Bezeichnung der Richtlinie:	**Datenschutzrichtlinie**
Verantwortlich für die Richtlinie:	**Chief Legal Officer**
Inkrafttreten:	**März 2023 (Aktualisierung der Datenschutzrichtlinie vom Mai 2018)**

DATENSCHUTZRICHTLINIE

Die Beschäftigten der NEP Group (**„NEP“**) sind für den Schutz von NEP- und Mitarbeiterinformationen unabhängig vom Medium verantwortlich.

Für weitere Informationen lesen Sie bitte dieses Dokument.

INHALT

ERLÄUTERUNG UND STATUS DIESER RICHTLINIE:

NEP Group, Inc. wird zusammen mit ihren Tochtergesellschaften (siehe www.nepgroup.com/contact-us) in dieser Richtlinie als „**NEP**“ / das bzw. die „**Unternehmen**“ / „**wir**“ / „**uns**“ / „**unser**“ bezeichnet. Im Rahmen der Geschäftstätigkeit muss NEP bestimmte Informationen über Einzelpersonen erfassen und verarbeiten. Diese Informationen stammen unter anderem von aktuellen, ehemaligen und potenziellen Beschäftigten, Stellensuchenden, Kunden, Akkreditierern, Lieferanten und anderen Personen, mit denen NEP kommuniziert und Geschäfte tätigt.

Dabei sind wir gegenüber diesen Personen dafür verantwortlich, dass wir ihre Daten mit Sorgfalt und unter Einhaltung der Gesetze zum Schutz der Privatsphäre und zum Datenschutz (**„Datenschutzgesetze**“) nutzen. Unsere Marken- und Unternehmenswerte verlangen, dass wir geeignete Verfahren zur Datenverwaltung einführen und einhalten, einschließlich der in dieser Datenschutzrichtlinie (**„Richtlinie“**) dargelegten.

In dieser Richtlinie wird in Teil A dargelegt, wie NEP die Daten der Beschäftigten verwendet, und in Teil B werden einige der wichtigsten Maßnahmen erläutert, die NEP in Bezug auf die Datenverarbeitung von den Beschäftigten erwartet. In dieser Richtlinie werden unsere Regeln zum Datenschutz und die Bedingungen dargelegt, die in Bezug auf die Beschaffung, den Umgang, die Verarbeitung, die Speicherung, den Transport und die Vernichtung von personenbezogenen Daten eingehalten werden müssen.

TEIL A: DATENSCHUTZRECHTLICHE VERANTWORTUNG VON NEP IHNEN GEGENÜBER

Diese Bekanntmachung (**„Bekanntmachung“**) beschreibt die Kategorien personenbezogener Daten, die das Unternehmen NEP, bei dem Sie angestellt oder unter Vertrag sind („**NEP**“, „**wir**“, „**uns**“ und „**unser**“), in Bezug auf Beschäftigte und Auftragnehmer (**„Beschäftigte“** und „**Sie**“) erhebt, und die Zwecke, für die diese Daten verwendet werden. Der für die Verarbeitung Ihrer personenbezogenen Daten Verantwortliche ist das zur NEP Group gehörige Unternehmen, bei dem Sie beschäftigt oder unter Vertrag sind.

1. Art der über Sie erfassten Informationen

Zu den personenbezogenen Daten, die NEP im Rahmen der Zusammenarbeit mit Ihnen verarbeitet, gehören:

- Namen, Adressen, Telefonnummern und andere persönliche Kontaktangaben;
- Geschlecht, Geburtsdatum, von staatlicher Seite vergebene Nummern (z. B. Sozialversicherungsnummer, Personalausweisnummer), Führerschein, Einwanderungsstatus, Familienstand, nächste Angehörige;
- Personalunterlagen wie Schulungen, Beurteilungen, Lebensläufe, Leistungs- und Disziplinarinformationen sowie Nachfolgeplanung;
- Bankverbindung, Vergütung, Boni, Sozialleistungen und Renteninformationen;
- Bilder von Überwachungskameras und Telefonaufzeichnungen;
- Ihre Nutzung unserer Systeme und bereitgestellte Hard- und Software (siehe auch Abschnitt 6) sowie
- Reiseprotokoll, Kopien von Reisepässen, Kopien von Führerscheinen, Passwörter und Kennungen sowie VISA-Informationen.

2. Art und Weise der Verarbeitung Ihrer personenbezogenen Daten

Wir verarbeiten Ihre personenbezogenen Daten nur, wenn wir damit einen legitimen Zweck verfolgen. NEP führt eine Reihe von Aktivitäten mit Ihren personenbezogenen Daten durch, die je nach dem Unternehmen, bei dem Sie beschäftigt sind, Folgendes umfassen können:

Vertragliche Verpflichtungen: für die Erfüllung eines Vertrags oder um einen Vertragsabschluss mit Ihnen vorzubereiten:

- Abwicklung von Gehaltszahlungen, Sozialleistungen und Renten;
- Organisation Ihrer Beschäftigung und Ihrer Beziehung zu NEP sowie
- Strafregisterüberprüfungen, Bonitätsprüfungen und Sicherheitsüberprüfungen (gegebenenfalls).

Gesetzliche Verpflichtungen: für die Erfüllung einer gesetzlichen Verpflichtung, der wir unterliegen:

- Unterlagen zu und Verwaltung von Gesundheit und Sicherheit;
- Überwachung der Chancengleichheit (soweit gesetzlich vorgeschrieben);
- jede potenzielle Änderung der Kontrolle über ein Konzernunternehmen oder jeder potenzielle Übergang von Arbeitsverhältnissen im Zusammenhang mit einem Unternehmensübergang oder einem Wechsel des Dienstleisters (in Europa im Rahmen der Betriebsübergangsrichtlinie). Unter diesen Umständen dürfen personenbezogene Daten nur an den potenziellen Erwerber oder Investor und dessen Berater weitergegeben werden, soweit dies nach geltendem Recht zulässig ist, sowie
- Einhaltung der geltenden Verfahren, Gesetze und Vorschriften, einschließlich aller damit verbundenen Untersuchungen zur Sicherstellung der Konformität oder möglicher Verstöße.

