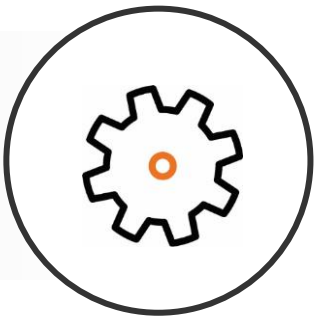
Das weltweit führende
Zertifizierungsprogramm
für Holzpellets

ENplus-Verfahrensdokument

Umgang mit vertraulichen und persönlichen Informationen



ENplus PD DE 2008: 2022, erste Ausgabe

gültig in Deutschland

Deutsches Pelletinstitut GmbH
Neustädtische Kirchstraße 8
10117 Berlin, Deutschland
Tel: + 49 30 688 1599 55
E-Mail: info@enplus-pellets.de

Name des Dokuments: Umgang mit vertraulichen und persönlichen Informationen
Titel des Dokuments: EN*plus* PD DE 2008: 2022, erste Ausgabe
Veröffentlichungsdatum: 01.10.2022
Datum des Inkrafttretens: 01.01.2023
Übergangsfrist(en): keine

Vorwort

Der 2010 gegründete European Pellet Council (EPC), ein Netzwerk von Bioenergy Europe AISBL, ist ein Dachverband, der die Interessen der europäischen Holzpelletbranche vertritt. Seine Mitglieder sind nationale Pelletverbände oder Bioenergieverbände aus zahlreichen Ländern innerhalb und außerhalb Europas. Der EPC bietet dem Pelletsektor eine Plattform zur Erörterung von Herausforderungen, die beim Übergang von einem Nischenprodukt zu einem wichtigen Energieträger zu bewältigen sind. Dazu gehören die Normung und Zertifizierung der Pelletqualität, Sicherheit, Versorgungssicherheit sowie Aus- und Weiterbildung.

Das Deutsches Pelletinstitut GmbH (**DEPI**) wurde 2008 als Tochtergesellschaft des Deutschen Energieholz- und Pellet-Verbandes e. V. (DEPV) als Kommunikationsplattform und Kompetenzzentrum für Themen rund um das Heizen mit Holzpellets gegründet. Im Jahr 2010 entwickelte das **DEPI** in Zusammenarbeit mit dem Deutschen Biomasseforschungszentrum Leipzig gGmbH (DBFZ) und proPellets Austria das EN*plus*-Programm für Holzpellets. 2011 wurden die Markenrechte für alle Länder außerhalb Deutschlands an den EPC übertragen.

Heute ist der EPC der führende Verband für das EN*plus*-Qualitätszertifizierungsprogramm für alle Länder außer Deutschland. In Deutschland wird das Programm durch das DEPI organisiert.

Dieses Dokument tritt am 01. Januar 2023 in Kraft.

Inhalt

Vorwort **3**

Einführung **5**

1. Geltungsbereich **6**

2. Normative Verweise **7**

3. Begriffe und Definitionen **8**

4. Allgemeine Anforderungen **12**

5. Vorgaben zum Schutz personenbezogener Daten **13**

6. Vorgaben zum Schutz vertraulicher Informationen **16**

Einführung

Das Hauptziel des ENplus-Programms ist die Gewährleistung einer gleichbleibend hohen Qualität von Holzpellets. Über das ENplus-Logo können Kunden und Verbrauchern die Qualität von Pellets auf transparente und überprüfbare Weise verfolgen.

Holzpellets sind ein erneuerbarer Brennstoff, der hauptsächlich aus Sägerestholz hergestellt wird. Holzpellets werden als Brennstoff sowohl für Heizungsanlagen in Privathaushalten als auch in Großanlagen im industriellen Maßstab verwendet. Da Holzpellets zu den Brennstoffen gehören, die bei Umschlagsprozessen beschädigt werden können, ist ein Qualitätsmanagement erforderlich, das die gesamte Lieferkette von der Auswahl des Rohstoffs bis zur Lieferung an den Endverbraucher abdeckt.

