| | |
|---|---|
| Titel der Richtlinie: | **Datenschutzrichtlinie** |
| Verantwortlicher der Richtlinie: | **General Counsel und SVP, Personalwesen** |
| Abteilung: | **Rechtsabteilung und Personalwesen** |
| Umgesetzt am: | **24. Mai 2018** |
| Datum der Überarbeitung: | |
| Nächster Prüfungstermin: | **24. Mai 2019** |

# DATENSCHUTZRICHTLINIE: ALLGEMEINE REGEL

Die Mitarbeiter der NEP Group („NEP“ oder das „Unternehmen“) sind für den Schutz der NEP-Unternehmensinformationen und der Mitarbeiterinformationen verantwortlich – unabhängig vom jeweiligen Medium.

**Nähere Einzelheiten und weitere Informationen entnehmen Sie bitte dem Inhalt dieser Richtlinie.**

## INHALTSVERZEICHNIS:

## ERKLÄRENDER HINWEIS UND STATUS DIESER RICHTLINIE

Die NEP Group, Inc. und ihre Tochtergesellschaften werden in dieser Richtlinie bezeichnet als „**NEP**“/ das/die „**Unternehmen**“ / „**wir**“/ „**uns**“/ „**unser**“. Die NEP muss bestimmte Informationen über Personen sammeln und verarbeiten, um seine Geschäfte effektiv zu führen. Diese Informationen stammen unter anderem von aktuellen, ehemaligen und zukünftigen Mitarbeitern, Arbeitern, Bewerbern, Kunden, Akkreditierten, Lieferanten und anderen Personen, mit denen NEP kommuniziert und Geschäfte macht.

Dabei sind wir diesen Personen gegenüber jedoch dafür verantwortlich, dass wir ihre Informationen sorgfältig und unter Einhaltung der Datenschutzgesetze („**Datenschutzgesetze**“) verwenden. Unsere Marken- und Organisationswerte erfordern, dass wir verantwortungsvolle Data Governance-Verfahren anwenden und einhalten, einschließlich derjenigen, die in dieser Datenschutzrichtlinie („**Richtlinie**“) dargelegt sind.

Diese Richtlinie legt (in Teil A) dar, wie NEP die Daten ihrer Mitarbeiter verwenden wird, und es werden (in Teil B) einige der wichtigsten Maßnahmen beschrieben, von denen NEP erwartet, dass diese von den Mitarbeitern des Unternehmens umgesetzt werden, wenn es um die Datenverarbeitungsaktivitäten von NEP geht. Diese Richtlinie legt unsere Regeln zum Datenschutz und die Bedingungen fest, die in Bezug auf die Beschaffung, Handhabung, Verarbeitung, Speicherung, den Transport und die Vernichtung personenbezogener Daten erfüllt werden müssen.

Vorbehaltlich des geltenden Rechts gilt diese Richtlinie für alle NEP-Mitarbeiter (Vollzeit- und Teilzeitkräfte), Zeitarbeiter, Auftragnehmer, Freiwillige, Praktikanten, Besucher, Verkäufer und andere Dritte.

Für NEP-Standorte, an denen das geltende Recht spezifische Richtlinien und/oder Verfahren anstelle oder zusätzlich zu dieser Richtlinie vorschreibt, können länderspezifische Ergänzungen zu dieser Richtlinie hinzugefügt werden.

## TEIL A – DIE VERANTWORTUNG VON NEPIHNEN GEGENÜBER IM RAHMEN DER DATENSCHUTZGESETZE

### 1. Das Datenschutzteam

NEP hat ein Team von Datenschutzbeauftragten ernannt, das NEP bei der Erfüllung seiner Verpflichtungen gemäß den Datenschutzgesetzen unterstützt. Die Schlüsselrolle der Datenschutzbeauftragten besteht aus folgenden Aufgaben:

- Eine Anlaufstelle und Unterstützung für die Mitarbeiter zu bieten;
- Durchführung und Unterstützung bei der Durchführung von Datenschutzfolgenabschätzungen;
- Die Schulung der Mitarbeiter;
- Die Zusammenarbeit mit der lokalen Datenschutzbehörde;
- Die Bearbeitung von Anträgen auf Zugang zu Informationen; und

Wenn Sie diese Richtlinie gelesen haben oder zu irgendeinem Zeitpunkt Fragen zum Umgang mit personenbezogenen Daten haben, wenden Sie sich bitte an Ihren örtlichen Datenschutzbeauftragten.

Ihren Datenschutzbeauftragten finden Sie bei der Rechtsabteilung, der Personalabteilung oder der IT-Abteilung.

## 2. Geltungsbereich der Datenschutzgesetze

Die Datenschutzgesetze regeln die Art und Weise, in der NEP Informationen, die lebende Personen identifizieren oder betreffen (personenbezogene Daten), verarbeiten darf und geben diesen Personen auch bestimmte Rechte und Rechtsmittel in Bezug auf diese Informationen. Die Gesetze regeln außerdem Marketingaktivitäten und den Einsatz von Online-Tracking-Technologien wie Cookies. Sie umfassen daher ein sehr breites Spektrum von Aktivitäten, die NEP (und seine Partner und Lieferanten im Auftrag von NEP) durchführen.

Die Gesetze schreiben einen höheren Sorgfaltsstandard in Bezug auf die Verwendung von „**Sensiblen Personenbezogenen Daten**“ vor, die Informationen über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, sexuelle Orientierung, genetische und biometrische Daten und, für die Zwecke dieser Richtlinie, strafrechtliche Verurteilungen und Straftaten umfassen. In dieser Richtlinie umfasst die Bezugnahme auf „**Personenbezogene Daten**“ Aktivitäten, die mit allen Arten von Informationen über Personen, einschließlich Sensibler Personenbezogener Daten, durchgeführt werden.

Datenschutzgesetze reglementieren Informationen, die von oder im Auftrag von NEP elektronisch oder in bestimmten Situationen als Teil bestimmter Arten von gut strukturierten manuellen Ablagesystemen gespeichert werden. Filmmaterial von Überwachungskameras und Audioaufnahmen sind ebenfalls abgedeckt.

