CHNP Centre Hospitalier Neuro-Psychiatrique	**Allgemeine Richtlinie zum Schutz personenbezogener Daten**	*CHNP-Direktion*
Freigabe durch das Direktionskomitee / Inkrafttreten	04.07.2019	Pol/2019/01 – Version 1.6

Inhaltsverzeichnis

1. Einleitung ... 2
- a. Vorwort ... 2
- b. Begriffsbestimmungen ... 3
- c. Ziel ... 4
- d. Rechtlicher und normativer Rahmen ... 5
- e. Anwendungsbereich ... 5
- f. Sanktionen und Risiken ... 6

2. Interne Verwaltung und Kontrolle – Funktionen und Zuständigkeiten ... 6
- a. Das CHNP als Verantwortlicher ... 6
- b. Direktionskomitee ... 7
- c. Datenschutzbeauftragter (DPO) ... 7
- d. Chief Information Security Officer (CISO) ... 9
- e. Abteilungs-/Bereichsleiter ... 10

3. Modalitäten für die Verarbeitung personenbezogener Daten beim CHNP ... 10
- a. Grundsätze für die Verarbeitung personenbezogener Daten ... 10
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz ... 10
  - Minimierung und Richtigkeit der personenbezogenen Daten ... 11
  - Begrenzung der Zwecke der Verarbeitung ... 11
  - Begrenzung der Speicherfrist ... 13
  - Vertraulichkeit/Sicherheit personenbezogener Daten ... 13
- b. Übermittlung personenbezogener Daten durch das CHNP ... 14
  - 1. Empfänger personenbezogener Daten ... 14
  - 2. Grenzüberschreitende Übermittlung personenbezogener Daten ... 15
- c. Verletzung des Schutzes personenbezogener Daten ... 15

4. Rechte der betroffenen Personen ... 16
- a. Modalitäten für die Ausübung der Rechte betroffener Personen ... 16
- b. Beschwerdemanagement ... 17

5. Cookie-Richtlinie ... 17

Bezugsdokumente ... 18

1. Einleitung

a. Vorwort

Als öffentliche Einrichtung des privaten Rechts stellt das Centre Hospitalier Neuro-Psychiatrique (im Folgenden „CHNP“) den Menschen in den Mittelpunkt und ist dabei stets um höchste Qualität bemüht.

Vor diesem Hintergrund ist das CHNP in besonderer Weise der Achtung der Privatsphäre und dem Schutz personenbezogener Daten verpflichtet. Diese Achtung dient der Vertrauensbildung und ist ein Wert, der dem CHNP besonders wichtig ist.

Das CHNP legt damit höchsten Wert auf:

- die Sicherheit der Informationssysteme, d. h. Gewährleistung der Verfügbarkeit, Vertraulichkeit und Vollständigkeit aller Informationsbestände und personenbezogenen Daten, die im Rahmen seiner öffentlich-rechtlichen Aufgaben gesammelt und verarbeitet werden

- den Schutz von IT-, Netzwerk-, Telekommunikations- (Festnetz- und Mobilfunk), Verarbeitungs- und Speicherressourcen für Informationsbestände und deren Nutzung im Rahmen seiner Leistungen

- die Einhaltung der gesetzlichen Verpflichtungen zum Schutz personenbezogener Daten und zur Sicherheit der Informationssysteme

Das CHNP muss umfangreiche personenbezogene Daten, darunter Gesundheitsdaten, erheben, übermitteln oder austauschen sowie ganz allgemein verarbeiten. Da Gesundheitsdaten im Sinne der geltenden europäischen und luxemburgischen Rechtsvorschriften als sensibel eingestuft werden können, sind diese verstärkt zu schützen, soweit ihre Offenlegung oder ihr Missbrauch die Rechte und Freiheiten der betroffenen Personen sowie die Achtung ihrer Privatsphäre beeinträchtigen kann.

Der Schutz personenbezogener Daten und die Aufrechterhaltung der Sicherheit der Informationssysteme verlangen, dass alle Beteiligten ihre diesbezüglichen Rechte, Verantwortlichkeiten und Verpflichtungen bei der Ausübung der Aufgaben des CHNP kennen.

Dieses Referenzdokument beschreibt den organisatorischen, rechtlichen und methodologischen Rahmen für den Schutz personenbezogener Daten innerhalb des CHNP, damit die Einhaltung der geltenden Vorschriften sichergestellt ist.

Für die Sicherheit der Informationssysteme wurde eine separate Richtlinie erstellt, die Informationssicherheitsrichtlinie. Sie ist in einzelne Richtlinien gegliedert, in denen die wichtigsten, in der Grundrichtlinie festgelegten Sicherheitsprinzipien beschrieben und ausführlich dargestellt werden.

b. Begriffsbestimmungen

Falls sich aus dem Zusammenhang nicht etwas anderes ergibt, sind die nachstehenden Ausdrücke und Begriffe für die Zwecke dieser Richtlinie wie folgt zu verstehen:

„Auftragsverarbeiter“ bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Namen des Verantwortlichen verarbeitet;

„Betroffene Person“ bezeichnet jede natürliche Person, deren personenbezogene Daten das CHNP verarbeitet;

„CHNP“ bezeichnet das Centre Hospitalier Neuro-Psychiatrique;

„CNPD“ bezeichnet die Nationale Kommission für den Datenschutz oder die zuständige Kontrollstelle im Großherzogtum Luxemburg;

„DSGVO“ bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG;

„Empfänger“ bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, und dies unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. (Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung);

„Informationsbestände“ bezeichnet Ressourcen, die Informationen beinhalten (Papierdokumente, elektronische Dateien, Datenbanken, Anwendungen, E-Mails, Hardware usw.);

„Informationssysteme“ bezeichnet alle technischen und personellen Mittel mit dem Ziel der Erhebung, Organisation, Verarbeitung, Speicherung, Verbreitung und Kommunikation von Informationen;

„Mitarbeiter“ bezeichnet das gesamte Personal des CHNP (sowohl Angestellte als auch Beamte), Mitarbeiter externer Dienstleister (reguläre Auftragsverarbeiter), die an den Standorten des CHNP tätig sind, oder jede andere Person, die ständig oder zeitweilig Zugriff auf die Informationsbestände und/oder Informationssysteme des CHNP hat;

„Personenbezogene Daten“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche 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;

„Sicherheit der Informationssysteme“ bezeichnet die Tätigkeit zum Schutz der Informationssysteme vor Zugriff, Benutzung, Offenlegung, Unterbrechung, Änderung, Verlust oder Zerstörung, welche nicht zulässig sind;

„Verantwortlicher“ bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

„Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten oder Datensätzen wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

„Verletzung des Schutzes personenbezogener Daten“ bezeichnet eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

c. Ziel

Das Ziel dieser Richtlinie besteht zunächst darin, die vom CHNP eingegangenen Verpflichtungen und die im Rahmen seiner täglichen Aktivitäten durchgeführten Maßnahmen zur Förderung eines verantwortungsvollen Umgangs mit personenbezogenen Daten in Übereinstimmung mit den geltenden Vorschriften zu beschreiben, auch um betroffene Personen darüber zu informieren.

