Energie Münchenbuchsee AG

Weisungen über den Datenschutz und die Informationssicherheit

Inhaltsverzeichnis

Versionskontrolle:

Datum	Version	Bemerkung	
23.06.2023	1.0	Dokumenterstellung	JS
13.07.2023	1.1	Review durch	RA Chantal Lutz
14.07.2023	1.2	Anpassungen	JS/DK
08.08.2023	1.3	Entfernen Kommentare/Anmerkungen	JS
18.08.2023	1.4	Genehmigung Verwaltungsrat	VR

1 Allgemeines und Zuständigkeit

1.1 Geltungsbereich

Die Energie Münchenbuchsee AG mit Sitz in Münchenbuchsee (nachfolgend "wir" oder "uns") ist für die Stromversorgung im Gemeindegebiet Münchenbuchsee hoheitlich zuständig. Wir bezwecken die Beschaffung, Speicherung, Übertragung und Verteilung sowie die sichere, wirtschaftliche und umweltverträgliche Versorgung des Gemeindegebiets mit Energie. Wir betreiben und unterhalten zudem einen Wärmeverbund. Diverse Dienstleistungen im Mandat, so z.B. im Bereich Wasserversorgung, Unterhalt Strassenbeleuchtung sowie Fakturierung, runden unser Angebot ab.

Wo es die Lesbarkeit vereinfacht, ist in dieser Richtlinie die männliche Form gewählt. Selbstverständlich sind sinngemäss und gleichermassen wertschätzend auch die Damen angesprochen. Basis für diese Richtlinie sind das kantonale Datenschutzgesetz (KDSG; Stand 01.01.2023 – für Kunden von Strom und Netzdienstleistungen) sowie das Datenschutzrecht für Schweizer Unternehmen (revDSG; Stand 01.09.2023 – für Kunden unserer betriebseigenen Dienstleistungen wie z. B. Wärmeverbundkunden).

Der Schutz personenbezogener Daten ist uns wichtig. Die vorliegende Richtlinie soll sicherstellen, dass Personendaten gesetzeskonform bearbeitet werden. Sie regelt gleichzeitig den sicheren und gesetzeskonformen Umgang mit IT-Ressourcen und geschäftlichen Informationen.

Wir bearbeiten erhaltene Informationen in einer Weise, welche mit den Unternehmenswerten im Einklang stehen. Diese Richtlinie ist für die Mitarbeitenden und die Geschäftsleitung verbindlich und bildet die Basis für die Verträge mit den datenverarbeitenden Unternehmen.

1.2 Zuständigkeit

Die Einhaltung von gesetzlichen Datenschutzvorgaben ist Sache der Unternehmensführung. Sie ist einerseits verpflichtet, die Vorgaben selbst einzuhalten und andererseits verpflichtet, die Einhaltung der Vorgaben durch ihre Mitarbeitenden sicherzustellen. Zuständig für Datenschutzfragen ist der Geschäftsführer der Energie Münchenbuchsee AG.

2 Datenschutz

2.1 Wann dürfen personenbezogene Daten bearbeitet werden?

Personenbezogene Daten der Energie Münchenbuchsee AG dürfen von den Mitarbeitenden ausschliesslich im Zusammenhang mit der Erfüllung ihrer Pflichten gegenüber dem Unternehmen bearbeitet werden.

Als "Bearbeitung" im Sinne dieser Datenschutzrichtlinie gilt jeder Umgang mit personenbezogenen Daten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten.