## 3. **Die Art der Informationen, die NEP von seinem Personal** aufbewahren darf

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

- Namen, Adressen, Telefonnummern und andere persönliche Kontaktdaten;
- Geschlecht, Geburtsdatum, Sozialversicherungsnummer / nationale Identifikationsnummer, Immigrationsstatus, Familienstand, nächste Angehörige;
- Personalakten einschließlich Schulungen, Beurteilungen, Fotos, Leistungs- und Disziplinarinformationen, Informationen zu Behinderungen, Lebensläufe und Nachfolgeplanung;
- Bankverbindung, Gehalt, Bonus, Leistungen und Pensionsangaben;
- Filmmaterial von Überwachungskameras und Anrufaufzeichnungen;
- Reisehistorie, Kopien von Reisepässen, Kopien von Führerscheinen, Passwortkennungen und Informationen zur Visumsberechtigung.

- Sensible personenbezogene Daten wie Informationen über die rassische oder ethnische Herkunft, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, genetische und biometrische Daten und strafrechtliche Verurteilungen oder Straftaten.

## 4. Die Art und Weise, in der NEP personenbezogene Daten verarbeiten darf

Personenbezogene Daten dürfen nur für einen legitimen Zweck verarbeitet werden. NEP wird eine Reihe von Maßnahmen mit den personenbezogenen Daten eines Mitarbeiters durchführen, einschließlich, aber nicht beschränkt auf:

- Gehalts-, Vorsorge- und Pensionsverwaltung;
- Verwaltung der Gesundheits- und Sicherheitsunterlagen;
- Strafregisterprüfungen, Bonitätsprüfungen und Freigaben (wo zutreffend);
- Bestätigung von Informationen in Lebensläufen und Bewerbungsschreiben, Bereitstellung von Referenzschreiben und Durchführung von Referenzprüfungen;
- Schulung und Beurteilung, einschließlich Leistungsbewertung und disziplinarische Aufzeichnungen;
- Personalverwaltung und Beförderungen;
- Nachfolgeplanung;
- Überwachung der Chancengleichheit;
- jede mögliche Änderung der Kontrolle über eine Konzerngesellschaft oder jede mögliche Versetzung im Zusammenhang mit einer Unternehmensübertragung oder einem Wechsel des Dienstleisters (in Europa gemäß der Richtlinie über erworbene Rechte). Unter diesen Umständen dürfen personenbezogene Daten dem potenziellen Käufer oder Investor und seinen Beratern nur im Rahmen des geltenden Rechts mitgeteilt werden;
- sonstige Angaben, die im Zusammenhang mit der Einstellung und Beförderung von Mitarbeitern oder der Vermarktung von NEP, seiner Produkte oder Dienstleistungen erforderlich sind;
- Bereitstellung von Personalinformationen für Kunden und Agenturen im Rahmen der Erbringung der Dienstleistungen von NEP;
- Aufzeichnungen durch Überwachungskameras aus Sicherheitsgründen;
- Betrieb einer Ethik- oder Whistleblowing-Hotline, die NEP jetzt oder in Zukunft betreiben kann;
- Einhaltung der geltenden Verfahren, Gesetze und Vorschriften, einschließlich aller damit zusammenhängenden Untersuchungen, um die Einhaltung der Vorschriften bei möglichen Verstößen sicherzustellen;
- Begründung, Ausübung oder Verteidigung der gesetzlichen Rechte von NEP;

- Alle anderen angemessenen Zwecke im Zusammenhang mit der Beschäftigung oder Beauftragung einer Person durch NEP;
- Bereitstellung und Verwaltung der Nutzung von Diensten Dritter, wie z. B. Reiseveranstalter oder Unternehmen, die Mobiltelefone, Firmenkreditkarten und Firmenfahrzeuge zur Verfügung gestellt haben, und Abrechnung dieser Dienste.

NEP kann auch personenbezogene Daten über Ihre nächsten Angehörigen sammeln und verarbeiten, damit diese im 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.

Um diese Zwecke zu erfüllen, behält sich NEP das Recht vor, nach eigenem Ermessen personenbezogene Daten (oder gegebenenfalls sensible personenbezogene Daten) an Strafverfolgungsbehörden, Regulierungsbehörden, Regierungsbehörden und andere Dritte weiterzugeben, soweit dies gesetzlich vorgeschrieben oder für Verwaltungszwecke erforderlich ist.

NEP kann personenbezogene Daten insbesondere für die oben genannten Zwecke an Auftragnehmer und Lieferanten weitergeben, die Dienstleistungen für NEP erbringen und die bei den oben genannten Verarbeitungstätigkeiten behilflich sein können. In einem solchen Fall ist NEP zusätzlich verpflichtet, mit den Auftragnehmern und Lieferanten, denen NEP personenbezogene Daten zur Verfügung stellt, einen Datenverarbeitungsvertrag abzuschließen.

NEP kann personenbezogene Daten an andere Konzerngesellschaften, Partner, Lieferanten, Strafverfolgungsbehörden und andere Organisationen außerhalb des Europäischen Wirtschaftsraums („**EWR**“) weitergeben (für diese Zwecke definiert, um das Vereinigte Königreich einzubeziehen), für folgende Zwecke:

- Personalverwaltung (z. B. Personalbeschaffung);
- Gehaltsabrechnung für Mitarbeiter außerhalb des EWR;
- Personalverlagerung;
- Visaanträge;
- Besteuerung und Registrierung von Mitarbeitern, die außerhalb des EWR tätig sind;
- Erfüllung der gesetzlichen Anforderungen von NEP;
- Erfüllung von Kundenverträgen zur Erbringung der Leistungen durch NEP;
- Gerichtsverfahren im Ausland; und
- Outsourcing von NEP-Funktionen.
- Akkreditierungen und Reisevisa.

Zu diesen Ländern können unter anderem die Länder gehören, in denen NEP tätig ist, sowie der Standort unserer Lieferanten und deren Rechenzentren, wie z. B. Microsoft (USA), zusammen mit anderen größeren Anbietern von Personalverwaltungs-Software.