Diese Richtlinie beschreibt durch allgemeine Erläuterungen die durch das CHNP vorgenommene Verarbeitung und die Rechte, über die die betroffenen Personen im Zusammenhang mit dieser Verarbeitung verfügen. Diese Richtlinie soll jedoch nicht alle Informationen detailliert auflisten, über die die betroffenen Personen zu unterrichten sind. Eine ausführlichere Dokumentation dieser Verarbeitung kann den entsprechenden Informationsbroschüren[1] entnommen werden.

Diese Richtlinie enthält ferner die innerhalb des CHNP geltenden Vorschriften zum Schutz personenbezogener Daten, um Risiken zu minimieren, und dient gleichzeitig den Mitarbeitern als Orientierung bei der Wahrnehmung ihrer Aufgaben. Das Ziel dieser Richtlinie besteht darin,

- für das CHNP Grundsätze und Regeln zur Verwaltung personenbezogener Daten zu formulieren und zu verbreiten, damit diese kommuniziert werden und für alle zugänglich und verständlich sind;

[1] Informationsbroschüre für Bewerber, Informationsbroschüre für das Personal, Informationsbroschüre für Patienten/Bewohner, Informationsbroschüre für Dienstleister.

- jeden Einzelnen zu verantwortungsbewusstem Handeln im Umgang mit und beim Schutz von innerhalb des CHNP verwendeten Informationsbeständen, einschließlich derjenigen, die personenbezogene Daten enthalten, zu veranlassen.

d. Rechtlicher und normativer Rahmen

In dieser Richtlinie sind die allgemeinen Regeln festgelegt, die für den Schutz personenbezogener Daten gelten.

Diese Grundsätze beruhen auf folgenden Rechtsvorschriften:

- DSGVO, anwendbar seit dem 25. Mai 2018;

- Luxemburgisches Gesetz vom 1. August 2018 betreffend die Organisation der nationalen Datenschutzkommission und die Anwendung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Es wird darauf hingewiesen, dass sich der für den Schutz der Informationsbestände geltende Rahmen, einschließlich derjenigen, die personenbezogene Daten enthalten, regelmäßig ändert. Das CHNP verpflichtet sich, die geltenden Vorschriften anzuwenden und die rechtliche Überwachung künftiger Entwicklungen sicherzustellen.

e. Anwendungsbereich

Diese Richtlinie gilt für alle Einrichtungen und Abteilungen des CHNP, für alle Mitarbeiter des CHNP sowie für die gesamte Verarbeitung personenbezogener Daten, die das CHNP durchführt, unabhängig davon, ob sie sich, ohne Anspruch auf Vollständigkeit, auf folgende betroffene Personen bezieht:

- ❖ Patienten/Bewohner, ihre gesetzlichen Vertreter und/oder ggf. ihre Ansprechpartner;
- ❖ Mitarbeiter, ungeachtet ihres Status (Festangestellte oder Angestellte mit befristeten Verträgen, Beamte, Praktikanten, Aushilfen, subventionierte Beschäftigte usw.);
- ❖ Bewerber beim CHNP;
- ❖ externe Angehörige von Gesundheitsberufen;
- ❖ Dienstleister, Lieferanten, Partner oder andere Organisationen, die mit dem CHNP in Kontakt stehen.

Für den Schutz personenbezogener Daten innerhalb des CHNP sowie die Einhaltung dieser Richtlinie und der entsprechenden Verfahren sind grundsätzlich alle Mitarbeiter verantwortlich.

Die unerlaubte oder zweckwidrige Verwendung personenbezogener Daten durch einen Mitarbeiter, einschließlich des Versuchs, Sicherheitsmaßnahmen zu umgehen, oder illegaler Aktivitäten, kann Disziplinarmaßnahmen gemäß den geltenden Richtlinien und Verfahren unterliegen.

f. Sanktionen und Risiken

Ein Verstoß gegen die DSGVO kann zu Geldbußen von bis zu 20 Millionen Euro oder 4 % des weltweiten Gesamtjahresumsatzes des Vorjahres führen, wobei der höhere der beiden Werte anzuwenden ist.

Neben den hohen Geldbußen, die erhebliche Auswirkungen auf die Tätigkeiten des CHNP haben könnten, kann die Verletzung der geltenden Vorschriften zum Schutz personenbezogener Daten ein Reputationsrisiko für das CHNP bzw. einen Imageverlust mit sich bringen.

Zudem ist zu beachten, dass ein Verstoß gegen die DSGVO auch aufgrund anderer gesetzlicher Vorschriften bestraft werden kann, wie beispielsweise eine strafrechtlich zu ahndende Verletzung des Berufsgeheimnisses. Der Urheber einer solchen Zuwiderhandlung könnte daher zusätzlich zu den unter Punkt 1.e genannten Disziplinarstrafen nach den geltenden Rechtsvorschriften strafrechtlich verfolgt werden.

Ferner könnten Ansprüche auf finanziellen Ausgleich infolge möglicher Zivilklagen der betroffenen Personen geltend gemacht werden.

2. Interne Verwaltung und Kontrolle – Funktionen und Zuständigkeiten

Um einen wirksamen Schutz personenbezogener Daten innerhalb des CHNP zu gewährleisten, wurde eine Organisation geschaffen, die sich mit dem Schutz der Informationsbestände und mit der Sicherheit der Informationssysteme in Übereinstimmung mit den geltenden Rechts- und Verwaltungsvorschriften befasst.