Mit diesem Dokument werden die Anforderungen an die Informationssicherheits- und Datenschutzziele der Deutsches Pelletinstitut GmbH beim Umgang mit vertraulichen und persönlichen Informationen bezüglich der zertifizierten Unternehmen, wie auch die Anforderungen der jeweiligen Beteiligten an den Prozeduren im Zusammenhang der Zertifizierung (z. B. die Zertifikatsbeantragung und Überwachungsinspektionen), wie auch das Zusammenspiel von Zertifizierungsstellen, Inspektionsstellen und Prüflaboren nach den gesetzgeberischen Vorgaben neu definiert.

Alle aufgeführten Maßnahmen und Verpflichtungen in diesem Dokument dienen dem Ziel, einen angemessenen und wirksamen Schutz potenziell kritischer Infrastrukturen, Systeme, Anwendungen und Informationen zu gewährleisten und die Anforderungen von Partnern und gesetzliche Vorgaben zu erfüllen. Vertrauliche und persönliche Informationen von Unternehmen und Partnern müssen geschützt werden. Dabei dienen die gesetzlich auferlegten Pflichten aus DS-GVO und GeschGehG als Leitlinie der Anforderungen. Weitergehende Pflichten als diejenigen aus den gesetzlichen Vorgaben werden nicht gefordert.

Das Dokument ist Teil des **ENplus-Handbuchs**, das aus ENplus-Standards, ENplus-Verfahrensdokumenten sowie ENplus-Leitfäden besteht.

Die aktuellen Versionen der verschiedenen Teile des **ENplus-Handbuchs** werden auf der der deutschen Webseite (www.enplus-pellets.de) des ENplus-Programms veröffentlicht.

Der Begriff „muss“ wird in diesem Dokument verwendet, um auf die Bestimmungen hinzuweisen, die verbindlich sind. Der Begriff „soll“ wird verwendet, um auf die Bestimmungen hinzuweisen, die zwar nicht verbindlich sind, von denen aber erwartet wird, dass sie übernommen und umgesetzt werden. Der Begriff „darf“ steht für die Erlaubnis etwas umzusetzen, während „kann“ sich auf die Fähigkeit oder die Möglichkeiten bezieht eine Anforderung umzusetzen.

Die fettgedruckten Begriffe werden in Kapitel 3 „Begriffe und Definitionen“ erläutert.

1. Geltungsbereich

Das **internationale ENplus-Management**, das **für Deutschland zuständige ENplus-Management (DEPI)** und die **nationalen ENplus-Lizenzgeber** nutzen Informationen über die ENplus-zertifizierten **Unternehmen**, die eine **Verarbeitung** i.S. der DS-GVO darstellen. Dasselbe gilt für **ENplus-Konformitätsbewertungsstellen** und andere Institutionen, die im Rahmen von ENplus tätig sind. Da diese Informationen auch einen geschäftlichen Wert haben und auch **personenbezogene Daten** enthalten können, müssen die an der **Vertraulichkeitskette beteiligten Stellen** die Vertraulichkeit der Daten und die Einhaltung der geltenden Rechtsvorschriften sicherstellen.

Der Umfang der gesammelten Informationen ist im **ENplus-Handbuch** festgelegt und umfasst insbesondere:

a) Daten, die sich auf zertifizierte **Unternehmen** beziehen;

b) Daten der **ENplus-Inspektionsstellen** und **ENplus-Prüflabore**;

c) Daten über Einrichtungen, die an den Zertifizierungsaktivitäten beteiligt sind;

d) Daten im Zusammenhang mit dem Beschwerde- und Einspruchsverfahren sowie dem Markenmissbrauchsverfahren;

e) Daten in Bezug auf Einrichtungen, die an der Verwaltung des Zertifizierungsprogramms beteiligt sind.

2. Normative Verweise

Die hier aufgeführten Dokumente sind wesentlich für die Anwendung dieses Handbuchs und der darin definierten Anforderungen. Für aufgeführte Dokumente ohne Datumsangabe gilt jeweils die aktuelle Version (schließt jegliche Neufassung mit ein).