Bitte beachten Sie, dass die Gesetze einiger Jurisdiktionen außerhalb des EWR möglicherweise nicht so strikt sind wie die Datenschutzgesetze, die im EWR gelten.

## 5. Aufbewahrung von Unterlagen

Die NEP ist gesetzlich verpflichtet, bestimmte Aufzeichnungen für einen Mindestzeitraum aufzubewahren. Die NEP darf personenbezogene Daten nicht länger aufbewahren, als dies erforderlich ist oder nach geltendem Recht vorgeschrieben ist.

## 6. Überwachung

Überwachung der NEP-Systeme

Die IT- und Kommunikationssysteme von NEP sollen eine effektive Kommunikation und Arbeitsweise innerhalb unserer Organisation fördern.

Aus geschäftlichen Gründen und zur Aufrechterhaltung der IT-Sicherheitsmaßnahmen wird die Nutzung der Systeme von NEP auf einer entsprechenden Plattform einschließlich der Telefon- (mobil und Festnetz) und Computersysteme (einschließlich E-Mail und Internetzugang) sowie deren persönliche Nutzung überwacht. Wenn Sie mit Hilfe von Passwörtern und Login-Namen auf den IT- und Kommunikationssystemen von NEP auf Dienste zugreifen, kann dies bedeuten, dass Ihre persönlichen Zugangsdaten von NEP eingesehen werden.

Eine Überwachung erfolgt nur, wenn und soweit dies gesetzlich zulässig oder erforderlich und für geschäftliche Zwecke notwendig und vertretbar ist. Dies ist erforderlich, damit Missbrauchsversuche und andere sicherheitsrelevante Ereignisse erkannt werden können und Informationen zur Verfügung stehen, die eine spätere Untersuchung und Weiterverfolgung unterstützen. Soweit gesetzlich zulässig und bei Verstößen gegen diese Richtlinie können Maßnahmen im Rahmen des Disziplinarverfahrens ergriffen werden.

NEP behält sich das Recht vor, den Inhalt von Nachrichten abzurufen, im Internet durchgeführte Recherchen zu überprüfen, die sofortige Rückgabe der von NEP bereitgestellten Geräte zu verlangen und auf diesen Geräten gespeicherte Zugangsdaten für folgende Zwecke zu verwenden (diese Liste ist nicht vollständig):

- zu überwachen, ob die Nutzung des E-Mail-Systems oder des Internets rechtmäßig und in Übereinstimmung mit dieser Richtlinie erfolgt (und die Mitarbeiter sind sich darüber bewusst, dass NEP Software verwenden kann, um die Identität von Absendern und Empfängern von E-Mails zu überwachen);
- um verlorene Nachrichten wiederzufinden oder um Nachrichten abzurufen, die aufgrund eines Computerausfalls verloren gegangen sind;
- um bei der Untersuchung unrechtmäßiger Handlungen, einschließlich solcher, die gegen unsere anderen Richtlinien oder geltendes Recht verstoßen, behilflich zu sein; und
- um jeglichen gesetzlichen Verpflichtungen nachzukommen.

Voraussetzung für die Nutzung unserer IT-Systeme ist, dass Sie sich professionell verhalten, den guten Namen des Unternehmens nicht in Verruf bringen und sich nicht unangemessen gegenüber Ihren Kollegen und anderen Personen verhalten, mit denen Sie während Ihrer Tätigkeit für NEP in Kontakt treten. Wird ein Verstoß gegen diese Bedingungen oder ein Missbrauch der IT-Systeme von NEP festgestellt, kann NEP gemäß den Disziplinarverfahren von NEP eine eingehendere Untersuchung durchführen, die die Prüfung und Weitergabe von Überwachungsaufzeichnungen an die für die Durchführung der Untersuchung benannten Personen sowie an alle am Disziplinarverfahren beteiligten Zeugen oder Führungskräfte umfasst. Dasselbe gilt, wenn NEP einen begründeten Verdacht hat, dass illegale Aktivitäten oder Handlungen stattgefunden haben, die gegen unsere anderen Richtlinien und Verfahren verstoßen würden.

Wenn nötig, können solche Informationen der Polizei oder einer anderen Strafverfolgungsbehörde übergeben werden. Ermittlungen und die Weitergabe von Informationen an die zuständigen Behörden erfolgen nur im gesetzlich zulässigen Umfang.

Überwachungskameras (CCTV)

Einige Gebäude und Standorte der NEP nutzen aus Sicherheitsgründen CCTV-Systeme zur Überwachung ihrer Außen- und Innenräume rund um die Uhr. Diese Daten werden aufgezeichnet. Die Verwendung von CCTV und die Aufzeichnung von CCTV-Daten erfolgt nur in Übereinstimmung mit den von NEP genehmigten Richtlinien.

## 7. Ihre Rechte an den Daten

Nach den Datenschutzgesetzen können Mitarbeiter von NEP berechtigt sein, eine Kopie ihrer persönlichen Daten anzufordern, diese zu korrigieren, zu löschen oder einzuschränken oder die NEP aufzufordern, einige dieser Daten an andere Organisationen weiterzugeben. Die Mitarbeiter können auch das Recht haben, der Verarbeitung ihrer persönlichen Daten zu widersprechen und, wenn NEP um ihre Zustimmung zur Verarbeitung der Daten gebeten hat, diese Zustimmung zu widerrufen. Diese Rechte können in einigen Situationen eingeschränkt sein – zum Beispiel, wenn NEP nachweist, dass das Unternehmen gesetzlich verpflichtet ist, Ihre Daten zu verarbeiten. In einigen Fällen kann dies bedeuten, dass die Daten auch dann gespeichert werden können, wenn der Mitarbeiter seine Zustimmung zurückzieht.

Wenn NEP personenbezogene Daten zur Erfüllung gesetzlicher oder vertraglicher Verpflichtungen benötigt, ist die Bereitstellung dieser Daten zwingend erforderlich: Wenn diese Daten nicht zur Verfügung gestellt werden, ist NEP nicht in der Lage, das Arbeitsverhältnis zu verwalten oder die uns auferlegten Verpflichtungen zu erfüllen. In allen anderen Fällen ist die Angabe der angeforderten personenbezogenen Daten freiwillig.