Diese Organisation basiert insbesondere auf der Ernennung eines Datenschutzbeauftragten (DPO) und eines Chief Information Security Officer (CISO).

a. Das CHNP als Verantwortlicher

Im Zuge der Ausübung seiner Aufgaben ist das CHNP Verantwortlicher für die gesamte, in seinen Abteilungen durchgeführte Verarbeitung personenbezogener Daten.

Das CHNP bestimmt die Zwecke der Verarbeitung personenbezogener Daten (therapeutische Betreuung, Verwaltung, Rechnungstellung, Einstellung von Personal usw.) und die Maßnahmen zu deren Umsetzung (welche personenbezogenen Daten werden verarbeitet, wie und von wem). Es stellt sicher, dass die Zwecke rechtmäßig sind und während der Verarbeitungszeit gemäß den geltenden Vorschriften beachtet werden.

Die Verarbeitung personenbezogener Daten durch das CHNP wird unter Punkt 3.a der Richtlinie sowie in den unter Punkt 1.c genannten Informationsbroschüren eingehender analysiert.

b. Direktionskomitee

Das Direktionskomitee des CHNP ist bei der Verarbeitung personenbezogener Daten für die Einhaltung der geltenden gesetzlichen Verpflichtungen, insbesondere im Hinblick auf die DSGVO, verantwortlich.

Zum Schutz personenbezogener Daten ergreift das Direktionskomitee unterschiedliche geeignete Maßnahmen:

- Aufbau einer Ablauforganisation gemäß den Empfehlungen der zuständigen Behörden;
- Umsetzung eines Konzepts zur Festschreibung gemäß den geltenden Vorschriften;
- Einführung geeigneter technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten und für die Sicherheit der Informationssysteme in Übereinstimmung mit der bestehenden Praxis;
- Umsetzung von Sensibilisierungsmaßnahmen für alle Mitarbeiter hinsichtlich des Schutzes personenbezogener Daten und der Sicherheit der Informationssysteme.

Das Direktionskomitee muss über die Maßnahmen entscheiden, die als Reaktion auf ein im Zuge einer Datenschutz-Folgenabschätzung ermitteltes Risiko zu ergreifen sind.

Ebenso stellt das Direktionskomitee sicher, dass der DPO oder der CISO bei der Durchführung eines Projekts oder der Analyse einer neuen Verarbeitung über die potenziellen Risiken einer Verarbeitung personenbezogener Daten unterrichtet und dazu konsultiert wird.

c. Datenschutzbeauftragter (DPO)

Das CHNP hat, wie in Artikel 37, Absatz 1 der DSGVO für Behörden und öffentliche Stellen vorgeschrieben, einen Datenschutzbeauftragten benannt.

Der DPO ist dafür verantwortlich, unabhängig Maßnahmen zu koordinieren, um die Verarbeitung personenbezogener Daten mit den geltenden Rechtsvorschriften zum Schutz personenbezogener Daten, insbesondere der DSGVO, in Einklang zu bringen.

Der DPO unterstützt das Direktionskomitee des CHNP bei der Umsetzung der verschiedenen Maßnahmen und Verfahren zum Schutz personenbezogener Daten. Er führt das Verzeichnis über die durch das CHNP durchgeführte Verarbeitung personenbezogener Daten.

Für die Erfüllung seiner Aufgabe berichtet der DPO der Verwaltungs- und Finanzdirektion des CHNP direkt und verfügt über die Handlungsfreiheit und die Mittel, die es ihm ermöglichen, geeignete organisatorische oder technische Lösungen zu empfehlen. Er erfüllt seine Aufgaben in vollem Umfang völlig unabhängig und objektiv.

Der DPO hat folgende wesentliche Aufgaben:

- Förderung einer Kultur des Schutzes personenbezogener Daten innerhalb des CHNP, insbesondere durch Sensibilisierung, Information und Schulung der Mitarbeiter mit Unterstützung durch die Geschäftsleitung;
- Unterrichtung und Beratung des CHNP sowie der Mitarbeiter über ihre Verpflichtungen nach den geltenden Rechtsvorschriften zum Schutz personenbezogener Daten, einschließlich der DSGVO, und Unterbreitung von Empfehlungen an sie;
- Überwachung der Einhaltung der geltenden Vorschriften zum Schutz personenbezogener Daten, einschließlich der DSGVO und der internen Regeln des CHNP zum Schutz personenbezogener Daten;
- Sammeln von Informationen zur Erfassung von Verarbeitungsvorgängen;
- Erstellen und Führen der Dokumentation, die für die Einhaltung des Grundsatzes der Rechenschaftspflicht erforderlich ist, einschließlich der Führung eines Verzeichnisses über die innerhalb des CHNP durchgeführten Verarbeitungsvorgänge;
- Analyse und Überprüfung der Konformität der Verarbeitung des CHNP oder Bewertung der Risiken im Zusammenhang mit den erfassten Verarbeitungsvorgängen und Beratung über Abhilfemaßnahmen;
- Im Rahmen von Privacy by Design auf Anfrage Analyse und Stellungnahme bezüglich der künftigen/geplanten Verarbeitung, um die Einhaltung der geltenden Vorschriften und aller damit verbundenen Tätigkeiten und Maßnahmen sicherzustellen (Auswirkungen auf das Leben der betroffenen Personen und Niveau der notwendigen Sicherheitsmaßnahmen);
- Auf Anfrage Beratung hinsichtlich der Datenschutz-Folgenabschätzung „DSFA“ oder „PIA“ (Notwendigkeit einer solchen Analyse, anzuwendende Verfahren, anzuwendende Maßnahmen zur Abwendung potenzieller Risiken) sowie Überprüfung ihrer Durchführung;
- Zusammenarbeit mit den wichtigsten internen Ansprechpartnern (zum Beispiel Direktionskomitee, gemischter Betriebsrat, IT, HR, Kommunikation, interne Dienste und CISO);
- Beteiligung bei der Erstellung und Umsetzung von Richtlinien, Leitlinien, Verfahren, Informationsbroschüren und sonstigen Unterlagen zum effizienten Schutz personenbezogener Daten und des Privatlebens der betroffenen Personen;
- Bewertung von Sicherheitsmaßnahmen in enger Zusammenarbeit mit dem CISO und dem Leiter der IT-Abteilung;
- Unabhängige Steuerung oder Organisation von Audits oder Kontrollen zur Überprüfung der Einhaltung des rechtlichen Rahmens oder der korrekten Anwendung der Verfahren und Bestimmungen zum Schutz personenbezogener Daten oder Erbringung von Nachweisen einer mangelnden Konformität;
- Gegebenenfalls Unterrichtung der CNPD über Datenschutz-Verletzungen, sobald diese dem DPO bekannt geworden sind, und dies unter den rechtlich geltenden Bedingungen sowie Beratung des CHNP über mögliche relevante Mitteilungen und Maßnahmen, die in Zusammenarbeit mit dem CISO und dem Leiter der IT-Abteilung zu ergreifen sind;
- Ausübung der Funktion einer Anlaufstelle für die CNPD und betroffene Personen bei Fragen zu der innerhalb des CHNP durchgeführten Verarbeitung;
- Sicherstellung der ordnungsgemäßen Bearbeitung von Anträgen zur Geltendmachung von Ansprüchen der betroffenen Personen und deren Übermittlung an die entsprechenden Stellen.