Berechtigte Interessen: für die Verfolgung berechtigter Interessen von NEP oder von Dritten:

- Begründung, Ausübung oder Wahrung gesetzlicher Rechte von NEP;
- Bestätigung von Informationen in Lebensläufen und Anschreiben, Erstellung von Referenzschreiben und Durchführung von Referenzprüfungen;
- Bereitstellung von Mitarbeiterinformationen für Kunden und Agenturen im Rahmen der Erbringung der Dienstleistungen von NEP;
- Kameraüberwachung aus Sicherheitsgründen;
- Überwachung der Chancengleichheit;
- jede potenzielle Änderung der Kontrolle über ein Konzernunternehmen oder jeder potenzielle Übergang von Arbeitsverhältnissen im Zusammenhang mit einem Unternehmensübergang oder einem Wechsel des Dienstleisters (in Europa im Rahmen der Betriebsübergangsrichtlinie). Unter diesen Umständen dürfen personenbezogene Daten nur an den potenziellen Erwerber oder Investor und dessen Berater weitergegeben werden, soweit dies nach geltendem Recht zulässig ist;
- alle anderen angemessenen Zwecke im Zusammenhang mit der Beschäftigung oder der Beauftragung einer Person durch NEP;

- Einhaltung der geltenden Verfahren, Gesetze und Vorschriften, einschließlich aller damit verbundenen Untersuchungen zur Sicherstellung der Konformität oder möglicher Verstöße;
- sonstige Offenlegungen, die im Zusammenhang mit der Beschäftigung von Mitarbeitern zur Förderung oder Vermarktung von NEP, seinen Produkten oder Dienstleistungen erforderlich sind;
- Betrieb einer Ethik- oder Whistleblowing-Hotline, die NEP möglicherweise bereitstellt;
- Bereitstellung und Verwaltung der Nutzung von Dienstleistungen, die von Dritten erbracht werden, zum Beispiel vom Unternehmen zur Verfügung gestellte Mobiltelefone, Firmenkreditkarten und Firmenwagen sowie die Abrechnung dieser Dienstleistungen, sowie
- Schulungen und Beurteilungen, einschließlich Leistungsbewertungen und disziplinarische Unterlagen;
- Personalverwaltung, Gehaltsentscheidungen und Beförderungen sowie
- Nachfolgeplanung.

In bestimmten Fällen bitten wir Sie um Ihre ausdrückliche Zustimmung zur Verwendung Ihrer Daten. Wann immer wir Sie um Ihre Zustimmung bitten, erklären wir Ihnen, in welchen Situationen wir Ihre Daten verwenden und für welche Zwecke.

NEP kann auch personenbezogene Daten über Ihre nächsten Angehörigen erheben und verarbeiten, damit diese in einem Notfall oder im Zusammenhang mit der Nutzung eines von NEP zur Verfügung gestellten Firmenwagens kontaktiert werden können. Deren personenbezogene Daten werden ebenfalls in Übereinstimmung mit den Datenschutzgesetzen und wie in dieser Richtlinie beschrieben verarbeitet. Wenn NEP Sie dazu auffordert, personenbezogene Daten über andere Personen (einschließlich Ihrer nächsten Angehörigen) anzugeben, erwartet NEP von Ihnen, dass Sie diese Personen über die Erhebung ihrer personenbezogenen Daten informieren und ihre Zustimmung zur Verarbeitung ihrer personenbezogenen Daten durch uns gemäß den Datenschutzgesetzen und wie in dieser Richtlinie beschrieben einholen.

3. An wen wir Ihre personenbezogenen Daten weitergeben

Mitunter kann es erforderlich sein, Ihre personenbezogenen Daten an verbundene Unternehmen und Dritte weiterzugeben. Wir tun dies nur, wenn dies für die Erfüllung des Arbeitsvertrags mit Ihnen oder für unsere legitimen Geschäftszwecke erforderlich bzw. gesetzlich zulässig ist.

So können Ihre personenbezogenen Daten beispielsweise an folgende Stellen weitergegeben werden: (i) verbundene Unternehmen für die Zwecke der Personalverwaltung; (ii) externe Lieferanten, die Ihre Sozialleistungen in unserem Namen verwalten; (iii) unsere Beratern und Versicherer; (iv) unsere sorgfältig ausgewählten Dienstleister, die von Zeit zu Zeit beauftragt werden, Dienstleistungen im Zusammenhang mit unserem Geschäft und im Rahmen von Verträgen mit uns zu erbringen, wie z. B. Verarbeiter von Mitarbeiterdaten, Gehalts-, Spesen- und anderen Vergütungsinformationen; und (iv) externe Parteien, wenn dies gesetzlich oder in einem Gerichtsverfahren verlangt wird oder wenn Sie dies anderweitig genehmigt haben.

4. Datenübermittlung

NEP kann personenbezogene Daten an andere Konzernunternehmen, Partner, Lieferanten, Strafverfolgungsbehörden und andere Organisationen außerhalb des Europäischen Wirtschaftsraums (**„EWR“**), des Vereinigten Königreichs oder des Landes, in dem Sie sich befinden (bei Mitarbeitern, die außerhalb des EWR arbeiten), zu folgenden Zwecken übermitteln:

- Personalverwaltung (z. B. Einstellung und Verwaltung von Personal);

- Gehaltsabrechnung;
- Personalverlagerung;
- Visumanträge;
- Steuern und Anmeldungen;
- Erfüllung gesetzlicher Anforderungen von NEP;
- Erfüllung von Kundenverträgen über die Erbringung der Dienstleistungen von NEP;
- Gerichtsverfahren im Ausland sowie
- Auslagerung von NEP-Aufgaben.

Zu den Ländern, in die personenbezogene Daten übermittelt werden können, gehören u. a. die USA (wo NEP seinen Hauptsitz hat und wo einige seiner Dienstleister, z. B. Microsoft, ansässig sind), die Länder, in denen NEP tätig ist, sowie Standorte von Lieferanten und deren Datenzentren.