ENplus ST 1001, *ENplus-Holzpellets – Anforderungen an Unternehmen* (weltweit gültig)

ENplus PD DE 2004, *ENplus-Zulassung und unabhängige Kontrolle von Konformitätsbewertungsstellen* (gültig in Deutschland)

Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

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

Bundesdatenschutzgesetz (BDSG)

3. Begriffe und Definitionen

Die Reihenfolge der in diesem Kapitel aufgeführten Begriffe und Definitionen weicht von jener in der englischen Version des Dokumentes ab um die Suche durch den Nutzer erleichtern.

3.1 Audit

Prüfung der Umsetzung aller Anforderungen des **ENplus-Handbuchs** durch gelistete Auditoren. Es wird unterschieden zwischen Vor-Ort- und Fernaudit sowie zwischen Erst-, Überwachungs- und Rezertifizierungsaudit.

3.2 Auftragsverarbeiter

Ist gem. Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die **personenbezogene Daten** im Auftrag des Verantwortlichen verarbeitet.

3.3 Beteiligte Stellen

Das **internationale ENplus-Management**, das **für Deutschland zuständige ENplus-Management (DEPI)** und die **nationalen ENplus-Lizenzgeber** zusammen mit den **ENplus-Konformitätsbewertungsstellen**, Akkreditierungsstellen und **unabhängige Kontrollstellen** sind die relevanten **beteiligten Stellen** am Prozess eines erfolgreichen Informationssicherheits- und Datenschutzmanagements.

3.4 Betroffene Person

siehe **Personenbezogene Daten**

3.5 DEPI

Das **DEPI** (Deutsches Pelletinstitut GmbH) ist das **für Deutschland zuständige ENplus- Management** und als **ENplus-Zertifizierungsstelle** verantwortlich für alle Zertifizierungsaktivitäten in Deutschland. Außerdem ist das **DEPI** als **ENplus-Inspektionsstelle** in Deutschland tätig.

3.6 ENplus-Handbuch

Der Begriff „**ENplus-Handbuch**“ ist gleichbedeutend mit „ENplus-Dokumentation“ und umfasst alle Dokumente zu Anforderungen, Anleitung und Verfahren des ENplus-Programms.

ANMERKUNG: Die verschiedenen Elemente des Handbuchs (Standards, Leitfäden und Verfahrensdokumente) werden in PD 2001 beschrieben.

3.7 ENplus-Inspektionsstelle

Eine Inspektionsstelle, die für die Durchführung von Audits im Rahmen des ENplus-Zertifizierungsprogramms zugelassen ist.

ANMERKUNG: Eine Inspektionsstelle kann eine eigenständige Organisation oder Teil einer Organisation sein.

3.8 ENplus-Konformitätsbewertungsstelle

Ein Sammelbegriff für **ENplus-Zertifizierungsstellen**, **ENplus-Inspektionsstellen** und **ENplus-Prüflabore**.

3.9 ENplus-Prüflabor

Ein Prüflabor, das für die Durchführung von Laboranalysen im Rahmen des ENplus-Zertifizierungsprogramms zugelassen ist.

3.10 ENplus-Zertifizierungsstelle

Eine Organisation, die für die Durchführung von Zertifizierungen im Rahmen des ENplus-Zertifizierungsprogramms zugelassen ist. Das **DEPI** ist die für alle Zertifizierungen in Deutschland zuständige **ENplus-Zertifizierungsstelle**.

3.11 Für Deutschland zuständiges ENplus-Management (DEPI)

Für das Management des ENplus-Programms in Deutschland gesamtverantwortlich zuständige Organisation.

3.12 Geschäftsgeheimnis

Nach § 2 Nr. 1 GeschGehG ist ein **Geschäftsgeheimnis** jede Information, die (1) weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher (2) von wirtschaftlichem Wert ist und die (3) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch das **für Deutschland zuständige ENplus-Management (DEPI)** ist und hinsichtlich derer (4) ein berechtigtes Interesse an der Geheimhaltung besteht.

3.13 Informationssicherheitsereignis

Ein **Informationssicherheitsereignis** ist jedes Ereignis, das in Hinsicht auf den Schutz **personenbezogener Daten** und **vertraulicher Informationen** sicherheitsrelevant sein könnte.