Der DPO ist an Werktagen wie folgt zu erreichen:

CHNP
17, avenue des Alliés
BP 111
L-9002 Ettelbrück

Tel.: +352 2682-2667

E-Mail: DPO@chnp.lu

Im Rahmen seiner Aufgaben ist der DPO an das Berufsgeheimnis gebunden.

d. Chief Information Security Officer (CISO)

Der Chief Information Security Officer ist verantwortlich für die Einrichtung einer geeigneten Verwaltung und Kontrolle der Sicherheit der Informationssysteme.

In dieser Eigenschaft definiert und formuliert der CISO angemessene und ausreichende funktionale und technische Regeln, damit die Sicherheit der Informationsbestände des CHNP, einschließlich der personenbezogenen Daten, über ihre gesamte Nutzungsdauer hinweg gewahrt ist. Des Weiteren muss er die Übereinstimmung dieser Maßnahmen mit den geltenden Vorschriften sicherstellen.

Der CISO unterstützt das Direktionskomitee des CHNP bei der Umsetzung der verschiedenen Maßnahmen und Verfahren, die für die Einrichtung einer geeigneten Verwaltung und Kontrolle der Sicherheit der Informationssysteme erforderlich sind.

Für die Erfüllung seiner Aufgabe berichtet der CISO der Verwaltungs- und Finanzdirektion des CHNP direkt und verfügt über die Handlungsfreiheit und die Mittel, die es ihm ermöglichen, geeignete organisatorische oder technische Lösungen zu empfehlen. Er erfüllt seine Aufgaben in vollem Umfang völlig unabhängig und objektiv.

Der CISO hat folgende wesentliche Aufgaben:

- Entwicklung einer effizienten Strategie zur Identifizierung und Bewertung der Risiken im Zusammenhang mit der Verwendung der Informationssysteme und Ausarbeitung eines Plans zur Reduzierung dieser Risiken;
- Aufrechterhaltung der Sicherheitsrichtlinien und Sicherstellung ihrer Umsetzung;
- Sicherstellung der Relevanz und Wirksamkeit der von den zuständigen Behörden auferlegten und/oder sich aus den geltenden Vorschriften ergebenden immateriellen Maßnahmen zum Schutz personenbezogener Daten (Passwort, Virenschutz, Filtern gefährlicher oder gesetzlich verbotener Seiten usw.);
- Beteiligung am Verfahren zur Bewältigung potenzieller Krisen und Sicherheitsvorfälle;
- Beteiligung an der Kontrolle der Einhaltung der geltenden Richtlinien über die Sicherheit von Informationssystemen.

Der Chief Information Security Officer (CISO) arbeitet bei der Definition von Sicherheitsstandards eng mit dem DPO und dem Leiter der IT-Abteilung zusammen und überwacht die ordnungsgemäße Anwendung dieser Standards in den Informationssystemen des CHNP.

Im Rahmen seiner Aufgaben ist der CISO an das Berufsgeheimnis gebunden.

e. Abteilungs-/Bereichsleiter

Die Abteilungs- und Bereichsleiter müssen sicherstellen, dass diese Richtlinie sowie die zugehörigen Regeln und Verfahren den Mitgliedern ihrer Teams bekannt sind und von diesen verstanden und eingehalten werden und dass diese Mitarbeiter regelmäßig an den vom DPO angebotenen Schulungen zum Schutz personenbezogener Daten teilnehmen.

Die Abteilungs- und Bereichsleiter unterstützen den DPO auch bei der Führung des Verzeichnisses über die Verarbeitungsvorgänge und beteiligen sich an der Umsetzung der Datenschutz-Folgenabschätzung, die bei jedem neuen und in ihren Verantwortungsbereich fallenden Projekt zur Verarbeitung personenbezogener Daten erforderlich wird.

Die Abteilungs- und Bereichsleiter stellen sicher, dass eine Verletzung des Schutzes personenbezogener Daten, die ihnen bekannt ist, unverzüglich gemäß dem Meldeverfahren für die Verletzung des Schutzes personenbezogener Daten von ihnen selbst oder durch ihre Mitarbeiter gemeldet wird. Die Abteilungs- und Bereichsleiter beteiligen sich im Übrigen an Audits durch den DPO und/oder den CISO und übermitteln alle in diesem Zusammenhang angeforderten Informationen auf transparente Weise.

3. Modalitäten für die Verarbeitung personenbezogener Daten beim CHNP

In seiner Funktion als Verantwortlicher ist das CHNP verantwortlich für die Erhebung, Verarbeitung und Speicherung der personenbezogenen Daten durch seine Abteilungen und Mitarbeiter.

Demnach verpflichtet sich das CHNP, personenbezogene Daten in Übereinstimmung mit den geltenden Vorschriften zu erheben und zu verarbeiten und die wichtigsten Grundsätze einzuhalten, die einer Verarbeitung personenbezogener Daten gemäß Artikel 5 der DSGVO zugrunde liegen.

a. Grundsätze für die Verarbeitung personenbezogener Daten

- #### Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Die vom CHNP durchgeführte Verarbeitung personenbezogener Daten ist rechtmäßig und beruht auf einer oder mehreren Legitimitätsgrundlagen, wie der Einhaltung einer gesetzlichen Verpflichtung, der Erfüllung eines Vertrages (Wohnen, Pflege usw.), den lebenswichtigen Interessen der betroffenen Person, ihrer ausdrücklichen Zustimmung oder dem berechtigten Interesse des CHNP. Wenn die Verarbeitung auf der Grundlage der Einwilligung der betroffenen Person erfolgt, so hat diese die Möglichkeit, ihre Einwilligung jederzeit zu widerrufen.