Wenn personenbezogene Daten von in der EU oder dem Vereinigten Königreich Beschäftigten aus dem EWR oder dem Vereinigten Königreichs übermittelt werden und wenn dies an ein NEP-Partnerunternehmen oder einen Lieferanten in einem Land erfolgt, das nicht Gegenstand einer Angemessenheitsentscheidung einer zuständigen Stelle wie der Europäischen Kommission ist, werden die Daten durch anerkannte Standardvertragsklauseln, wie sie von der Europäischen Kommission genehmigt wurden, oder durch die verbindlichen Unternehmensregeln eines Anbieters angemessen geschützt.

Wenn Sie eine Mitarbeiterin oder ein Mitarbeiter außerhalb des EWR sind und Ihre personenbezogenen Daten in ein anderes Land übermittelt werden, ergreift NEP Maßnahmen, um sicherzustellen, dass solche Übermittlungen in Übereinstimmung mit den geltenden lokalen Standards des Lands erfolgen, in dem Sie sich befinden.

NEP hat eine konzerninterne Datenübermittlungsvereinbarung auf der Grundlage genehmigter Übermittlungsmechanismen eingeführt, die die Übermittlung personenbezogener Daten innerhalb der NEP Group ermöglicht und erleichtert.

Wenn Sie mehr über diese Sicherheitsvorkehrungen und deren Anwendung erfahren möchten, kontaktieren Sie uns bitte über die weiter unten angegebenen Kontaktdaten oder wenden Sie sich an Ihren regionalen Datenschutzbeauftragten.

5. Aufbewahrung von Daten

NEP ist gesetzlich verpflichtet, bestimmte Daten für einen Mindestzeitraum aufzubewahren. NEP bewahrt personenbezogene Daten nicht länger auf, als es notwendig ist oder als es das geltende Recht vorschreibt. Weitere Informationen über die Vorgehensweise von NEP bei der Aufbewahrung von Daten erhalten Sie von Ihrem regionalen Datenschutzbeauftragten.

6. Überwachung

Überwachung der Systeme von NEP

Aus geschäftlichen Gründen und zur Umsetzung von IT-Sicherheitsmaßnahmen kann die Nutzung der Systeme von NEP auf entsprechenden Plattformen, wie Telefon (Mobiltelefone und Festnetz) und Computersysteme (wie E-Mail und Internetzugang), einschließlich deren private Nutzung überwacht werden, wenn und soweit dies zulässig oder gesetzlich vorgeschrieben und für geschäftliche Zwecke notwendig und vertretbar ist.

Soweit dies gesetzlich zulässig ist, können bei Verstößen gegen diese Richtlinie Maßnahmen im Rahmen von Disziplinarverfahren ergriffen werden.

Alle Geräte (insbesondere Computer und Mobiltelefone), die NEP den Beschäftigten im Rahmen ihrer Tätigkeit für das Unternehmen zur Verfügung stellt, sind ausschließlich für den geschäftlichen Gebrauch bestimmt.

NEP behält sich das Recht vor, den Inhalt von Nachrichten abzurufen, im Internet durchgeführte Suchen zu überprüfen, die sofortige Rückgabe der von NEP zur Verfügung gestellten Geräte zu verlangen und auf die auf diesen Geräten gespeicherten Daten zu folgenden Zwecken zuzugreifen:

- um zu überwachen, ob die Nutzung des E-Mail-Systems oder des Internets rechtmäßig ist und im Einklang mit dieser Richtlinie steht (und die Beschäftigten willigen ein, dass NEP Software einsetzen kann, um die Identität von Absendern und Empfängern von E-Mails zu überwachen);
- um verlorene Nachrichten zu finden oder um Nachrichten wiederherzustellen, die durch einen Computerausfall verloren gegangen sind;
- um bei der Untersuchung von unrechtmäßigen Handlungen mitzuwirken, einschließlich solcher, die gegen unsere anderen Richtlinien oder geltendes Recht verstoßen; sowie
- um einer gesetzlichen Verpflichtung nachzukommen.

Eine der Bedingungen für die Nutzung unserer IT-Systeme ist, dass Sie sich professionell verhalten, den guten Namen des Unternehmens nicht in Verruf bringen und sich gegenüber Ihren Kolleginnen und Kollegen sowie anderen Personen, mit denen Sie während Ihrer Tätigkeit für NEP über Kommunikationsmittel in Kontakt treten, nicht unangemessen verhalten. Wenn Hinweise für einen Verstoß gegen diese Bedingungen oder für einen Missbrauch der IT-Systeme von NEP vorliegen, kann NEP eine ausführlichere Untersuchung gemäß unseren Regeln für Disziplinarverfahren durchführen, welche die Prüfung und Offenlegung von Überwachungsaufzeichnungen gegenüber denjenigen, die für die Untersuchung benannt wurden, und allen Zeugen oder Managern, die am Disziplinarverfahren beteiligt sind, beinhaltet. Gleiches gilt, wenn NEP den begründeten Verdacht hat, dass unrechtmäßige Aktivitäten oder Handlungen, die gegen unsere anderen Richtlinien und Verfahrensregeln verstoßen, stattgefunden haben.

Kameraüberwachung

Einige Gebäude und Standorte von NEP werden aus Sicherheitsgründen 24 Stunden am Tag mit Überwachungskameras außen und innen überwacht. Diese Daten werden aufgezeichnet und können archiviert werden, um sie zu einem späteren Zeitpunkt einzusehen. Der Einsatz von Kameraüberwachung und die Aufzeichnung von Videoüberwachungsdaten erfolgt nur in Übereinstimmung mit den von NEP genehmigten Leitlinien.