3.14 Internationales ENplus-Management

Bioenergy Europe AISBL, repräsentiert durch das European Pellet Council (EPC), ist das zuständige Management des ENplus-Zertifizierungsprogramms mit der Gesamtverantwortung für das Management des ENplus-Programms außerhalb Deutschlands.

3.15 Mitarbeiter

Sämtliche Arbeitskräfte, die für ein Unternehmen, eine Behörde oder eine Institution tätig sind bzw. an einem Projekt beteiligt sind und am Erreichen des Ziels mitarbeiten, unabhängig von Ihrem Sozialversicherungsstatus. Umfasst sind damit insbesondere Arbeitnehmer, Angestellte, Freelancer, Selbständige, Praktikanten oder Studentische Hilfskräfte.

3.16 Nationaler ENplus-Lizenzgeber

Das für die Umsetzung des ENplus-Zertifizierungsprogramms in einem bestimmten Land zuständige Management, das durch das **internationale ENplus-Management** ernannt wird.

ANMERKUNG: Die Kontaktdaten der für die verschiedenen Länder zuständigen **nationalen ENplus-Lizenzgeber** sind auf der **offiziellen ENplus-Webseite** zu finden.

3.17 Offizielle ENplus-Webseite

Die offizielle Webseite des ENplus-Zertifizierungsprogrammes, die vom **Internationalen ENplus-Management** für alle Länder außer Deutschland (www.enplus-pellets.eu)und vom **DEPI** für Deutschland (www.enplus-pellets.de) betrieben wird

3.18 Personenbezogene Daten

Sind nach Art. 4 Nr. 1 DS-GVO 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 (im Folgenden „**betroffene Person**“).

3.19 Technische und organisatorische Maßnahmen (TOMs)

Sind die nach Art. 32 (DS-GVO) vorgeschriebenen Maßnahmen, um die Sicherheit der **Verarbeitung personenbezogener Daten** zu gewährleisten. Jeder Verantwortliche hat die TOMs in seinem Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren (siehe **(Daten)Verantwortlicher**).

3.20 Unabhängige Kontrolle der EN*plus*-Konformitätsbewertungsstellen

Unabhängige Kontrolle der **EN*plus*-Zertifizierungsstelle** (**DEPI**) sowie der zugelassenen **EN*plus*-Inspektionsstellen** und **EN*plus*-Prüflabore**. **EN*plus*-Inspektionsstellen**, die nicht über die erforderliche Akkreditierung verfügen, müssen eine erweiterte Kontrolle durchlaufen.

ANMERKUNG: Einzelheiten zur **unabhängigen Kontrolle der EN*plus*-Konformitätsbewertungsstellen** sind in PD DE 2004 festgelegt.

3.21 Unabhängige Kontrollstelle

Unabhängige Stelle, die jährlich die Arbeit aller in Deutschland tätigen **EN*plus*-Konformitätsbewertungsstellen** prüft.

3.22 Unternehmen

Ein Unternehmen, das die in EN*plus* ST 1001 definierten Bestimmungen umsetzt.

3.23 (Daten)Verantwortlicher

Ist gem. Art. 4 Nr. 7 DS-GVO 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.

3.24 Verarbeitung

Der Begriff des „Verarbeitens“ umfasst nach Art. 4 Nr. 2 DS-GVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit **personenbezogenen Daten** wie bspw. (nicht abschließend) das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Kenntnisnahme, 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.

3.25 Vertrauliche Informationen

Vertrauliche Informationen umfassen

a) alle **Geschäftsgeheimnisse**

b) alle betrieblichen Angelegenheiten vertraulicher Natur, deren Geheimhaltung durch das **für Deutschland zuständige ENplus-Management (DEPI)** angeordnet oder deren Geheimhaltungsbedürftigkeit offensichtlich ist

c) alle betrieblichen Informationen vertraulicher Natur, die für ein berufliches Spezialgebiet fachfremd sind (z. B. bei einem Informatiker Daten zu einem chemischen Prozess)

d) alle nicht offenkundigen betrieblichen Informationen vertraulicher Natur, die im Rahmen des Arbeitsverhältnisses direkt oder über Dritte, insbesondere von Unternehmen oder Kooperationspartnern, generiert werden und deren Vertraulichkeit entweder offenkundig oder mitgeteilt wurde.