Als "personenbezogene Daten" gelten Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu

einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

2.2 Wer darf personenbezogene Daten bearbeiten und wie hat die Bearbeitung zu erfolgen?

Unsere Mitarbeitenden dürfen personenbezogene Daten ausschliesslich gemäss den ihnen zustehenden Berechtigungen bearbeiten. Diese Berechtigungen werden bei Eintritt des Mitarbeitenden durch den Vorgesetzten des Mitarbeitenden gemäss den internen Vorgaben festgelegt und durch IT-Service-Provider umgesetzt. Die Berechtigungen können durch den Vorgesetzten des Mitarbeitenden im Rahmen der internen Vorgaben ständig angepasst werden. Die Verarbeitung von Personendaten, welche im Rahmen des öffentlichen Auftrags verarbeitet werden, ist streng zweckgebunden. Darüber hinaus gehende Verarbeitungen, z.B. zu Marketingzwecken, sind unzulässig. Eine Nutzung von personenbezogenen Daten durch die Mitarbeitenden zu anderen Zwecken als zur Verrichtung der Arbeitstätigkeit ist untersagt. Es gilt das Gebot der Datensparsamkeit, insbesondere werden besonders schützenswerte Personendaten nur erfasst, wenn dies im Interesse des Kunden ist und im Rahmen des öffentlichen Auftrags nur, wenn dies in einem Gesetz explizit vorgesehen oder dies für die Erfüllung der Aufgabe zwingend erforderlich ist.

Mitarbeitende sind verpflichtet, zu jeder Zeit sicherzustellen, dass keine unberechtigte Dritte Kenntnis von personenbezogenen Daten nehmen können.

Mitarbeitende verpflichten sich, bei der Bearbeitung von personenbezogenen Daten die Vorgaben der auf das Unternehmen anwendbaren Datenschutzgesetze, welche in Bezug auf die konkrete Datenbearbeitung gelten, zu beachten. Ein Überblick über diese Vorgaben gibt die vorliegende Richtlinie. Es finden regelmässig interne wie externe Schulungen statt.

Auftragsdatenverarbeitende Partner orientieren sich wie unsere Mitarbeitenden an unserer Weisung über den Datenschutz und die Informationssicherheit. Mit unseren Partnern, welche in unserem Auftrag personenbezogene Daten verarbeiten, schliessend wir einen Vertrag ab, welcher auf dem vorliegenden Dokument basiert.

Mitarbeitende und Kunden nehmen zur Kenntnis, dass die Übermittlung von Informationen und Daten über das Internet nicht vollständig sicher ist. Obwohl wir geeignete technische Massnahmen zur Sicherung personenbezogener Daten implementiert haben, kann eine vollständige Sicherheit nicht garantiert werden.

Wir orientieren uns bezüglich des Standards zur Datensicherheit am gängigen Industriestandart.

2.3 Was für Rechte haben die betroffenen Personen?

Wenn die Voraussetzungen erfüllt sind, haben Kunden und andere betroffene Personen das Recht auf:

- Auskunft über den Umfang ihrer Personendaten, die Art der Speicherung und die Bearbeitungsweise sowie einer allfälligen Bekanntgabe an Dritte;
- eine Kopie ihrer personenbezogenen Daten in einem allgemein gebräuchlichen Format (nach revDSG);
- Übermittlung ihrer personenbezogenen Daten an ein anderes Unternehmen (nach revDSG);
- auf Berichtigung oder Löschung ihre personenbezogenen Daten;
- auf Widerspruch gegen die Bearbeitung ihrer personenbezogenen Daten durch uns.

Sämtliche Gesuche von Kunden oder andere betroffenen Personen müssen umgehend an die Geschäftsleitung weitergeleitet werden. Anfragen werden nur schriftlich und nicht telefonisch beantwortet. Es muss stets ein Identitätsnachweis (bspw. ID-/Passkopie) der betroffenen Person vorliegen. Gesuche werden innert Monatsfrist per Einschreiben beantwortet.

Mitarbeitende sind verpflichtet, im Rahmen der Kontaktpflege mit betroffenen Personen die Richtigkeit der personenbezogenen Daten regelmässig zu überprüfen. Stellt sich heraus, dass im System erfasste personenbezogene Daten nicht mehr aktuell sind, hat der Mitarbeitende diese umgehend zu berichtigen. Ist eine Berichtigung nicht möglich oder kann der Kunde die Richtigkeit seiner Daten bei Zweifeln nicht nachweisen, so erstattet der Mitarbeitende Meldung an die Geschäftsleitung.