Im Übrigen erfolgt durch das CHNP keine Erhebung ohne das Wissen der betroffenen Personen oder ohne dass diese darüber unterrichtet wurden. Das CHNP verpflichtet sich damit, die Unterrichtung der betroffenen Person über die Verarbeitung ihrer personenbezogenen Daten zu gewährleisten.

- Minimierung und Richtigkeit der personenbezogenen Daten

Das CHNP stellt sicher, dass die erhobenen personenbezogenen Daten im Hinblick auf das mit der Erhebung verfolgte Ziel und für die Zwecke der Verarbeitung absolut notwendig, relevant und nicht übermäßig sind. Das CHNP ist bestrebt, den Umfang der erhobenen personenbezogenen Daten zu minimieren und sie korrekt und auf dem neuesten Stand zu halten, indem es die Wahrnehmung der Rechte der betroffenen Personen erleichtert.

Das CHNP trifft alle nach vernünftigem Ermessen notwendigen Maßnahmen, um fehlerhafte personenbezogene Daten schnellstmöglich zu löschen oder zu korrigieren.

- Begrenzung der Zwecke der Verarbeitung

Personenbezogene Daten werden durch das CHNP für spezifische Ziele sowie bestimmte, ausdrückliche Zwecke erhoben, die den betroffenen Personen in transparenter Form zur Kenntnis gebracht werden. Diese personenbezogenen Daten dürfen in der Folge nicht in einer Weise verwendet werden, die mit diesen Zwecken unvereinbar ist. Demnach verpflichtet sich das CHNP, die erhobenen personenbezogenen Daten nicht für andere Zwecke zu verwenden als diejenigen, die der betreffenden Person mitgeteilt wurden.

➢ *Verarbeitung personenbezogener Daten von Patienten/Bewohnern*

1) Das CHNP ist verpflichtet, personenbezogene Daten seiner Patienten/Bewohner im Rahmen seiner Tätigkeit als öffentliche Krankenhauseinrichtung zu erheben, zu verarbeiten und zu speichern, und dies insbesondere zu den folgenden wesentlichen Zwecken:

❖ Überprüfung der Identität und Kontaktaufnahme zum Patienten/Bewohner;
❖ Bewertung und Verarbeitung von Aufnahmeanträgen, einschließlich der Organisation vorbereitender Maßnahmen (Vorgespräch, Sozialerhebung, Beziehung zum zukünftigen Patienten/Bewohner usw.);
❖ Gegebenenfalls Erstellung der medizinischen Diagnose;
❖ Verwaltung von Anträgen auf Zuteilung eines freien Platzes sowie das Führen einer Warteliste für noch offene Anträge;
❖ Vorbereitung, Abwicklung und Verwaltung von Pflege-, Unterbringungs- oder Aufnahmeverträgen je nach Gegenstand der Aufnahme;
❖ Patienten-/Bewohnerverwaltung und -erfassung;
❖ Medizinische und therapeutische Betreuung, Pflegemanagement und medizinische Behandlungen;
❖ Führen und Aktualisieren der Patientenakte sowie Aufbewahrung gesundheitsrelevanter Dokumente, gegebenenfalls einschließlich der Beschaffung von Unterlagen zu medizinischen Untersuchungen in Dritteinrichtungen;
❖ Kommunikation mit externen Angehörigen der Gesundheitsberufe (behandelnde Ärzte, Fachärzte, zuständige Sozialarbeiter usw.) zum Zwecke der Kontinuität der Betreuung;
❖ Verwaltung der Verschreibung und Abgabe von Medikamenten;

- Umgang mit Infektionskrankheiten;
- Bewertung, Überwachung sowie soziale und medizinisch-soziale Begleitung des Patienten/Bewohners (Sozialhilfeanträge, Anträge auf Vormundschaft/Pflegschaft, Suche nach einer Unterkunft oder Einrichtung für die Zeit nach einem Krankenhausaufenthalt usw.);
- Pflegebewertung;
- Verwaltung sozio-kultureller Aktivitäten;
- Verwaltung des Patienten-/Bewohnerrufsystems und des Zugangskontrollsystems;
- Rechnungsmanagement;
- Verwaltung und Überwachung der Verpflegung, der Reinigung von Einzel- und Gemeinschaftsräumen sowie der Wäscherei;
- Sicherheit der Patienten/Bewohner insbesondere mittels Videoüberwachungskameras an den Standorten des CHNP;
- Verwaltung der Zimmer und Wohnungen, die bestimmten Patienten im Anschluss an den Krankenhausaufenthalt zur Verfügung gestellt werden;
- Überwachung der Einhaltung interner Richtlinien und Verfahren;
- Beschwerdemanagement;
- Gegebenenfalls und in Ausnahmefällen wissenschaftliche Forschung;
- Einhaltung der gesetzlichen Verpflichtungen, einschließlich Befolgung von Anträgen der Justizbehörden (Pfändungsbeschluss, gerichtliches Gutachten usw.).

Weitere Einzelheiten zur Verarbeitung personenbezogener Daten von Patienten/Bewohnern können den entsprechenden Informationsbroschüren entnommen werden. Diese stehen auf der Internetseite chnp.lu[2] zur Verfügung bzw. sind auf Anfrage in elektronischer Form oder in Papierform beim DPO erhältlich.