7. Ihre Rechte in Bezug auf Ihre Daten

Gemäß den Datenschutzgesetzen haben Sie möglicherweise das Recht, NEP um eine Kopie Ihrer personenbezogenen Daten zu bitten, diese Daten zu korrigieren, zu löschen oder ihre Verarbeitung einzuschränken, oder NEP zu bitten, einige dieser Daten an andere Organisationen zu übertragen. Sie haben möglicherweise auch das Recht, einer bestimmten Verarbeitung Ihrer personenbezogenen Daten zu widersprechen und, wenn NEP Sie um Ihre Zustimmung zur Verarbeitung personenbezogener Daten gebeten hat, diese Zustimmung zu widerrufen. Diese Rechte können in bestimmten Situationen eingeschränkt sein, z. B., wenn NEP nachweist, dass die Verarbeitung Ihrer Daten gesetzlich vorgeschrieben ist. Unter Umständen kann dies bedeuten, dass die Daten auch dann gespeichert werden, wenn Sie Ihre Zustimmung zurückziehen.

Wenn NEP personenbezogene Daten benötigt, um gesetzlichen oder vertraglichen Verpflichtungen nachzukommen, ist die Bereitstellung dieser Daten obligatorisch: Wenn diese Daten nicht bereitgestellt werden, kann NEP das Beschäftigungsverhältnis nicht ordnungsgemäß verwalten oder die uns auferlegten Verpflichtungen nicht erfüllen. In allen anderen Fällen ist die Angabe der angeforderten personenbezogenen Daten freiwillig.

Ihre Daten werden nicht für eine automatisierte Entscheidungsfindung verwendet (eine Entscheidung, die ausschließlich mit automatisierten Mitteln ohne menschliche Beteiligung getroffen wird), die rechtliche Auswirkungen hat oder sich auf andere Weise erheblich auf Sie auswirkt.

Um Ihre Rechte in Bezug auf Ihre Daten auszuüben, Bedenken oder Beschwerden zu äußern oder Fragen zur Verarbeitung personenbezogener Daten von Beschäftigten durch NEP zu stellen, wenden Sie sich bitte an Ihren regionalen Datenschutzbeauftragten.

Sie haben das Recht, sich direkt bei den Datenschutzbehörden zu beschweren. Die zuständige Datenschutzbehörde ist die Aufsichtsbehörde in dem Land, in dem Ihr Arbeitgeber ansässig ist.

TEIL B: IHRE DATENSCHUTZRECHTLICHE VERANTWORTUNG GEGENÜBER ANDEREN

8. Datenschutzteam

NEP hat ein Team von regionalen Datenschutzbeauftragten ernannt, die das Unternehmen bei der Einhaltung seiner Verpflichtungen im Rahmen der Datenschutzgesetze unterstützen. Die Hauptaufgabe der regionalen Datenschutzbeauftragten besteht darin:

- eine Anlaufstelle und Unterstützung für die Beschäftigten zu bieten;
- Datenschutz-Folgenabschätzungen durchzuführen und zu begleiten;
- Schulungen für die Beschäftigten anzubieten;
- mit der lokalen Datenschutzbehörde in Verbindung zu treten sowie
- Anträge auf Zugang zu Informationen und zu anderen Rechten der betroffenen Personen zu bearbeiten.

Wenn Sie nach der Lektüre dieser Richtlinie oder zu irgendeinem Zeitpunkt Fragen zum Umgang mit personenbezogenen Daten haben, wenden Sie sich bitte an Ihren regionalen Datenschutzbeauftragten.

Ihre regionale Datenschutzbeauftragte oder Ihren regionalen Datenschutzbeauftragten finden Sie hier: (https://nepanywhere.oak.com/u/5EA8F785).

Wenn Sie Ihren regionalen Datenschutzbeauftragten aus irgendeinem Grund nicht erreichen können, wenden Sie sich bitte an Information Services oder NEP Legal.

Dieser Teil der Richtlinie soll die Beschäftigten darüber informieren, wie sie unter bestimmten Umständen mit personenbezogenen Daten umzugehen haben. Alle Beschäftigten sind verpflichtet, die Datenschutzgesetze einzuhalten. Jede und jeder Einzelne muss sich der eigenen Verantwortung für den Datenschutz gegenüber anderen gemäß den Datenschutzgesetzen bewusst sein.

Dazu gehört auch die Notwendigkeit, die unten aufgeführten Leitlinien und Verfahren zu befolgen. Wichtige Punkte, die Sie beachten sollten:

- Überlegen Sie, welche Pflichten Sie gemäß den Datenschutzgesetzen und dieser Richtlinie haben und wie sich diese auf Ihre täglichen Aktivitäten auswirken.
- Geben Sie personenbezogene Daten (oder geschäftlich sensible Daten) nur auf einer Need-to-know-Basis weiter. Geben Sie nicht eine ganze Datenbank frei, wenn nur ein Teil davon benötigt wird.
- Überprüfen Sie die Kontaktdaten des Empfängers, bevor Sie Daten weitergeben. Senden Sie die Daten wie vorgesehen oder gefährden Sie das Unternehmen?
- Verwenden Sie einen Passwortschutz für Dokumente und Dateien, wo immer dies sinnvoll ist.

- Verwenden Sie personenbezogene Daten nur in der Weise, in die die betroffene Person eingewilligt hat oder wie in dieser Richtlinie dargelegt.
- Gehen Sie mit gesundem Menschenverstand vor, wenn Sie entscheiden, wie Sie personenbezogene Daten schützen, verwenden und entsorgen. Überlegen Sie, wie Sie möchten, dass mit Ihren personenbezogenen Daten umgegangen wird.

Dieser Abschnitt dient als allgemeine Orientierungshilfe und stellt keinen umfassenden oder erschöpfenden Leitfaden dar. Je nach der genauen Art Ihrer Tätigkeit haben Sie möglicherweise zusätzliche Verpflichtungen gegenüber anderen im Rahmen der Datenschutzgesetze.