Bei Fragen zur Verarbeitung personenbezogener Daten durch NEP wenden Sie sich bitte an das Datenschutzteam.

### 8. Beschwerden

Jeder einzelne Mitarbeiter, der glaubt, dass eine andere Person seine Datenschutzrechte verletzt haben könnte, wird von uns ermutigt, dies seinem Vorgesetzten oder einer anderen Person, die im Rahmen des Beschwerdeverfahrens der Geschäftseinheit bzw. des örtlichen Beschwerdeverfahrens angegeben ist, mitzuteilen.

Mitarbeiter mit ungeklärten Bedenken haben auch das Recht, sich direkt an die Datenschutzbehörden zu wenden. Die zuständige Datenschutzbehörde ist die Aufsichtsbehörde des Landes, in dem das Unternehmen ansässig ist, bei dem Sie beschäftigt sind.

## TEIL B – Ihre datenschutzrechtlichen Verpflichtungen gegenüber Dritten

Dieser Teil der Richtlinie soll die Mitarbeiter darüber informieren, wie sie unter bestimmten Umständen mit personenbezogenen Daten umgehen sollten. Jeder Mitarbeiter ist zur Einhaltung der Datenschutzgesetze verpflichtet. Es ist wichtig, dass jeder Einzelne sich seiner eigenen Datenschutzverantwortung gegenüber anderen im Rahmen der Datenschutzgesetze bewusst ist, wozu auch die Einhaltung der nachstehenden Richtlinien und Verfahren gehört. Hier sind einige wichtige Punkte, die zu beachten sind:

- Berücksichtigen Sie Ihre Verantwortlichkeiten im Rahmen der Datenschutzgesetze und dieser Richtlinie und wie sie sich auf Ihre täglichen Aktivitäten auswirken.
- Geben Sie personenbezogene Daten (oder kommerziell sensible Daten) nur dann weiter, wenn es jeweils erforderlich ist. Geben Sie nicht eine ganze Datenbank frei, wenn nur ein Teil davon benötigt wird.
- Überprüfen Sie die Daten des Empfängers ganz genau, bevor Sie Daten weitergeben. Versenden Sie Daten bestimmungsgemäß oder gefährden Sie das Unternehmen?
- Verwenden Sie Passwortschutz für Dokumente und Dateien, wann immer möglich.
- Verwenden Sie personenbezogene Daten nur in der Weise, wie die betroffene Person zugestimmt hat oder wie in dieser Richtlinie dargelegt.
- Entscheiden Sie nach dem gesunden Menschenverstand, wie personenbezogene Daten geschützt, verwendet und entsorgt werden sollten. Denken Sie darüber nach, wie Ihre eigenen personenbezogenen Daten behandelt werden sollten.

Dieser Abschnitt ist als allgemeiner Leitfaden gedacht und stellt keine umfassende oder erschöpfende Anleitung dar. Abhängig von der genauen Art Ihrer Tätigkeit haben Sie möglicherweise zusätzliche Pflichten gegenüber anderen im Rahmen der Datenschutzgesetze.

Ihre allgemeinen Verantwortlichkeiten sind wie folgt:

### 9. Grundsätze des Datenschutzes

Bei der Verarbeitung personenbezogener Daten muss NEP und müssen sämtliche Mitarbeiter des Unternehmens bestimmte Datenschutzgrundsätze innerhalb der Datenschutzgesetze beachten. Dazu gehört, dass personenbezogene Daten:

- korrekt und rechtmäßig verarbeitet werden müssen;

- nur für einen oder mehrere bestimmte und rechtmäßige Zwecke verarbeitet werden und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden, es sei denn, dies ist nach geltendem Recht ausdrücklich gestattet;
- in Bezug auf die Zwecke, für die sie verarbeitet werden, angemessen und relevant sein müssen und nicht übertrieben sein dürfen;
- genau sein und, wo nötig, auf dem neuesten Stand gehalten werden müssen;
- nicht länger aufbewahrt werden dürfen, als es für die Zwecke, für die sie verarbeitet wurden, erforderlich ist;
- in Übereinstimmung mit den Rechten einer Person verarbeitet werden, einschließlich des Rechts, unter bestimmten Umständen folgendes zu verlangen: Zugang zu personenbezogenen Daten, deren Portierung auf einen Dritten, deren Löschung, wenn sie unrichtig oder nicht mehr erforderlich sind, und die nicht Gegenstand wesentlicher automatisierter Entscheidungsprozesse sind;
- sicher aufbewahrt werden; und
- nur dann in ein Land oder Gebiet außerhalb des EWR übertragen werden dürfen oder von dort aus darauf zugegriffen werden darf, wenn dieses Land oder Gebiet ein angemessenes Schutzniveau für die Rechte und Freiheiten von Personen in Bezug auf die Verarbeitung personenbezogener Daten gewährleistet oder wenn angemessene vertragliche Garantien zum Schutz der Daten vorhanden sind.

## 10. Daten sicher aufbewahren

Die Bestimmungen dieses Abschnitts und des Abschnitts 11 (Meldung vermuteter Datenschutzverletzungen) beziehen sich nicht nur auf personenbezogene Daten, sondern auf alle Informations-, IT- und Kommunikationssysteme, für deren Sicherheit Sie in Bezug auf die Ihnen zugewiesenen oder von Ihnen verwendeten Geräte verantwortlich sind, und Sie dürfen nicht zulassen, dass diese von anderen Personen als in Übereinstimmung mit dieser Richtlinie verwendet werden.