2.4 Bekanntgabe an Behörden nach KDSG

Personendaten werden einer Behörde bekanntgegeben, wenn:

a) die verantwortliche Behörde zur Erfüllung ihrer Aufgabe gesetzlich dazu verpflichtet oder ermächtigt ist;
b) von der antragstellenden Behörde der Nachweis vorliegt, dass sie zu deren Bearbeitung gesetzlich befugt ist und keine Geheimhaltungspflicht entgegensteht; oder
c) die betroffene Person ausdrücklich zugestimmt hat.

2.5 Bekanntgabe an Private nach KDSG

Personendaten werden Privatpersonen bekanntgegeben, wenn:

a) wir gesetzlich dazu verpflichtet oder ermächtigt sind; oder
b) die betroffene Person ausdrücklich zugestimmt hat.

2.6 Welche personenbezogenen Daten werden durch uns bearbeitet?

Mitarbeitende dürfen personenbezogene Daten nur so weit von betroffenen Personen erheben und bearbeiten, als dies der Zweck der Datenbearbeitung erfordert (Datensparsamkeit).

Wir erheben und bearbeiten personenbezogene Daten über betroffene Personen in erster Linie, um unsere Dienstleistungen gemäss den auf uns anwendbaren gesetzlichen, vertraglichen und/oder regulatorischen Verpflichtungen zu erbringen. Darüber hinaus werden personenbezogene Daten bearbeitet, um interessierte Personen über das Leistungsangebot zu informieren.

Von uns werden keine besonders schützenswerten Personendaten erhoben/verarbeitet, mit Ausnahme von Daten über Massnahmen der sozialen Hilfe und Betreibungsdaten, soweit sie das Vertragsverhältnis direkt betreffen (Zahlungsverzug, Zahlungsabsprachen) oder wenn die Erfüllung einer gesetzlichen Aufgabe es zwingend erfordert.

Einige Datenbearbeitungen wie diejenige der Archivierung sind erforderlich, damit wir unseren gesetzlichen und/oder vertraglichen Verpflichtungen nachkommen können.

2.7 Wie werden die personenbezogenen Daten gespeichert und geschützt?

Wir schützen die personenbezogenen Daten gegen unerlaubten Zugriff, gegen gesetzeswidrige Datenbearbeitungen, Verlust und Zerstörung. Personenbezogene Daten werden nur so lange aufbewahrt, als dies aufgrund rechtlicher, regulatorischer und/oder anderweitigen Vorgaben erlaubt ist bzw. sich aus unseren berechtigten Interessen ergibt (namentlich im Rahmen der gesetzlichen Verjährungsfristen zwecks Abwehr oder Geltendmachung von Ansprüchen) sowie, sofern diese Dauer

kürzer ist, so lange, als die betroffene Person ihre Einwilligung zur entsprechenden Datenbearbeitung gegeben hat.

Soweit zulässig und machbar und um das Recht auf Privatsphäre der betroffenen Personen zu schützen, unternehmen wir angemessene Schritte, um Informationen zu entfernen oder zu anonymisieren. Zudem wird die Menge an personenbezogenen Daten, die von uns genutzt oder an Drittpersonen oder Behörden etc. übermittelt werden, auf ein Minimum beschränkt.

2.8 Reaktion auf das Bekanntwerden eines Datenschutz-Sicherheitsvorfalles

Stellen Mitarbeitende einen Verdacht auf einen Datenschutzvorfall im Unternehmen fest oder erhalten diese Kenntnis über einen Datenschutz-Sicherheitsvorfall (wie zum Beispiel Phishing-Mails, fehlende Verschlüsselungen, Datenlöschung, Verlust von Arbeitsgeräten oder Papierakten sowie sonstiger Malwareverdacht), müssen diese den Vorfall umgehend der Geschäftsleitung melden. Über mögliche Datenschutz-Sicherheitsvorfälle wird ein Register geführt. Dies gilt unabhängig davon, ob sich der Verdacht erhärtet hat oder nicht.