9. Grundsätze des Datenschutzes

Bei der Verarbeitung personenbezogener Daten müssen NEP und die Beschäftigten bestimmte in den Datenschutzgesetzen enthaltene Datenschutzgrundsätze beachten. Dazu gehört, dass die personenbezogen Daten:

- nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden müssen;
- nur für einen oder mehrere festgelegte und rechtmäßige Zwecke verarbeitet werden dürfen und nicht in einer Weise weiterverarbeitet werden dürfen, die mit diesen Zwecken unvereinbar ist, es sei denn, dies ist nach geltendem Recht ausdrücklich zulässig;
- den Zwecken entsprechen, für die sie verarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen;
- richtig sind und, falls erforderlich, auf dem neuesten Stand gehalten werden;
- nicht länger aufbewahrt werden, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;
- in Übereinstimmung mit den Rechten des Einzelnen verarbeitet werden, einschließlich des Rechts, unter bestimmten Umständen Zugang zu personenbezogenen Daten zu erhalten, sie an einen Dritten zu übermitteln, sie zu löschen, wenn sie unrichtig sind oder nicht mehr benötigt werden, und nicht Gegenstand bedeutender automatisierter Entscheidungs-prozesse zu sein;
- sicher aufbewahrt werden sowie
- nur dann in ein Land oder Gebiet außerhalb des Landes oder Gebiets, in dem die personenbezogenen Daten erhoben wurden, übermittelt oder von dort abgerufen werden dürfen, wenn dieses andere Land oder Gebiet ein angemessenes Schutzniveau für die Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten gewährleistet oder wenn angemessene vertragliche Garantien zum Schutz der Daten vorhanden sind.

10. Sichere Aufbewahrung von Daten

Die Bestimmungen dieses Abschnitts und des Abschnitts 4 (Meldung mutmaßlicher Verstöße gegen die Datensicherheit) beziehen sich nicht nur auf personenbezogene Daten, sondern auf alle Informations-, IT- und Kommunikationssysteme. Sie sind verantwortlich für die Sicherheit, der Ihnen zugewiesenen oder von Ihnen genutzten Geräte und Sie dürfen nicht zulassen, dass diese von anderen Personen als in dieser Richtlinie vorgesehen genutzt werden.

Sicherheit von Computern/Laptops:

- Alle IT-Benutzer haben eigene Kontodaten erhalten. Sie dürfen Konten oder Passwörter nicht weitergeben. Sie dürfen keine Konten verwenden, die Ihnen nicht zugewiesen sind, und Ihre Kontodaten nicht an andere weitergeben.

- Sie sollten Ihren Computer, Laptop oder Ihr Handheld-Gerät immer sperren, abmelden oder herunterfahren, wenn Sie das Gerät unbeaufsichtigt lassen (z. B., um an Besprechungen teilzunehmen oder während der Mittagspause). Die IT-Systeme von NEP sind, soweit
- möglich, so konzipiert, dass sie nach einer bestimmten Zeit der Inaktivität automatisch gesperrt oder beendet werden.
- Am Ende eines jeden Arbeitstages sollten Sie sicherstellen, dass Ihr Computer ordnungsgemäß heruntergefahren und Ihr Monitor ausgeschaltet ist. Wenn Sie einen Laptop haben, sollten Sie ihn sicher aufbewahren, zum Beispiel in einem verschlossenen Schrank oder in einer Schublade.
- Stellen Sie sicher, dass sensible Geschäftsinformationen, die auf einem Bildschirm angezeigt werden, nicht einfach eingesehen werden können.
- Sie müssen ein sicheres Passwort verwenden (z. B. eine Mischung aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen) und es vertraulich behandeln. Sie sollten es regelmäßig ändern. Wenn Sie glauben, dass jemand Ihr Passwort kennt, müssen sie es umgehend ändern.
- Änderungen oder Wartungsarbeiten an Ihrem Computer oder Ihrer IT-Ausrüstung oder die Installation von Hard- oder Software auf von NEP verwalteten Geräten dürfen nur vom Information Services Team von NEP, den entsprechenden Mitarbeitern oder autorisierten Personen mit ausdrücklicher Genehmigung des Information Services Teams vorgenommen werden.
- Melden Sie den Verlust oder Diebstahl eines Geräts wie eines Laptops oder Mobiltelefons sofort, auch wenn Ihr Telefon für den persönlichen Gebrauch bestimmt ist.
- Melden Sie jede verdächtige Aktivität auf Ihrem Computer, die nicht normal zu sein scheint.

<u>Zugriff auf elektronisch gespeicherte Daten</u>:

- Verwenden Sie Passwörter, um den Zugriff auf sensible Dateien zu beschränken.
- Umgehen Sie keine festgelegten Sicherheitsklassifizierungen oder Berechtigungsstufen.
- Erstellen Sie ein Protokoll für Änderungen an Datenbanken oder Dokumenten, die sensible Informationen enthalten.
- Verhindern Sie keine geplanten IT-Backup-Prozesse.

<u>Sicherheit von Mobilgeräten:</u>

- Wenn Sie Zugang zu den von NEP unterstützten IT-Systemen oder der IT-Infrastruktur erhalten haben, sind Sie für deren Sicherheit verantwortlich und haben angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass sie nicht von Unbefugten benutzt werden, verloren gehen, gestohlen oder beschädigt werden, insbesondere auf Reisen oder wenn Sie sich außerhalb des Büros befinden.
- Mobilgeräte dürfen zu keiner Zeit, insbesondere nicht über Nacht, im Fahrzeug verbleiben. Sollte dies unumgänglich sein, sollten Sie dafür sorgen, dass sie nicht zu sehen sind.
- Wenn Sie Mobilgeräte z. B. in öffentlichen Verkehrsmitteln oder an einem öffentlichen Ort wie einem Hotelfoyer verwenden, sollten Sie sicherstellen, dass der Bildschirm nicht von anderen gelesen werden kann, und Sie sollten hinsichtlich dieses Risikos entsprechende Vorsichtsmaßnahmen treffen.