Computer-/Laptop-Sicherheit:

- Alle IT-Benutzer erhalten eindeutige Kontodaten. Sie dürfen weder Konten noch Passwörter mit anderen Benutzern teilen. Sie dürfen keine Konten verwenden, die Ihnen nicht zugeordnet sind, oder Ihre Kontodaten an andere weitergeben.
- Sie müssen Ihren Computer oder Laptop oder Ihr Handheld-Gerät immer dann sperren, abmelden oder herunterfahren, wenn Sie das Gerät unbeaufsichtigt lassen (z. B. bei Meetings oder in der Mittagspause). Die IT-Systeme von NEP sind so konzipiert, dass sie nach einer bestimmten Zeit der Inaktivität automatisch gesperrt oder abgeschaltet werden.
- Am Ende eines jeden Arbeitstages müssen Sie sicherstellen, dass Ihr Computer ordnungsgemäß heruntergefahren und Ihr Monitor ausgeschaltet ist. Wenn Sie einen Laptop haben, müssen Sie ihn sicher aufbewahren, zum Beispiel in einem verschlossenen Schrank oder einer Schublade.
- Stellen Sie sicher, dass vertrauliche Geschäftsinformationen, die auf einem Bildschirm angezeigt werden, nicht einfach von außerhalb unserer Räumlichkeiten eingesehen werden können.

- Sie müssen ein starkes Passwort verwenden (z. B. eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen) und dieses Passwort geheim halten. Sie sollten es regelmäßig ändern und wenn Sie glauben, dass jemand Ihr Passwort kennt, müssen Sie es sofort ändern.
- Änderungen oder Wartungsarbeiten an Ihrem Computer oder Ihrer IT-Ausrüstung oder die Installation von Hardware oder Software auf NEP-unterstützten Anlagen dürfen nur mit ausdrücklicher Genehmigung des Information Services-Teams von NEP, seinen Mitarbeitern oder autorisierten Personen durchgeführt werden.

Zugriff auf elektronisch gespeicherte Daten:

- Verwenden Sie Passwörter, um den Zugriff auf sensible Dateien zu beschränken.
- Umgehen Sie keine festgelegten Sicherheitsgruppierungen oder Berechtigungsstufen.
- Erhalten Sie einen Prüfpfad aufrecht für Änderungen an Datenbanken oder Dokumenten, die sensible Informationen enthalten.
- Verhindern Sie keine geplanten IT-Backup-Prozesse.

Sicherheit tragbarer Geräte:

- Wenn Sie Zugang zu NEP-gestützten IT-Systemen oder -Infrastrukturen erhalten haben, sind Sie verantwortlich für deren Sicherheit und dafür, dass diese nicht von Unbefugten benutzt werden, verloren gehen, gestohlen oder beschädigt werden, insbesondere auf Reisen oder wenn Sie sich außerhalb des Büros aufhalten.
- Tragbare Geräte dürfen zu keinem Zeitpunkt, insbesondere nicht über Nacht, in Fahrzeugen verbleiben. Wenn dies unvermeidlich sein sollte, dann müssen Sie darauf achten, dass die Geräte außer Sichtweite bleiben.
- Wenn Sie tragbare Geräte z. B. in öffentlichen Verkehrsmitteln oder an einem öffentlichen Ort wie einem Hotel-Foyer benutzen, müssen Sie sicherstellen, dass der Bildschirm nicht von anderen Personen gelesen werden kann, und Sie sollten entsprechende Vorsichtsmaßnahmen treffen.
- Wenn Sie Ihr tragbares Gerät in einem externen oder fremden Netzwerk, z. B. in einem Hotel oder Flughafen, verwenden, müssen Sie angemessene Maßnahmen ergreifen, um sicherzustellen, dass das Netzwerk sicher ist, z. B. durch die Verwendung eines Netzwerks, das von einem seriösen Unternehmen bereitgestellt wird und das vorzugsweise gesperrt und nicht uneingeschränkt verfügbar ist. Wenn Sie Zweifel an der Sicherheit des Netzwerks haben, dürfen Sie Ihr Gerät nicht damit verbinden.
- Sie dürfen nicht versuchen, eine Verschlüsselungssoftware oder Sicherheitsfunktionen auf den tragbaren Geräten zu umgehen.
- NEP verwendet eine Kombination der folgenden Sicherheitsfunktionen auf tragbaren Geräten, um deren Sicherheit zu gewährleisten:

- Benutzernamen/Passwörter und PIN-Nummern;
- Antivirenschutz;
- Datenverschlüsselung;
- Kontosperre nach fehlgeschlagenen Zugriffsversuchen;
- Geräte-/Anwendungssperre nach Inaktivität;
- Konto- oder Gerätesperre bei Diebstahl/Verlust;
- Überwachung der Nutzung; und
- Löschen von Inhalten auf verlorenen oder gestohlenen Geräten.

Sicherheit von Papierkopien personenbezogener Daten vor Ort:

- Halten Sie Ihren Schreibtisch frei von persönlichen Daten und vertraulichen Geschäftsinformationen.
- Lassen Sie personenbezogene Daten oder geschäftskritische vertrauliche Informationen zu keinem Zeitpunkt unbeaufsichtigt auf dem Schreibtisch liegen.
- Wenn Sie sensible personenbezogene Daten oder vertrauliche Geschäftsinformationen ausdrucken, stellen Sie sicher, dass Sie sich beim Drucker aufhalten, um zu verhindern, dass die Ausdrucke von jemand anderem entnommen werden.
- Lassen Sie keine personenbezogenen Daten oder geschäftskritische vertrauliche Informationen in Besprechungsräumen oder anderen Bereichen des Büros zurück, nehmen Sie sie mit und entsorgen Sie sie sicher, wenn Sie sie nicht mehr benötigen. Wischen Sie Whiteboards vor dem Verlassen von Besprechungsräumen ab, es sei denn, Sie wurden ausdrücklich darauf hingewiesen, dies nicht zu tun.
- Bewahren Sie personenbezogene Daten und vertrauliche Geschäftsinformationen über Nacht an einem sicheren Ort auf, z. B. in einem abschließbaren Aktenschrank, einer Schublade oder in einem geschützten Bereich/Raum.
- Befolgen Sie alle spezifischen Anweisungen in Bezug auf Ihren Standort oder Ihre Abteilung.