3.26 Vertraulichkeitskette

Das **internationale ENplus-Management**, das **für Deutschland zuständige ENplus-Management (DEPI)**und **die nationalen ENplus-Lizenzgeber** bilden zusammen mit den Zertifizierungsstellen, Inspektions- und Prüfstellen, Akkreditierungsstellen und **unabhängige Kontrollstellen** als **beteiligte Stellen** eine **Vertraulichkeitskette**.

4. Allgemeine Anforderungen

4.1 Die in diesem Kapitel definierten Anforderungen müssen von allen am ENplus-Zertifizierungsprogramm **beteiligten Stellen** erfüllt werden.

4.2 Die Vorgaben der relevanten Gesetze, Normen und Anforderungen aus Verträgen müssen eingehalten werden und erfahren durch interne und/oder externe **Audits** eine regelmäßige Überprüfung. Die Änderungen müssen regelmäßig bewertet und im Zuge der kontinuierlichen Verbesserung eingearbeitet werden.

4.3 Alle Stellen, die Teil der Vertraulichkeitskette sind, unterliegen den vorgegebenen Vertraulichkeitsanforderungen und sind verpflichtet, gesammelte Informationen nur in Übereinstimmung mit den Bestimmungen der ENplus-Standards, ENplus-Verfahrensdokumenten und ENplus-Leitfäden weiterzugeben. Die genannten Stellen der Vertraulichkeitskette werden zur Einhaltung der nachfolgenden Anforderungen verpflichtet. Sie werden auch aufgrund der Umsetzung der Datenschutzvorgaben und der transparenten Informationssicherheitsmechanismen ausgewählt. Verstöße fließen in die Bewertung im Rahmen der **unabhängigen Kontrolle der ENplus-Konformitätsbewertungsstellen** (ENplus PD DE 2004) ein und können zum Entzug der Zulassung führen.

4.4 **Vertrauliche Informationen** und **personenbezogene Daten** sind möglichst so zu verarbeiten, dass sie anonymisiert und mit anderen Daten zusammengeführt werden, so dass die zusammengefassten Daten niemanden identifizieren und nicht zur Ableitung **vertraulicher Informationen** oder **personenbezogener Daten** verwendet werden können. Anonymisierte Daten fallen nicht mehr unter den Schutz der DS-GVO.

4.5 Jedes (potenzielle) **Informationssicherheitsereignis** muss gemeldet werden. Der Meldeweg muss dem Umfang des Ereignisses sowie der zeitlichen Dringlichkeit einer Reaktion entsprechend angemessen gewählt werden. Bei weniger kritischen Ereignissen soll eine E-Mail gesendet werden. In anderen Fällen soll telefonisch alarmiert werden.

4.6 Die externe Kommunikation von Sicherheitsvorfällen und damit verbundenen Ereignissen, Situationen oder Aktivitäten muss koordiniert erfolgen. **Mitarbeiter** sind nicht befugt, eigenmächtig Informationen im Zusammenhang mit Informationssicherheitsvorfällen herauszugeben.

5. Vorgaben zum Schutz personenbezogener Daten

5.1 Das **für Deutschland zuständige ENplus-Management (DEPI)** und die anderen Stellen der **Vertraulichkeitskette** verpflichten sich zur Einhaltung aller anwendbaren Gesetze bezüglich der **Verarbeitung personenbezogener Daten** (DS-GVO).

5.2 Das **für Deutschland zuständige ENplus-Management (DEPI)** handelt als **(Daten)Verantwortlicher** und kann auch als Datenverarbeiter im Auftrag auftreten.