2) Das CHNP ist verpflichtet, personenbezogene Daten seiner Mitarbeiter und Bewerber für die im Rahmen von Bewerbungsverfahren üblichen Zwecke sowie für die Personalverwaltung zu erheben, zu verarbeiten und zu speichern, insbesondere jedoch für folgende Zwecke:

- Bewerbungs- und Einstellungsmanagement neuer Mitarbeiter;
- Beurteilung und Bewertung der Fähigkeiten in Bezug auf einen bestehenden und zukünftigen Bedarf innerhalb des CHNP;
- Ausarbeitung und gegebenenfalls Erstellung eines Arbeitsvertrags oder Praktikums-/ Aushilfsvertrags für erfolgreiche Bewerber;
- Bewerberüberprüfung (Identität des Mitarbeiters, Berufserlaubnis usw.);
- Mitteilungen an die Zentralstelle für Sozialversicherungen (CCSS) oder sonstige zuständige Behörden[3];
- Organisation und Planung der Arbeitszeiten;
- Personalmanagement und -verwaltung;
- Karriereplanung, Personalentwicklung, einschließlich Schulungsmanagement;
- Lohnverwaltung und Management der Gehaltsabrechnungen;
- Urlaubsverwaltung und -anzeige[4];
- Abführen von Steuern;
- Gehaltspfändung oder Lohnabtretung aufgrund eines Gerichtsurteils;
- Management und Meldung von Arbeitsunfällen oder sonstigen Schadenereignissen mit Mitarbeiterbeteiligung;

[2] https://www.pontalize.lu/wp-content/uploads/sites/3/2018/08/notice_DP_admission_pontalize_FR.pdf

[3] Staatliche Verwaltung und Gesundheitsministerium für Mitarbeiter mit Beamtenstatus.

[4] Anzeigepflichtig sind zum Beispiel: Mutterschaftsurlaub, Erziehungsurlaub, Arbeitsbefreiung, unbezahlter Urlaub, Überstunden für verbeamtete Mitarbeiter usw.

- Verwaltung und Konfiguration der Computerzugänge und Computerwartung, einschließlich gegebenenfalls der logistischen Organisation (Überlassung von Ausrüstungen – Telefonie, Dienstfahrzeug, Computer-Hardware usw.);
- Organisation der Sozialwahlen;
- Sensibilisierung für und Management der Sicherheit von Personen, Anlagen, Systemen und Ressourcen;
- Social Relationship Management (Einladung der Mitarbeiter zu Veranstaltungen des CHNP, z. B. Jahresmitarbeiterfest);
- Veröffentlichung von Mitarbeiterdaten im internen Verzeichnis „Who's Who" oder auf der Internetseite des CHNP[5];
- Management von Disziplinarverfahren oder gegebenenfalls Entlassungen;
- Gegebenenfalls Behandlung von Beschwerden wegen Mobbings;
- Überwachung der Einhaltung interner Richtlinien und Verfahren sowie Einhaltung gesetzlicher Verpflichtungen.

Weitere Einzelheiten zur Verarbeitung personenbezogener Daten von Mitarbeitern des CHNP können der im Intranet des CHNP[6] verfügbaren Informationsbroschüre entnommen werden. Sie ist auf Anfrage ebenfalls in elektronischer Form oder in Papierform beim DPO erhältlich.

Weitere Einzelheiten zur Verarbeitung personenbezogener Daten von Bewerbern auf eine Stelle beim CHNP können der Informationsbroschüre zur Verarbeitung personenbezogener Daten im Rahmen der Bewerbung entnommen werden. Diese steht auf der Internetseite des CHNP zur Verfügung und ist auf Anfrage in elektronischer Form oder in Papierform beim DPO erhältlich.

- Begrenzung der Speicherfrist

Das CHNP speichert personenbezogene Daten für einen Zeitraum, der nicht länger ist, als es die Zwecke, für die die personenbezogenen Daten erhoben und verarbeitet werden, erfordern. Wie lange die durch das CHNP verarbeiteten Daten gespeichert werden, wird den betroffenen Personen zur Kenntnis gebracht. Die Dauer kann je nach Art der betroffenen Person (Mitarbeiter, Patient, Bewohner, Dienstleister usw.), der Art der personenbezogenen Daten, dem Zweck der Verarbeitung und den gesetzlichen oder behördlichen Anforderungen, in denen die Speicher- und/oder Verjährungsfristen festgelegt sind, variieren.

Das CHNP verpflichtet sich, Verfahren zur Anonymisierung[7] personenbezogener Daten einzurichten, wenn es notwendig ist, bestimmte, diesen personenbezogenen Daten zugeordnete Informationen zu speichern, ohne dass es zwingend erforderlich ist, die Identität der betroffenen Personen, auf die sie sich beziehen, zu speichern.

- Vertraulichkeit/Sicherheit personenbezogener Daten

Das CHNP ergreift alle erforderlichen Maßnahmen, um die Sicherheit und Vertraulichkeit der ihm übermittelten personenbezogenen Daten zu gewährleisten und insbesondere zu verhindern, dass diese ohne Zustimmung der betroffenen Person unrechtmäßig abgerufen, versehentlich verändert, gestohlen, beschädigt oder an unbefugte Dritte weitergegeben werden.

[5] Mit Ausnahme von Fotos, deren Veröffentlichung der Mitarbeiter über ein separates Formular zustimmen muss; http://inside/sites/default/files/SecD/RGPD_FR_2018_05_14.pdf

7 Die „Anonymisierung" ist ein irreversibler Vorgang, bei dem personenbezogene Daten so verändert werden, dass sie einer betroffenen Person nicht mehr zugeordnet werden können (definitiv nicht identifizierbare Daten). Anonymisierte Daten unterliegen nicht mehr der DSGVO und können daher ohne Risiko für andere als die zum Zeitpunkt ihrer Erhebung definierten Zwecke verwendet werden.

Die vom CHNP angewandten notwendigen und geeigneten technischen und organisatorischen Maßnahmen zielen darauf ab, die Vertraulichkeit personenbezogener Daten zu gewährleisten und einen versehentlichen oder unrechtmäßigen Verlust, eine versehentliche oder unrechtmäßige Zerstörung oder Änderung, eine unrechtmäßige Verwendung, eine Offenlegung oder einen Zugriff auf personenbezogene Daten durch unbefugte Dritte zu verhindern.

Das CHNP verlangt zudem von jedem Auftragsverarbeiter angemessene Vorkehrungen für die Sicherheit und Vertraulichkeit personenbezogener Daten und stellt sicher, dass sich die Auftragsverarbeiter durch Aufnahme geeigneter Rechtsbestimmungen in den Verträgen zur Erfüllung ihrer Verpflichtungen verpflichten. Darüber hinaus bittet das CHNP seine Auftragsverarbeiter und Dienstleister, der Vertraulichkeit der gemäß den geltenden Datenschutzbestimmungen übermittelten personenbezogenen Daten besondere Aufmerksamkeit zu schenken.

b. Übermittlung personenbezogener Daten durch das CHNP

1. Empfänger personenbezogener Daten

Die vom CHNP erhobenen personenbezogenen Daten werden nicht nur von den internen Abteilungen des CHNP, sondern auch von autorisierten externen Empfängern verwendet.