Sicherheit von Papierkopien personenbezogener Daten außerhalb des Standorts:

- Nehmen Sie personenbezogene Daten oder geschäftskritische vertrauliche Informationen nur dann außerhalb des Büros oder außerhalb des Standorts mit, wenn dies unbedingt erforderlich ist.
- Seien Sie sich der Risiken von Verlust oder Diebstahl bewusst und treffen Sie geeignete Vorsichtsmaßnahmen, um sicherzustellen, dass personenbezogene Daten oder vertrauliche Geschäftsinformationen sicher aufbewahrt werden.

- Lassen Sie keine personenbezogenen Daten oder geschäftssensible vertrauliche Informationen in Zügen oder anderen öffentlichen Verkehrsmitteln oder an anderen öffentlichen Orten unbeaufsichtigt. Stellen Sie sicher, dass geschäftskritische Informationen nicht einfach eingesehen werden können, wenn Sie sich an einem öffentlichen Ort befinden.
- Speichern oder archivieren Sie personenbezogene Daten oder geschäftskritische vertrauliche Informationen nur bei einem von NEP zugelassenen Anbieter, mit dem ein schriftlicher Vertrag besteht.

Einsatz von mobilen Speichermedien:

Tragbare/entfernbare Medien („**Medien**“) umfassen alle tragbaren Geräte, die in der Lage sind, Daten zu speichern, zu übertragen, zu manipulieren oder zu entfernen und umfassen (sind aber nicht darauf beschränkt) mobile Geräte, Flash-Discs/Stifte, Wechselfestplatten und optische Medien (CDs, DVDs usw.).

- Daten dürfen nur dann von den IT-Systemen von NEP an andere Medien übertragen werden, wenn eine echte geschäftliche Rechtfertigung vorliegt und die Bestimmungen dieser Richtlinie und die Anweisungen des Information Services-Teams befolgt werden.
- NEP überwacht alle aus dem Netzwerk kopierten Daten, um unberechtigte Datenübertragungen zu erkennen und Sicherheitsverletzungen zu verhindern.
- Der Datenaustausch, egal ob intern oder mit externen Parteien, muss immer über NEP-Informationssysteme wie E-Mails oder gemeinsam genutzte Datenbereiche erfolgen. Medien für die Datenübertragung dürfen nur verwendet werden, wenn alle anderen Optionen ausgeschöpft sind.
- Alle Medien, die physisch zwischen NEP und/oder einem Kunden übertragen werden, sollten per Spezialzustellung versendet werden (um sicherzustellen, dass die Medien nachverfolgt und bei Verlust wiederhergestellt werden können).

- Beachten Sie vor der Verwendung von Medien:
    - Sie dürfen nur Medien verwenden, die über NEP Information Services erworben oder von diesem Team autorisiert und verschlüsselt wurden;
    - Die Medien müssen nachverfolgbar sein, um die Ankunft am Bestimmungsort zu gewährleisten;
    - Medien müssen vor der Verwendung mit Hilfe von Virenscanner-Software, die vom NEP-Information Services-Team zur Verfügung gestellt wird, auf Malware/Vireninfektionen überprüft werden und dürfen nicht verwendet werden, wenn eine potenzielle Infektion festgestellt wird;
    - Speichern Sie nur Daten, die unbedingt erforderlich sind, d. h. laden Sie nicht die gesamte Datenbank herunter, wenn nur kleine Teile davon benötigt werden;
    - Überprüfen Sie, ob das mobile Speichermedium die persönlichen Daten verschlüsseln kann;

- Stellen Sie sicher, dass die auf dem Medium gespeicherten Dateien passwortgeschützt sind und das Passwort separat an das verschlüsselte Medium gesendet wird;
- Löschen Sie Daten sofort von den Medien, wenn sie nicht mehr benötigt werden; und
- Nicht wiederverwendbare Medien sind am Ende ihres erforderlichen Lebenszyklus gemäß den Empfehlungen des Information Services-Teams ordnungsgemäß zu entsorgen/zerstören.

Einschränkungen bei der Nutzung nicht zugelassener Geräte oder Software:

- Sie dürfen keine unlizenzierte Software, Software von Dritten, frei verfügbare Software oder ähnliche Software auf Ihren Computer oder andere IT-Geräte herunterladen, da sie Viren oder sonstige schädliche Codes enthalten kann, der die Sicherheit der Systeme von NEP beeinträchtigen könnte.

Zugriff durch Dritte:

- NEP ist für die Handlungen und Unterlassungen ihrer Lieferanten und Auftragnehmer verantwortlich, die im Namen des Unternehmens auf personenbezogene Daten zugreifen oder diese verarbeiten dürfen. Wenn Sie Auftragnehmer, Berater und Zeitarbeiter beauftragen, die Zugang zu den Systemen und/oder persönlichen Daten von NEP haben, müssen diese zunächst eine Vereinbarung unterzeichnen, die Bestimmungen enthält, die die personenbezogenen Daten von NEP angemessen schützen, z. B. eine Vertraulichkeits- und Sicherheitsvereinbarung. Wenden Sie sich an Ihren Datenschutzbeauftragten, um sich über die erforderlichen Bestimmungen zu informieren.
- Insbesondere erfordert jedes Projekt, das die Anbindung eines Dritten/Lieferanten an die Systeme von NEP beinhaltet, eine spezifische Bewertung der Risiken und zusätzliche Vertragsbedingungen in Bezug auf die Sicherheit.
- Alle Änderungen am Zugriff durch Dritte/Auftragnehmer auf das Netzwerk von NEP müssen überprüft und dokumentiert werden, um die Aufrechterhaltung der Sicherheit zu gewährleisten.
- Wird der Zugang eines Dritten/Auftragnehmers nicht mehr benötigt, muss die Verbindung beendet und die vom Dritten/Auftragnehmer erhaltenen personenbezogenen Daten gemäß den Vertragsbedingungen zurückgegeben oder vernichtet werden.
- Alle Drittanbieter und Auftragnehmer müssen NEP über ihren Hauptansprechpartner über alle Vorfälle im Bereich der Informationssicherheit informieren, die sie selbst oder ihre Kunden erleiden.