2.9 Welche Sanktionen drohen Mitarbeitenden?

Mitarbeitende sind verpflichtet, die Vertraulichkeit in Bezug auf sämtliche Daten (einschliesslich personenbezogene Daten) und Informationen sicherzustellen, über welche sie im Rahmen des Anstellungs- oder Mandatsverhältnisses Kenntnis erlangen. Die Mitarbeitenden nehmen zur Kenntnis, dass sie im Falle eines Verstosses gegen diese Pflicht der Vertraulichkeit durch uns und/oder direkt durch die betroffene Person zur Verantwortung gezogen werden können.

2.10 Speicherbegrenzung

Personendaten werden nur so lange gespeichert, wie sie für die Verarbeitungszwecke erforderlich sind. Die Dauer der Datenspeicherung bei einer gesetzlichen Aufbewahrungspflicht beträgt in der Regel zehn Jahre. Anschliessend werden die Daten gelöscht bzw. anonymisiert. Vorbehalten bleiben besondere Aufbewahrungsvorschriften sowie Vorschriften über die öffentlichen Archive (nach KDSG).

3 Informationssicherheit

3.1 Wie ist der Umgang mit Informatikmitteln?

Unsere IT-Ressourcen dienen in erster Linie der Erfüllung dienstlicher Zwecke. Der sorgfältige und verantwortungsvolle Umgang mit allen Informatikmitteln garantiert einen störungsfreien Betrieb und minimiert das Risiko von Geschäftsgeheimnis- und Datenschutzverletzungen.

3.1.1 Generell

Im Zusammenhang mit den Informatikmitteln gelten folgende Vorgaben:

a) Wir stellen allen Mitarbeitenden die für ihre Arbeit benötigten IT-Ressourcen zur Verfügung.
b) An den bereitgestellten IT-Ressourcen dürfen keine unautorisierten Änderungen an den Grundeinstellungen vorgenommen werden. Solche Änderungen führt ausschliesslich die IT-Abteilung bzw. der IT-Partner durch.
c) Mitarbeitende, die Informatikmittel von uns mit fremden Netzwerkgeräten (Modems, LAN-Kabel, USB-Modems, Wireless-Router usw.) verbinden sind für die Datensicherheit verantwortlich und schützen ihre Informatikmittel gemäss den internen Vorgaben
d) Für den Support sämtlicher IT-Ressourcen und die Entsorgung von ausgedienten oder defekten Informatikmittel ist ausschliesslich die IT-Abteilung bzw. der IT-Partner zuständig.

3.1.2 Bring your own device (BYOD)

a) Die Mitarbeitenden stellen ihre privaten Mobiltelefone zur Verfügung.
b) Für die geschäftliche Verwendung der privaten Mobiltelefone erhalten die Mitarbeitenden eine Spesenentschädigung gemäss Spesenreglement.
c) Aus Reparatur oder Verlust resultierende Kosten sind von den Mitarbeitenden zu tragen.
d) Es dürfen keine geschäftlichen Dokumente oder E-Mails auf privaten Backups oder Clouds gespeichert werden.
e) Bei Verlust des privaten Mobiltelefons ist uns dies unverzüglich zu melden.
f) Spätestens am letzten Arbeitstag müssen alle geschäftlichen Daten, Anwendungen und Passwörter unwiderruflich gelöscht werden.
g) Für private oder selbst administrierte mobile Geräte darf das Gäste-Netzwerk verwendet werden.