Interne Empfänger entsprechen den internen Abteilungen des CHNP, die berechtigt sind, auf personenbezogene Daten zuzugreifen oder diese zu erhalten, um sie im Rahmen ihrer Zuständigkeiten zu verarbeiten, z. B. ganz allgemein (unabhängig vom Status der betroffenen Person) und ohne Anspruch auf Vollständigkeit: Angehörige der Gesundheitsberufe, Mitarbeiter des CHNP, die für die therapeutische oder medizinische Betreuung des Patienten/Bewohners zuständig sind, das Secrétariat Médical, die Apotheke, die Aufnahmeabteilung, die Sozialarbeiter des CHNP, die Finanz- und Buchhaltungsabteilung für das Rechnungsmanagement, die IT-Abteilung oder die speziell für die Verarbeitung von Mitarbeiterdaten zuständige Personalabteilung.

Im Rahmen der Kontinuität der Pflege, der medizinischen und therapeutischen Betreuung, der Verwaltung und Finanzplanung oder der Einhaltung gesetzlicher Verpflichtungen und Auflagen ist das CHNP jedoch verpflichtet, bestimmte personenbezogene Daten an externe Empfänger weiterzugeben.

Externe Empfänger greifen im Rahmen ihrer jeweiligen Aufgabe(n) auf personenbezogene Daten zu oder werden mit diesen versorgt. Im Wesentlichen handelt es sich um:

- öffentliche Einrichtungen oder Verwaltungsbehörden (Nationale Gesundheitskasse, Ministerium für Gesundheit, Pflegeversicherung usw.),
- externe Gesundheitseinrichtungen oder Angehörige der Gesundheitsberufe (behandelnder Arzt oder externer Spezialist, externe Apotheken oder Labors, Krankenwagen, Pflegeeinrichtungen für die Betreuung nach einem Krankenhausaufenthalt usw.) sowie
- Dienstleister oder Auftragsverarbeiter des CHNP, die Leistungen für das CHNP erbringen und auf personenbezogene Daten ausschließlich zum Zwecke der Erbringung der betreffenden Leistungen zugreifen können (für die Wäscherei sowie die Herstellung und Lieferung von Mahlzeiten zuständiges Personal, Sicherheitsmitarbeiter, die Versicherungsgesellschaft, externe Rechtsberater usw.).

Jede Übermittlung oder Weitergabe personenbezogener Daten, die nicht unter einen Vertrag, die gesetzlichen Verpflichtungen des CHNP, die lebenswichtigen Interessen der betroffenen Person oder die berechtigten Interessen des CHNP fällt, bedarf der ausdrücklichen Zustimmung der betroffenen Person.

Das CHNP kann mit Zustimmung und auf Anweisung der betroffenen Person Informationen über sie an andere Dritte weitergeben.

Schließlich ist es auch möglich, dass das CHNP verpflichtet ist, personenbezogene Daten an Aufsichts-, Polizei- oder Justizbehörden weiterzugeben, wenn dies aufgrund von Gesetzen, Vorschriften oder Gerichtsverfahren oder zum Schutz der Interessen, Rechte und des Eigentums des CHNP erforderlich ist.

2. Grenzüberschreitende Übermittlung personenbezogener Daten

Das CHNP übermittelt keine personenbezogenen Daten in Länder außerhalb der Europäischen Union, es sei denn, diese betreffen den Hauptwohnsitz oder die Betreuung eines Patienten nach einem Krankenhausaufenthalt.

Die Übermittlung von Daten an Empfänger außerhalb der Europäischen Union ist grundsätzlich verboten. Es gibt jedoch Ausnahmen von diesem Verbot, sofern angemessene Maßnahmen zum Schutz und zur Sicherung der übermittelten personenbezogenen Daten getroffen werden.

Wenn das CHNP bestimmte personenbezogene Daten, die außerhalb der Europäischen Union erhoben wurden, übermitteln müsste, würden die betroffenen Personen detailliert unterrichtet und es würden spezifische Maßnahmen zur Kontrolle dieser Übermittlungen ergriffen.

c. Verletzung des Schutzes personenbezogener Daten

Eine Verletzung des Schutzes personenbezogener Daten kann versehentlich (z. B. versehentliche Offenlegung, Verlust oder Diebstahl eines Datenträgers mit personenbezogenen Daten durch einen Dritten, Übermittlung von Daten an den falschen Empfänger) oder böswillig (z. B. Diebstahl eines Datenträgers mit personenbezogenen Daten durch einen Mitarbeiter, Computerpiraterie) erfolgen.

Wenn ein Mitarbeiter von einer solchen versehentlichen oder böswilligen Verletzung personenbezogener Daten Kenntnis erlangt, so ist er verpflichtet, dies intern unverzüglich über das Formular zur Meldung unerwünschter Ereignisse gemäß dem im Intranet verfügbaren Meldeverfahren für die Verletzung des Schutzes personenbezogener Daten zu melden.

Als Verantwortlicher ist das CHNP verpflichtet, ein internes Verzeichnis der ihm bekannten Verletzungen des Schutzes personenbezogener Daten zu führen und die CNPD innerhalb von 72 Stunden zu informieren, es sei denn, diese Verletzung des Schutzes personenbezogener Daten stellt wahrscheinlich kein Risiko für die Rechte und Freiheiten der betroffenen Person(en) dar.

Ebenso ist das CHNP verpflichtet, die betroffene Person zu informieren, wenn eine solche Verletzung des Schutzes personenbezogener Daten wahrscheinlich ein hohes Risiko für diese Person mit sich bringt.

Einzelheiten zu den verschiedenen Arten von Verletzungen des Schutzes personenbezogener Daten und die Modalitäten der Mitteilungen sind dem Meldeverfahren für die Verletzung des Schutzes personenbezogener Daten im Intranet zu entnehmen:

4. Rechte der betroffenen Personen

Jede betroffene Person verfügt über Rechte an den sie betreffenden personenbezogenen Daten, die sie jederzeit und kostenlos[8] unter Nachweis ihrer Identität ausüben kann.