Sicherung von personenbezogenen Daten:

- Nach Möglichkeit sollten die Daten in einem vernetzten Speicher abgelegt werden, da diese leicht durch automatisierte Prozesse gesichert werden können. Wechselmedien wie USB-Sticks und CDs sollten nicht zum Speichern geschäftskritischer Informationen verwendet werden, da sie nicht gesichert werden und daher bei Verlust, Beschädigung oder versehentlichem Löschen nicht wiederhergestellt werden können.

Vernichtung personenbezogener Daten:

Personenbezogene Daten in Papierform sollten nach Möglichkeit über getrennte sichere Abfallbehälter oder über Aktenvernichter entsorgt werden.

- Vergewissern Sie sich, dass jegliche IT-Hardware, mobile Geräte, mobile Speichermedien oder andere Geräte vor der Entsorgung ordnungsgemäß von allen personenbezogenen Daten bereinigt wurden. Nicht wiederverwendbare Medien wie CD-ROMs müssen am Ende ihres Lebenszyklus ordnungsgemäß entsorgt oder vernichtet werden. Wenden Sie sich an das Team von Information Services, um sicherzustellen, dass dies korrekt durchgeführt wird.

E-Mail- und Systemnutzung:

- Sie dürfen nicht versuchen, Virenschutzsoftware zu umgehen, indem Sie sie beispielsweise deaktivieren.
- Mitarbeiter sollten vorsichtig sein, wenn sie E-Mails aus unbekannten externen Quellen öffnen oder wenn eine E-Mail aus irgendeinem Grund verdächtig erscheint (z. B. wenn der Name eines Anhangs mit .exe endet).
- Das Team von Information Services sollte unverzüglich informiert werden, wenn ein vermuteter Virus erhalten oder identifiziert wird.
- NEP behält sich das Recht vor, den Zugriff auf E-Mails-Anhänge zum Zwecke der effektiven Nutzung der IT-Systeme von NEP und zur Einhaltung dieser Richtlinie zu sperren.
- NEP behält sich außerdem das Recht vor, keine (ein- oder ausgehende) E-Mail-Nachricht zu versenden, wenn der Verdacht besteht, dass ein Virus angehängt wurde.
- NEP erlaubt die gelegentliche Nutzung von Internet-, E-Mail- und Telefonsystemen, um persönliche E-Mails zu versenden, im Internet zu surfen und persönliche Telefonate unter bestimmten Bedingungen zu führen. Der persönliche Gebrauch ist ein Privileg und kein Recht. Dieses Privileg darf weder missbraucht noch überstrapaziert werden und die NEP behält sich das Recht vor, die Genehmigung jederzeit zu widerrufen. NEP behält sich das Recht vor, den Zugang zu bestimmten Telefonnummern oder Internetseiten einzuschränken oder zu unterbinden, wenn der persönliche Gebrauch als übertrieben betrachtet wird. Die folgenden Bedingungen müssen erfüllt sein, damit der persönliche Gebrauch fortgesetzt werden kann:
    - Die Nutzung muss minimal sein und im Wesentlichen außerhalb der normalen Arbeitszeiten erfolgen;
    - Die Nutzung darf die geschäftlichen oder bürotechnischen Verpflichtungen nicht beeinträchtigen; und
    - Die Nutzung darf für NEP keine Grenzkosten verursachen.
- Der gesamte E-Mail-Verkehr im Zusammenhang mit Geschäftsaktivitäten muss über ein zugelassenes Firmen-E-Mail-System abgewickelt werden.

Kundenkontaktdaten:

- Sie dürfen keine Adressbücher oder irgendwelche anderen Dokumente oder Geräte mit Geschäftskontakten unbeaufsichtigt lassen.
- Wenn Sie Geschäftskontakte elektronisch speichern, müssen Sie diese in einem sicheren Bereich im NEP-Netzwerk speichern.

## 11. Meldung vermuteter Datensicherheitsverletzungen

Eine Verletzung der Datensicherheit kann im Zusammenhang mit oder als Folge eines der folgenden Ereignisse auftreten (diese Liste ist nicht vollständig):

- Diebstahl von Daten (einschließlich physischer Kopien) oder Geräten (Laptops, Handys, Speichersticks, CD-ROMs usw.), auf denen Daten gespeichert sind;
- Unkenntnis des Anwenders / mangelnde Schulung;
- Unerlaubter Zugriff/Kopieren;
- Falsche Sicherheitsklassifizierung/Markierung/Etikettierung;
- Ungesicherter Übertragungsmodus;
- Verwendung unkontrollierter oder nicht autorisierter Medien;
- Verlust oder möglicher Verlust von Medien, Geräten oder Ausrüstung;
- Verlust oder möglicher Verlust von Sicherungsmedien;
- Unzulässige Aufbewahrung von Informationen;
- Falschadressierung / Fehlleitung personenbezogener Daten;
- Falsche Methode zur Entsorgung von Daten oder Medien;
- Hacking/Abfangen;
- Abhören/Spionage;
- Unangemessene Freigabe zur öffentlichen Nutzung;
- Zugang durch unbeaufsichtigte Instandhalter/Auftragnehmer;
- Unangemessene Zugangskontrollen, die eine unbefugte Nutzung durch Mitarbeiter oder andere Personen ermöglichen; oder
- Informationen, die durch eine Täuschung von NEP erhalten wurden.

Wenn Sie von einer Verletzung der Sicherheit personenbezogener Daten (oder einer sonstigen Gefährdung der Datensicherheit) erfahren oder den Verdacht haben, dass die Datensicherheit gefährdet ist, müssen Sie dies unverzüglich Ihrem Datenschutzbeauftragten und Ihrem Vorgesetzten melden, damit die zuständige Datenschutzbehörde und die von der Verletzung der Datensicherheit betroffene Person benachrichtigt werden können. Es liegt in Ihrer Verantwortung, sicherzustellen, dass diese Meldung ankommt und dass der Datenschutzbeauftragte und Ihr Vorgesetzter sich darüber bewusst sind, dass diese Meldung gesendet wurde (das Senden einer E-Mail oder das Hinterlassen einer

Sprachnachricht kann unzureichend sein, wenn Sie nicht sicher sein können, dass der Empfänger die Nachricht gelesen bzw. abgehört hat – das müssen Sie immer überprüfen).