3.1.3 Anwendungen

Im Zusammenhang mit den Anwendungen gelten folgende Vorgaben:

a) Die Informatikmittel beinhalten ein Set an Standard-Anwendungen. Ein individueller Bedarf ist dem Vorgesetzten zu melden, welcher zusammen mit der IT-Abteilung bzw. dem IT-Partner abschliessend über die Freigabe der individuellen Anwendung entscheidet.
b) Mit Ausnahme der privaten Mobiltelefone dürfen keine fremden, nicht bewilligten bzw. freigegebenen IT-Ressourcen verwendet werden.
c) Auf zur Verfügung gestellten mobilen Geräten dürfen die für dienstliche Zwecke benötigten Anwendungen installiert werden.
d) Es ist insbesondere untersagt, nicht freigegebene Anwendungen auf Informatikmitteln von uns ohne Zustimmung durch die IT-Abteilung oder des IT-Partners herunterzuladen oder zu installieren.

4 Wie schütze ich Informationen?

4.1 Zugangsdaten

Wird ein Mitarbeitender aufgefordert, ein Passwort für den Zugang zu einem System, etc. auszuwählen, ist er dafür verantwortlich, dass dieses Passwort vertraulich verwaltet wird. Passwörter dürfen nicht an andere Mitarbeitende oder an Dritte weitergegeben werden.

Im Zusammenhang mit den Zugangsdaten gelten folgende Vorgaben:

a) Für sämtliche Zugänge ist ein neues, einzigartiges und starkes Passwort zu wählen. Die für die IT-Ressourcen verwendeten Passwörter dürfen nicht für private Zwecke verwendet werden.
b) Werden Mitarbeitende aufgefordert, ein Passwort für den Zugang zu einem System, etc. auszuwählen, sind sie dafür verantwortlich, dass dieses Passwort vertraulich verwaltet wird. Passwörter dürfen weder an andere Mitarbeitende, noch an Dritte weitergegeben werden.
c) Sämtliche Zugangsdaten (Benutzernamen, Passwort, etc.) für die IT-Ressourcen sind geheim zu halten und dürfen nirgends notiert oder aufgezeichnet werden. Gehen Zugangsdaten verloren oder besteht ein Verdacht auf Missbrauch muss umgehend eine Meldung die Geschäftsleitung gemacht werden.

4.2 Datenspeicherung

Im Zusammenhang mit der Datenspeicherung gelten folgende Vorgaben:

a) Sämtliche geschäftlichen Informationen sind ausschliesslich auf den von uns bereitgestellten Dateiablagesystemen (Laufwerke oder Clouddienste). Die Serverlaufwerke werden regelmässig gesichert. Lokal gespeicherte Informationen sind nicht von der Datensicherung erfasst.
b) Es ist verboten, geschäftliche Informationen auf einer privaten Cloud oder nicht freigegeben Clouddiensten (Dropbox, GoogleDrive, etc.) zu speichern.

4.3 Schutzstufen

Im Zusammenhang mit den Schutzstufen gelten folgende Vorgaben:

a) Sämtliche Informationen sind entweder als öffentlich, intern, vertraulich oder geheim klassifiziert. Die Schutzstufen werden separat geregelt und jährlich überprüft.
b) Die Informationen werden in separaten Laufwerken gespeichert, die Berechtigungen werden bei Eintritt vergeben und bei Bedarf angepasst.
c) Informationen, die Geschäftsgeheimnisse oder Personendaten enthalten, sind in jedem Fall zumindest als «intern», besonders schützenswerte Personendaten zumindest als «vertraulich» zu klassifizieren.

4.4 Clean Desk und Clear Screen Policy

Es herrscht eine strikte Clean Desk und Clean Screen Policy. Im Zusammenhang mit dieser Policy gelten folgende Vorgaben:

a) Es werden keine physischen Informationsträger (externe Speichermedien, Papier etc.) unbeaufsichtigt liegen gelassen. Bei längerer Abwesenheit am Arbeitsplatz von mehr als 10 Minuten müssen physische Informationsträger, die als «vertraulich» klassifizierte Informationen enthalten, weggeschlossen werden.
b) Dokumente mit als «vertraulich» klassifizierten Informationen sind unverzüglich und persönlich aus dem Drucker zu entfernen.
c) Whiteboards mit geschäftlichen Informationen sind nach Gebrauch zu reinigen / gebrauchte Flipcharts sind fachgerecht zu entsorgen.
d) Beim Verlassen des Arbeitsplatzes sind die Arbeitsplatzsysteme zu sperren (Windows Taste + L) oder es erfolgt eine Abmeldung vom System.