- Wenn Sie Ihr Mobilgerät in einem externen oder fremden Netzwerk verwenden, z. B. in einem Hotel oder Flughafen, sollten Sie angemessene Maßnahmen ergreifen, um sicherzustellen, dass das Netzwerk sicher ist, etwa durch die Nutzung eines von einem seriösen Unternehmen bereitgestellten Netzwerks, das vorzugsweise passwortgeschützt und nicht uneingeschränkt verfügbar ist. Wenn Sie Zweifel an der Sicherheit des Netzwerks haben, sollten Sie Ihr Gerät nicht mit diesem verbinden.
- Sie dürfen nicht versuchen, Verschlüsselungssoftware oder Sicherheitsfunktionen auf den Mobilgeräten zu umgehen.
- NEP verwendet eine Kombination der folgenden Sicherheitsfunktionen auf Mobilgeräten:
    - Benutzernamen/Passwörter und PIN-Nummern;
    - Antivirenprogramme;
    - Datenverschlüsselung;
    - Kontosperrung nach fehlgeschlagenen Zugriffsversuchen;
    - Geräte- bzw. Anwendungssperre nach Inaktivität;
    - Konto- oder Gerätesperre nach Diebstahl/Verlust;
    - Überwachung der Nutzung sowie Löschung von Inhalten auf verlorenen oder gestohlenen Geräten.

<u>Sicherheit personenbezogener Daten in Papierform im Büro:</u>

- Bewahren Sie personenbezogene Daten und sensible Geschäftsinformationen nicht auf Ihrem Schreibtisch auf.
- Lassen Sie personenbezogene Daten oder sensible Geschäftsinformationen nicht unbeaufsichtigt auf den Schreibtischen liegen.
- Wenn Sie sensible personenbezogene Daten oder sensible Geschäftsinformationen ausdrucken, stellen Sie sicher, dass Sie am Drucker stehen, um sie an sich zu nehmen, damit sie nicht von jemand anderem genommen werden.
- Lassen Sie keine personenbezogenen Daten oder sensible Geschäftsinformationen in Besprechungsräumen oder anderen Bereichen der Niederlassung zurück, nehmen Sie sie mit und entsorgen Sie sie sicher, wenn Sie sie nicht mehr benötigen. Wischen Sie Whiteboards ab, bevor Sie Sitzungsräume verlassen, es sei denn, Sie haben eine klare Anweisung, dies nicht zu tun.
- Bewahren Sie Unterlagen mit personenbezogenen Daten und sensiblen Geschäftsinformationen über Nacht an einem sicheren Ort auf, z. B. in einem abschließbaren Aktenschrank, einer Schublade oder in einem zutrittsbeschränkten oder abschließbaren Bereich/Raum.
- Befolgen Sie alle speziellen Anweisungen, die für Ihren Standort oder Ihre Abteilung gelten.

<u>Sicherheit personenbezogener Daten in Papierform außerhalb des Büros:</u>

- Nehmen Sie personenbezogene Daten oder sensible Geschäftsinformationen nur dann außerhalb des Büros oder des Firmengeländes mit, wenn dies unbedingt erforderlich ist.
- Seien Sie sich der Risiken eines Verlusts oder Diebstahls bewusst und treffen Sie geeignete Vorsichtsmaßnahmen, um sicherzustellen, dass personenbezogene Daten oder sensible Geschäftsinformationen sicher aufbewahrt sind.

- Lassen Sie personenbezogene Daten oder sensible Geschäftsinformationen niemals unbeaufsichtigt in der Bahn, in anderen öffentlichen Verkehrsmitteln oder an anderen öffentlichen Orten liegen. Stellen Sie sicher, dass sensible Geschäftsinformationen nicht leicht einzusehen sind, wenn Sie sich an einem öffentlichen Ort aufhalten.
- Speichern oder archivieren Sie personenbezogene Daten oder sensible Geschäfts-informationen außerhalb des Unternehmens nur bei einem von NEP zugelassenen Anbieter, mit dem ein schriftlicher Vertrag besteht.

Verwendung mobiler Speichermedien:

Mobile Speichermedien (**„Medien**“) sind alle tragbaren Geräte, die Daten speichern, übertragen, ändern oder löschen können, wie zum Beispiel Mobilgeräte, USB-Sticks, externe Festplatten und optische Medien (CDs, DVDs usw.).

- Daten dürfen nur dann von den IT-Systemen von NEP auf andere Medien übertragen werden, wenn es einen triftigen geschäftlichen Grund dafür gibt und die Bestimmungen dieser Richtlinie sowie die Anweisungen des Information Services Teams befolgt werden.
- NEP überwacht alle Daten, die aus dem Netzwerk kopiert werden, um unbefugte Datenübermittlungen zu erkennen und Sicherheitsverstöße zu verhindern.
- Der Austausch von Daten sowohl intern wie auch mit externen Parteien sollte immer über NEP-Informationssysteme wie E-Mail oder gemeinsame Datenbereiche erfolgen. Datenträger sollte nur dann zur Datenübermittlung verwendet werden, wenn alle anderen Möglichkeiten ausgeschöpft sind.
- Alle Medien, die physisch zwischen NEP und/oder einem Kunden ausgetauscht werden, sollten per Spezialversand verschickt werden (um sicherzustellen, dass die Medien nachverfolgt und bei Verlust wiedergefunden werden können).
- Bevor Sie Medien verwenden, beachten Sie bitte:
    - Sie dürfen nur Medien verwenden, die über NEP Information Services erworben oder von NEP Information Services autorisiert wurden und verschlüsselt sind.
    - Die Medien sollten nachverfolgt werden können, um sicherzustellen, dass sie am vorgesehenen Zielort ankommen.
    - Die Medien müssen vor der Verwendung mit einer vom NEP Information Services Team zur Verfügung gestellten Virenscanning-Software auf Malware/Viren überprüft werden und dürfen nicht verwendet werden, wenn möglicherweise Schadprogramme darauf vorhanden sind.
    - Speichern Sie nur Daten, die unbedingt erforderlich sind, d. h., laden Sie nicht die gesamte Datenbank herunter, wenn nur kleine Teile davon benötigt werden.
    - Prüfen Sie, ob das mobile Speichermedium die personenbezogenen Daten verschlüsseln kann.
    - Stellen Sie sicher, dass die Dateien auf dem Medium mit einem Passwort geschützt sind und das Passwort separat vom verschlüsselten Datenträger übermittelt wird.
    - Löschen Sie die Daten umgehend von den Medien, sobald sie nicht mehr benötigt werden.
    - Nicht wiederverwendbare Medien müssen am Ende ihres Lebenszyklus gemäß den Empfehlungen des Information Services Teams ordnungsgemäß entsorgt/vernichtet werden.