Sie sollten versuchen, so viele Informationen wie möglich zur Verfügung zu stellen (einschließlich, aber nicht beschränkt auf die folgenden Informationen):

- Um welche Art von Daten handelt es sich (sensibel oder nicht)?
- Wann ist der Sicherheitsverstoß passiert?
- Wie ist der Verstoß erfolgt (z. B. durch Diebstahl oder durch den Verlust von Daten oder bei Verdacht auf unberechtigten Zugriff);
- Wenn die Daten beschädigt oder verfälscht wurden, in welcher Weise wurden sie beschädigt oder verfälscht?
- Wie viele personenbezogene Daten (von wie vielen Personen) sind von dem Verstoß betroffen?
- Wer sind die Personen, deren Daten verloren gegangen sind (d. h. sind es Mitarbeiter, Kunden, Auftraggeber oder Lieferanten)?
- Maßnahmen, die ergriffen wurden oder ergriffen werden müssen, um weitere Probleme zu vermeiden, unabhängig davon, ob es sich bei dem Verstoß um eine Wiederholung handelt oder ob weitere Daten betroffen sind; und
- Alle bekannten vertraglichen Verpflichtungen gegenüber Dritten bezüglich der Sicherheit der persönlichen Daten (z. B. gegenüber Kunden von NEP).

Sie sollten anschließend dabei helfen, die Verletzung der Datensicherheit zu stoppen oder zu mindern.

### 12. **Stellen Sie sicher, dass Personen wissen, wie ihre Daten von NEP** verwendet werden

Unter bestimmten Umständen ist die ausdrückliche Zustimmung von Personen erforderlich. NEP verfügt über Standard-Datenschutzerklärungen und -klauseln, die in die Standardverträge aufgenommen werden, um sicherzustellen, dass diese Anforderung erfüllt wird, und um denjenigen, die wissen müssen, wann eine ausdrückliche Zustimmung eingeholt werden sollte, einen Leitfaden zur Verfügung zu stellen.

### 13. **Stellen Sie sicher, dass Ihre personenbezogenen Daten korrekt und auf dem neuesten Stand sind.**

Eventuelle Ungenauigkeiten in den personenbezogenen Daten müssen von den Mitarbeitern in allen relevanten Systemen von NEP korrigiert werden. Jede Aktualisierung oder Änderung von Informationen, die von einer Person zu einem beliebigen Zeitpunkt mitgeteilt wird, muss auch in den Aufzeichnungen von NEP vorgenommen werden.

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

## 14. Sichere Entsorgung personenbezogener Daten

Wenn personenbezogene Daten nicht mehr benötigt werden, müssen Sie sicherstellen, dass diese sorgfältig und sicher entsorgt werden.

Wenn ein Mitarbeiter ein Auskunftsersuchen unter Bezugnahme auf ein Datenschutzgesetz erhält, wenden Sie sich bitte umgehend an Ihren Datenschutzbeauftragten, um sicherzustellen, dass diese Anfrage innerhalb der vorgeschriebenen Fristen ordnungsgemäß bearbeitet wird.

## 15. Bewertung der Auswirkungen auf die Privatsphäre

Wenn Sie neue Prozesse, Richtlinien oder Verfahren einführen, ein neues Projekt starten oder neue Systeme kaufen, die die Handhabung oder Übertragung großer Mengen personenbezogener Daten beinhalten oder die einen wesentlichen Einfluss auf die Privatsphäre oder die Sicherheit der von oder im Auftrag von NEP verarbeiteten personenbezogenen Daten haben könnten, dann sollten Sie eine Datenschutzfolgenabschätzung (Privacy Impact Assessment; kurz: „**PIA**“) durchführen. Bitte beachten Sie die PIA-Richtlinien von NEP. Dies kann auch der Fall sein, wenn Sie eine bestimmte Funktion oder Dienstleistung auslagern oder im Rahmen einer wesentlichen Beschaffung.

## 16. Schulung

Sie müssen an allen Kursen zum Schutz und zur Verarbeitung personenbezogener Daten teilnehmen, zu denen Sie von NEP aufgefordert werden. Dazu können auch Kurse außerhalb des Unternehmens und E-Learning-Kurse gehören.

## 17. Externe Beratung durch Ihre lokale Datenschutzbehörde

Auf der Website des European Data Protection Board, der britischen ICO und anderer Datenschutzbehörden finden Sie eine Reihe nützlicher Hinweise.

## 18. Datenschutz und Disziplinarmaßnahmen

Verstößt eine Person gegen diese Richtlinie (oder wird vermutet, dass sie gegen die Richtlinie verstoßen hat), können entsprechende Disziplinarmaßnahmen in Übereinstimmung mit dem entsprechenden Disziplinarverfahren ergriffen werden.

Je nach Schwere des Vergehens können Disziplinarmaßnahmen zu einer fristlosen Kündigung führen.

NEP behält sich auch das Recht vor, andere Maßnahmen gegen eine Person zu ergreifen, die nicht entlassen wurde (einschließlich der Aufhebung des Rechts auf autorisierten Zugriff auf personenbezogene Daten), soweit dies unter den gegebenen Umständen angemessen ist.

Wenn eine Person Zweifel hat, ob sie personenbezogene Daten korrekt und rechtmäßig verarbeitet, sollte sie sich vor der Verarbeitung an das Datenschutzteam wenden.

### 19. Überwachung und Überprüfung dieser Richtlinie

Diese Richtlinie wird regelmäßig überprüft. Über wesentliche Änderungen der Richtlinie werden Sie über die Website von NEP informiert.

## GENEHMIGUNG

Die Genehmigung zur Einführung dieser Richtlinie wurde erteilt von:

_____ _____
Chief Executive Officer Datum

_____ _____
Justitiar und Chief Compliance Officer Datum

_____ _____
Senior Vice President of Human Resources Datum

## Revisionsverlauf

| **Datum** | **Revisionszusammenfassung** (Beginn mit Abschnittsnummer/Titel) |
|---|---|
| 1. Mai 2018 | Inkrafttreten der Richtlinie |
| | |
| | |
| | |