4.5 Zutritts- und Zugangsbeschränkung für externe Personen

Im Zusammenhang mit der Zutritts- und Zugangsbeschränkung gelten folgende Vorgaben:

a) Zutritt zu nicht öffentlich zugänglichen Räumen darf nur autorisierten bzw. angemeldeten Personen gewährt werden. Der Zutritt zum Empfang ist ohne Anmeldung erlaubt. Die Kunden werden nicht alleine gelassen.
b) Externe Personen dürfen sich nur in Begleitung in den Räumlichkeiten aufhalten. Sie haben sich am Empfang anzumelden und werden abgeholt. Sie werden nach dem Besuch wieder nach draussen begleitet.
c) Die Nutzung von Fotokopierern und Scannern durch externe Dritte ist ohne explizite Erlaubnis untersagt.
d) Die Haupteingangstüre ist beim Verlassen der Büros mit dem Schlüssel abzuschliessen.

5 Spezifische Nutzungs- und Schutzvorgaben

Das verantwortungsbewusste Handeln im Gebrauch mit IT-Ressourcen ist der entscheidende Sicherheitsfaktor. Es gelten die folgenden Schutzvorschriften (auch für eigens eingebrachte IT-Medien/BYOD):

5.1 Schutz vor Malware

a) Schutzsoftware darf nicht umgangen oder deaktiviert werden.
b) Es müssen immer sämtliche offiziellen Aktualisierungen und Updates installiert werden.
c) Verdächtige E-Mails bzw. solche von unbekannten Absendern müssen umgehend der Geschäftsleitung gemeldet werden. Enthaltene Dateien (Attachments) oder Links dürfen auf keinen Fall geöffnet oder gespeichert werden. Die IT-Abteilung bzw. der IT-Partner entscheiden zusammen mit der Geschäftsleitung abschliessend über das weitere Vorgehen.
d) Es dürfen keine Anhänge, die von unbekannten oder verdächtigen Absendern stammen, geöffnet werden.
e) Generell dürfen Werbungen oder Pop-Ups in Nachrichten/im Internet nicht angeklickt werden.
f) Externe Links dürfen nur dann angeklickt werden, wenn die URL auf eine vertrauenswürdige bzw. bekannte Webseite führt.
g) Auffälligkeiten und konkrete Verdachte müssen umgehend gemeldet werden.

5.2 E-Mail

Im Zusammenhang mit der E-Mailnutzung gelten folgende Vorgaben:

a) Mitarbeitende sind für die Kontrolle und Pflege ihres Postfachs verantwortlich.
b) Das automatisierte Um- oder Weiterleiten von persönlichen E-Mailadressen an die geschäftliche E-Mail-Adresse sowie in die Gegenrichtung ist nicht gestattet.
c) Abgehende E-Mails sind mit einer einheitlichen Signatur gemäss Vorgabe von uns zu versehen.
d) Bei Abwesenheiten ist eine Abwesenheitsmeldung zu aktivieren.
e) Besondere Personendaten und Informationen der Klassifizierung «vertraulich» oder höher dürfen nur im internen Netzwerk unverschlüsselt übertragen werden. Beim Versand an externe E-Mailadressen sind solche Informationen verschlüsselt zu übertragen.
f) Backups der Postfächer und Mailserver werden für mindestens ein (1) Jahr hinterlegt.
g) Zur Wiederherstellung von geschäftlichen E-Mails oder bei begründetem Verdacht auf Missbrauch kann die IT-Abteilung bzw. der IT-Partner auf Ankündigung hin über das Archivsystem auf die E-Mails der Mitarbeitenden zugreifen.
h) Der Inhalt von privaten E-Mails bleibt als Teil der Privatsphäre geschützt. Private E-Mails sind von den internen und externen Absendern durch die Vermerkoption «privat» zu kennzeichnen. Wir nehmen weder Einsicht noch bearbeiten wir E-Mails weiter, die als «privat» gekennzeichnet sind. Wenn kein Unterscheidungsvermerk zwischen privaten und geschäftlichen E-Mails besteht und die private Natur eines E-Mails aufgrund der Adressierungselemente nicht erkennbar ist, darf davon ausgegangen werden, dass das E-Mail geschäftlich ist.