Jede betroffene Person hat damit das Recht,

- über die Verarbeitung sie betreffender personenbezogener Daten unterrichtet zu werden;
- auf sie betreffende personenbezogene Daten zuzugreifen und, falls erforderlich, sie berichtigen zu lassen, sofern sie unvollständig oder unrichtig sind;
- jederzeit ihre Einwilligung zu widerrufen, wenn die jeweilige Verarbeitung auf der Grundlage der Einwilligung der betroffenen Person erfolgte;
- nicht einer ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruhenden Entscheidung unterworfen zu werden;

- in bestimmten Fällen Folgendes zu verlangen:
    - Löschung ihrer personenbezogenen Daten;
    - Übermittlung ihrer personenbezogenen Daten in einem strukturierten, allgemein gebräuchlichen und maschinenlesbaren Format, insbesondere um sie an einen anderen Verantwortlichen weiterzugeben;
    - Einschränkung der Verarbeitung ihrer personenbezogenen Daten;
    - Unterlassung der Verarbeitung ihrer personenbezogenen Daten.

Weitere Informationen zu den Rechten, über die die betroffenen Personen gemäß den für den Schutz personenbezogener Daten geltenden Rechtsvorschriften verfügen, finden diese auf der Website der CNPD unter https://cnpd.public.lu.

a. Modalitäten für die Ausübung der Rechte betroffener Personen

Alle Rechte der betroffenen Personen können auf Anfrage beim DPO des CHNP ausgeübt werden, und zwar per:

- Post an folgende Adresse:

CHNP
17, avenue des Alliés
BP 111
L-9002 Ettelbrück

- E-Mail an: DPO@chnp.lu

[8] Der Verantwortliche kann jedoch die Zahlung von Gebühren für offensichtlich unbegründete oder übermäßige Anfragen oder für die Erstellung weiterer Kopien verlangen, die von der betroffenen Person angefordert werden.

Jeder Anfrage ist eine Kopie von Vorder- und Rückseite des gültigen Ausweises der betroffenen Person beizufügen.

Zu diesem Zweck stellt das CHNP auf seiner Website www.chnp.lu ein Merkblatt zu den Modalitäten für die Ausübung der Rechte betroffener Personen zur Verfügung.

Für die Beantwortung verfügt das CHNP ab Erhalt der Anfrage der betroffenen Person über eine Frist von einem Monat. Bei einer ungenauen Anfrage wird das CHNP um Klärung ersuchen. Die einmonatige Frist kann um weitere zwei Monate verlängert werden, wenn die Anfrage komplex ist. In diesem Fall wird das CHNP die Gründe für die Verschiebung innerhalb eines Monats nach Erhalt der Anfrage angeben.

b. Beschwerdemanagement

Jede betroffene Person, die mit der Art und Weise, in der das CHNP ihre personenbezogenen Daten verarbeitet, nicht zufrieden ist oder Grund zu der Annahme hat, dass die Sicherheit ihrer personenbezogenen Daten gefährdet ist, wird gebeten, sich unter folgender E-Mail-Adresse an das CHNP zu wenden: DPO@chnp.lu

Jede Beschwerde wird intern sorgfältig und transparent geprüft.

Darüber hinaus ist jede betroffene Person berechtigt, die CNPD anzurufen, wenn sie der Ansicht ist, dass ihre Rechte verletzt wurden – dies entweder auf dem Postweg: ***CNPD – 1, avenue du Rock'n Roll – L-4361 Esch-sur-Alzette*** oder online über die Website der CNPD: cnpd.public.lu

5. Cookie-Richtlinie

Ein Cookie ist eine Datei, die aus mehreren Zeichen besteht und an das Endgerät des Benutzers gesendet wird, wenn dieser eine Website besucht. Das Cookie wird von der besuchten Seite in einem dafür vorgesehenen Verzeichnis auf dem Computer des Benutzers abgelegt. Die in diesem Cookie enthaltenen Informationen können beispielsweise den Computer, die besuchten Seiten und die Dauer der Sitzung identifizieren.

Das CHNP verwendet nur analytische Cookies. Analytische Cookies sind Cookies, mit denen die Nutzung und Leistung der besuchten Website (besuchte Inhalte, Verlauf, meistbesuchte Seiten usw.) festgestellt und so deren Funktionsfähigkeit verbessert werden kann. Diese Cookies können vom CHNP oder von Drittanbietern gesetzt werden.

Das CHNP verwendet von Google Analytics entwickelte Statistiken und Auswertungsprogramme, um den Zugriff auf die Website statistisch auszuwerten. Die Daten werden so anonymisiert, dass sie einer bestimmten betroffenen Person nicht mehr zugeordnet werden können (die IP-Adresse wird von Google automatisch gekürzt, sodass keine Identifizierung möglich ist). Benutzer sind als anonyme Benutzer registriert. Cookies sind nur für den Server, der sie erstellt hat, lesbar und ermöglichen keinen Zugriff auf persönliche Informationen des Benutzers oder sonstige Informationen, die sich auf dem Computer des Benutzers befinden. Die erfassten Informationen werden ausschließlich zur Erstellung von Berichten über die Nutzung der Website verwendet.

Weitere Einzelheiten zur Cookie-Richtlinie des CHNP können dem Impressum auf der Website www.chnp.lu entnommen werden.

Bezugsdokumente

- ISO/IEC 27002:2013 & ISO/IEC 27001:2013
- INFORMATIONSSICHERHEITSRICHTLINIE UND GESONDERTE RICHTLINIEN
- Dieser Richtlinie zugrundeliegende(s) Verfahren:
  - MELDEVERFAHREN FÜR DIE VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN
- INFORMATIONSBROSCHÜREN
- IMPRESSUM AUF DER WEBSITE DES CHNP

***

Diese allgemeine Richtlinie, die für alle auf der Website des CHNP zugänglich ist, wird zur Berücksichtigung von Änderungen bei Rechts- und Verwaltungsvorschriften sowie Änderungen in der Unternehmensorganisation regelmäßig aktualisiert. Sie werden gebeten, die Richtlinie regelmäßig durchzulesen.