogener Daten.

Der Juristische Dienst ist für die Überwachung und Auslegung der Rechtsvorschriften im Bereich des Datenschutzes und die rechtliche Unterstützung der Arbeit von Systemen zur Verwaltung personenbezogener Daten zuständig.

Der Unternehmenssicherheitsdienst ist für die Überwachung der Anwendung von Maßnahmen zum Schutz personenbezogener Daten und die Bereitstellung professioneller Unterstützung in seinem Bereich für die Arbeit des Systems zur Verwaltung personenbezogener Daten verantwortlich.

Diese Richtlinie wird mindestens einmal jährlich oder nach jeder Änderung des Rechts- oder Risikoumfelds, die ihre Wirksamkeit und Anwendung beeinträchtigen könnte, überprüft.

Der Datenschutzbeauftragte ist verantwortlich für die Überwachung der Umsetzung der Bestimmungen dieser Richtlinie sowie für Vorschläge zur Verbesserung und Erweiterung des Datenschutzsystems im Unternehmen.

In Slavonski Brod, am 24. Mai 2018

Im Namen des Vorstands:

Ivica Marić, CEO