Einschränkungen bei der Verwendung nicht autorisierter Geräte oder Software:

- Hardware, die nicht vom Information Services Team beschafft und/oder verwaltet wird (z. B. eigene oder fremde Laptops, Tablets, Smartphones, Mobiltelefone, Speichersticks usw.) darf ohne ausdrückliche Genehmigung des Information Services Teams nicht an NEP-Geräte oder -Netzwerke angeschlossen oder dort installiert werden.
- Sie dürfen keine unlizenzierte Software, Software von Drittanbietern, frei verfügbare Software oder ähnliche Software auf Ihren Computer oder andere IT-Geräte herunterladen, da sie Viren oder anderen Schadcode enthalten können, die die Sicherheit der Systeme von NEP beeinträchtigen können.

Zugriff durch Dritte:

- NEP ist für die Handlungen und Unterlassungen seiner Lieferanten und Auftragnehmer verantwortlich, die in unserem Namen auf personenbezogene Daten zugreifen oder diese verarbeiten. Wenn Sie Auftragnehmer, Berater und Aushilfspersonal beschäftigen, der Zugang zu den Systemen von NEP und/oder personenbezogenen Daten haben, müssen diese zunächst eine Vereinbarung unterzeichnen, die Bestimmungen enthält, die die personenbezogenen Daten von NEP angemessen schützen, z. B. solche zu Vertraulichkeit und Sicherheit. Wenden Sie sich an den Leiter der Personalabteilung oder den zuständigen Justiziar, um sich über die erforderlichen Bestimmungen zu informieren.
- Insbesondere erfordert jedes Projekt, das den Anschluss eines Dritten/Lieferanten an die Systeme von NEP vorsieht, eine spezielle Bewertung der Risiken und zusätzliche Vertragsbedingungen mit Bezug zur Sicherheit.
- Alle Änderungen am Zugang von Dritten/Lieferanten zum Netzwerk von NEP sind zu überprüfen und zu dokumentieren, um sicherzustellen, dass die Sicherheit gewährleistet ist.
- Wenn der Zugriff Dritter/Auftragnehmer nicht mehr erforderlich ist, muss der Zugang beendet werden und alle personenbezogenen Daten, die der Dritte/Auftragnehmer erhalten hat, sind gemäß den Vertragsbedingungen zurückzugeben oder zu vernichten.
- Alle Drittanbieter und Auftragnehmer sind verpflichtet, NEP über ihren Hauptansprechpartner über alle Vorfälle im Bereich der Informationssicherheit, die bei ihnen oder ihren Kunden auftreten, zu informieren.

Datensicherung:

- Wann immer es möglich ist, sollten Daten in einem Netzwerkspeicher gespeichert werden, da sie so mit Hilfe automatisierter Prozesse leicht gesichert werden können. Wechseldatenträger wie USB-Sticks und CDs sollten nicht für die Speicherung geschäftskritischer Daten verwendet werden, da sie dann nicht gesichert werden und daher nicht wiederhergestellt werden können, wenn sie verloren gehen, beschädigt oder versehentlich gelöscht werden.

Vernichtung personenbezogener Daten:

Personenbezogene Daten in Papierform müssen über Abfallbehälter für vertrauliche Dokumente oder mit Hilfe von Aktenvernichtern entsorgt werden. Wenn kein Behälter für vertrauliche Abfälle zur Verfügung steht, wenden Sie sich bitte an den für den jeweiligen Standort bzw. das Gebäude zuständigen Facility Manager, um die Abholung zu organisieren.

- Stellen Sie sicher, dass sämtliche personenbezogenen Daten von IT-Hardware, Mobilgeräten, mobilen Speichermedien oder anderen Geräten vor deren Vernichtung ordnungsgemäß gelöscht werden. Nicht wiederverwendbare Medien wie CD-ROMs müssen am Ende ihres Lebenszyklus ordnungsgemäß entsorgt oder vernichtet werden. Wenden Sie sich an das Information Services Team, um sicherzustellen, dass dies korrekt durchgeführt wird.

E-Mail und Systemnutzung:

- Es ist nicht gestattet, eine Virenschutzsoftware zu umgehen, indem Sie sie beispielsweise deaktivieren.
- Mitarbeiterinnen und Mitarbeiter sollten Vorsicht walten lassen, wenn sie E-Mails von unbekannten externen Quellen öffnen oder wenn eine E-Mail aus irgendeinem Grund verdächtig erscheint (z. B., wenn ihr Name auf .exe endet).
- Das Information Services Team sollte sofort informiert werden, wenn Sie einen mutmaßlichen Virus empfangen oder identifiziert haben oder wenn Sie einen Link in einer E-Mail angeklickt haben und aufgefordert wurden, persönliche Informationen preiszugeben.
- NEP behält sich das Recht vor, den Zugriff auf E-Mail-Anhänge zu blockieren, um eine effektive Nutzung der IT-Systeme von NEP und die Einhaltung dieser Richtlinie zu gewährleisten.
- NEP behält sich außerdem das Recht vor, keine E-Mail-Nachrichten (eingehend oder ausgehend) zu übermitteln, wenn der Verdacht besteht, dass sie einen Virus enthalten.
- Vorbehaltlich bestimmter Bedingungen, die unten aufgeführt sind, erlaubt NEP die gelegentliche Nutzung von Internet-, E-Mail- und Telefonsystemen, um private E-Mails zu versenden, im Internet zu surfen und private Telefongespräche zu führen. Die private Nutzung ist ein Privileg und kein Recht. Sie darf weder missbraucht noch überstrapaziert werden und NEP behält sich das Recht vor, die Erlaubnis jederzeit zurückzuziehen. NEP behält sich das Recht vor, den Zugang zu bestimmten Telefonnummern oder Internetseiten einzuschränken oder zu verhindern, wenn die private Nutzung als übermäßig angesehen wird. Die folgenden Bedingungen müssen erfüllt sein, damit die private Nutzung fortgesetzt werden kann:
    - Die Nutzung muss minimal sein und im Wesentlichen außerhalb der normalen Arbeitszeiten stattfinden;
    - die Nutzung darf nicht mit geschäftlichen oder dienstlichen Verpflichtungen kollidieren und
    - durch die Nutzung dürfen NEP keine Grenzkosten entstehen.
- Die Nutzung von Webmail-Seiten (wie Hotmail, Yahoo und Gmail) zum Senden oder Empfangen von geschäftsbezogenen Informationen ist verboten, es sei denn, es liegt ein triftiger geschäftlicher Grund vor, der vom Information Services Team genehmigt wurde. Der gesamte E-Mail-Verkehr im Zusammenhang mit geschäftlichen Aktivitäten ist über ein genehmigtes E-Mail-System des Unternehmens abzuwickeln.