5.3 Internetnutzung

Der Internetzugang auf Geräten, die von uns zur Verfügung gestellt wurden, ist für geschäftliche Zwecke bestimmt. Es gelten folgende Vorgaben:

a) Es dürfen nur Webseiten abgerufen bzw. Dateien heruntergeladen werden, die geschäfts- oder auftragsrelevant sind.
b) Up- und Downloads von grossen Dateien sind zu verhindern insbesondere sind die Installationen von Spielen und grossen Audio- und Videodateien aus dem Internet verboten;

c) Der Besuch von Webseiten, die über kein SSL-Zertifikat verfügen, ist zu vermeiden.
d) Der Besuch des Darknets (Thor-Browser) ist verboten.
e) Der Besuch von Webseiten mit folgenden Inhalten ist verboten: pornografische, sexistische, rassistische oder gewaltverherrlichende Äusserungen bzw. Darstellungen; kostenpflichtige Webseiten; Pyramiden- und Schneeballsysteme; Terrorismusförderung und -finanzierung; sonstige, rechtswidrige oder gegen die guten Sitten verstossende Inhalte.
f) Geschäftliche, mind. als «intern» klassifizierte Informationen dürfen nicht ins Internet hochgeladen werden, z.B. um Übersetzungen in Gratistools zu erwirken oder um Zusammenfassungen oder Antworten zu erhalten (bspw. mittels KI-Tools).

5.4 Videotelefonie / Remote Support

Für Telefonie- und Videokonferenzen sowie ggf. für den Remote Support gelten folgende Vorgaben:

a) Von unterwegs oder von zu Hause ist zwecks Wahrung des Geschäftsgeheimnisses ein Headset oder Kopfhörer zu tragen. Die Nutzung der Freisprechanlage ist im Beisein Dritter verboten.
b) Kameras sind so einzustellen, dass nur die Teilnehmenden und nicht auch unbeteiligte Dritte eingeblendet werden/Einsicht haben.
c) Der Arbeitsplatz ist während einer aktiven Telefon- oder Video-Konferenz /beim Remote Support nicht zu verlassen.
d) Es dürfen nur Bildschirme geteilt werden, welche die für die Teilnehmenden bestimmen Informationen enthalten und wenn die anderen Anwendungen bzw. Informationen ausgeblendet werden.
e) Bei grösseren Konferenzen ab 10 Personen ist die Videokonferenz so voreinzustellen, dass die Mikrofone und Kameras der Teilnehmenden von Beginn weg ausgeschaltet sind.

6 Kontakt

Bei Fragen oder Anmerkungen wenden Sie sich bitte an folgende Stelle:

Energie Münchenbuchsee AG
Geschäftsleitung
Löwenstrasse 4
3053 Münchenbuchsee
datenschutz@emag.energy

7 Inkrafttreten

Die vorliegende Weisung wurde an der Verwaltungsratssitzung vom 18.08.2023 genehmigt und tritt per 01.09.2023 in Kraft.

Energie Münchenbuchsee AG

Hermann Ineichen
Präsident des Verwaltungsrates

Daniel Krebs
Geschäftsführer