Kontaktdaten der Kunden:

- Sie dürfen keine gedruckten Adressbücher, andere Unterlagen oder Geräte mit Geschäftskontakten unbeaufsichtigt lassen.
- Die elektronische Speicherung von Geschäftskontakten muss in einem sicheren Bereich im NEP-Netzwerk erfolgen.

11. Meldung mutmaßlicher Verletzungen der Datensicherheit

Eine Verletzung der Datensicherheit kann z. B. durch Diebstahl von Daten (wie zum Beispiel physischer Kopien), ungesicherte Übermittlungsmethoden oder eine falsche Art der Entsorgung von Daten oder Datenträgern verursacht werden.

Wenn Sie von einer Verletzung der Sicherheit personenbezogener Daten (oder anderer Daten) Kenntnis erlangen oder den Verdacht haben, dass eine solche aufgetreten ist, müssen Sie dies unverzüglich Ihrem regionalen Datenschutzbeauftragten, dem IT Service Desk, ITSecurity@nepgroup.com und Ihrem Vorgesetzten melden, der gegebenenfalls die zuständige Datenschutzbehörde und die von der Verletzung der Datensicherheit betroffenen Personen benachrichtigt.

Weitere Informationen darüber, wie Sie mutmaßliche Verletzungen der Datensicherheit melden können, entnehmen Sie der ***Verfahrensanweisung für Sicherheitsvorfälle*** *von NEP*.

12. Gewährleistung der Richtigkeit und Aktualität personenbezogener Daten

Ungenauigkeiten in den von NEP gespeicherten personenbezogenen Daten sollten von den Beschäftigten in allen relevanten Systemen korrigiert werden. Aktualisierungen oder Änderungen an den von einer Person bereitgestellten Informationen sollten auch in den Unterlagen von NEP vorgenommen werden.

Die betroffenen Personen müssen über ihr Recht auf Zugang, Berichtigung, Löschung oder Einschränkung der Verarbeitung ihrer erhobenen personenbezogenen Daten informiert werden.

13. Sichere Vernichtung personenbezogener Daten

Wenn personenbezogene Daten nicht mehr benötigt werden, ist sicherzustellen, dass sie sorgfältig und sicher vernichtet werden.

Wenn Sie ein Auskunftsersuchen erhalten, das sich auf ein Datenschutzgesetz bezieht, wenden Sie sich bitte unverzüglich an Ihren regionalen Datenschutzbeauftragten, um sicherzustellen, dass die Anfrage innerhalb der vorgeschriebenen Fristen ordnungsgemäß bearbeitet wird.

14. Datenschutz-Folgenabschätzungen

Wenn Sie neue Prozesse, Richtlinien oder Verfahren einführen, ein neues Projekt in Angriff nehmen oder neue Systeme kaufen, die die Verarbeitung oder Übermittlung großer Mengen personenbezogener Daten beinhalten oder, die wesentliche Auswirkungen auf den Datenschutz oder die Sicherheit personenbezogener Daten haben könnten, die von oder im Namen von NEP verarbeitet werden, sollten Sie eine Datenschutz-Folgenabschätzung **(„Privacy Impact Assessment – PIA“**) durchführen. Bitte wenden Sie sich an die regionalen Datenschutzbeauftragten. Dies kann auch notwendig sein, wenn Sie eine bestimmte Funktion oder Dienstleistung auslagern oder im Rahmen einer größeren Beschaffung.

15. Schulungen

Alle Schulungen über den Schutz und den Umgang mit personenbezogenen Daten, zu denen NEP Sie auffordert, sind von Ihnen zu besuchen. Dazu können auch Kurse außerhalb des Hauses und E-Learning-Kurse gehören.

16. Datenschutz und Disziplinarmaßnahmen

Verstößt eine Person gegen einen Aspekt dieser Richtlinie (oder wird sie verdächtigt, gegen sie verstoßen zu haben), können gemäß der entsprechenden Disziplinarverfahrensanweisung geeignete Disziplinarmaßnahmen ergriffen werden.

Je nach Schwere des Verstoßes kann eine Disziplinarmaßnahme zur fristlosen Entlassung führen.

NEP behält sich außerdem das Recht vor, gegen eine Person andere Maßnahmen zu ergreifen, die unter den gegebenen Umständen angemessen sind (wie zum Beispiel den Entzug der Zugriffsberechtigung für personenbezogene Daten).

Wenn Sie unsicher sind, ob eine Verarbeitung personenbezogener Daten geboten und rechtmäßig ist, sollten Sie sich vor der Verarbeitung an Ihren regionalen Datenschutzbeauftragten wenden.

17. Änderungen an dieser Datenschutzrichtlinie

Diese Richtlinie wird regelmäßig von der Rechtsabteilung des Konzerns überprüft. Sie werden über die Website von NEP über alle wesentlichen Änderungen der Richtlinie informiert.

Die Genehmigung zur Einführung dieser Richtlinie wurde erteilt von:

Chief Executive Officer	03.03.2023 | 10.06 Uhr PST Datum
Chief Legal Officer	03.03.2023 | 10.08 Uhr PST Datum