5.3 Auftragsverarbeiter

a) dürfen **personenbezogene Daten** nur insoweit verarbeiten, als dies für die Erfüllung des Vertrags erforderlich ist;

b) stellen sicher, dass alle **erforderlichen technischen und organisatorischen Maßnahmen (TOMs)** getroffen werden, um **personenbezogene Daten** vor zufälliger oder unrechtmäßiger Zerstörung oder zufälligem Verlust, Änderung, unbefugter Weitergabe oder unbefugtem Zugriff und allen anderen unrechtmäßigen Formen der **Verarbeitung** zu schützen, wobei jeder Vorfall in Bezug auf die vorgenannten Punkte im Folgenden als „Sicherheitsvorfall“ bezeichnet wird;

c) benachrichtigen unverzüglich den Verantwortlichen schriftlich über einen Sicherheitsvorfall, und zwar innerhalb drei Arbeitstagen nach dem Eintreten des Sicherheitsvorfalls oder unmittelbar nach Bekanntwerden des Sicherheitsvorfalls, je nachdem, welcher Zeitpunkt der spätere ist; in der Benachrichtigung sind die Auswirkungen des Sicherheitsvorfalls auf alle **betroffenen Personen**, die davon betroffen sein könnten, angemessen detailliert zusammenzufassen;

d) kooperieren in angemessener Weise mit dem Verantwortlichem bei dessen Untersuchung des Sicherheitsvorfalls und machen ohne vorherige schriftliche Zustimmung des Verantwortlichen keine öffentliche Bekanntgabe des Sicherheitsvorfalls;

e) erstatten dem Verantwortlichen alle angemessenen Abhilfekosten, die entstanden sind, wenn der Sicherheitsvorfall auf den **Auftragsverarbeiter** zurückzuführen ist;

f) informieren den Verantwortlichen unverzüglich schriftlich über jede Anfrage (z. B. auf Auskunft oder Löschung), jeden Einspruch oder jede Beschwerde einer **betroffenen Person** oder einer Aufsichtsbehörde und arbeiten mit dem Verantwortlichen bei der Bearbeitung der Anfrage, des Einspruchs oder der Beschwerde angemessen zusammen;

g) verarbeiten **personenbezogene Daten** nur innerhalb des Europäischen Wirtschaftsraums oder in Ländern außerhalb des Europäischen Wirtschaftsraums, die von der Europäischen Kommission als ein angemessenes Schutzniveau anerkannt wurden (zusammen die „zulässigen Länder“) und gewähren keinem Empfänger außerhalb der zulässigen Länder Zugang zu **personenbezogenen Daten** oder übermitteln diese, es sei denn, der Verantwortliche hat einem solchen Zugang oder einer solchen Übermittlung schriftlich zugestimmt;

h) arbeiten nicht mit Unterauftragnehmern zusammen, es sei denn, der Verantwortliche hat der Vergabe von Unteraufträgen vorher schriftlich zugestimmt;

i) ergreifen alle erforderlichen Maßnahmen, um die Zuverlässigkeit und Vertrauenswürdigkeit seiner **Mitarbeiter** zu gewährleisten, die Zugang zu **personenbezogenen Daten** ha-

ben, und stellen sicher, dass alle **Mitarbeiter** und Beauftragten, die zum Zugang zu **personenbezogenen Daten** befugt sind, dies nur dann tun dürfen, wenn sie verpflichtet sind, die **personenbezogenen Daten** vertraulich zu behandeln, es sei denn, die Offenlegung der Daten ist zur ordnungsgemäßen Erfüllung ihrer Aufgaben oder zur Einhaltung einer Verpflichtung nach EU-Recht oder dem Recht eines Mitgliedstaates, dem der **Auftragsverarbeiter** unterliegt, erforderlich; in diesem Fall informiert der **Auftragsverarbeiter** den Verantwortlichen vor der Offenlegung der **personenbezogenen Daten** über die geltende rechtliche Verpflichtung, es sei denn, das Gesetz verbietet die Weitergabe dieser Informationen aus wichtigen Gründen des öffentlichen Interesses;

j) löschen oder geben bei Beendigung des Vertrages alle **personenbezogenen Daten** nach Wahl des Verantwortlichen zurück, es sei denn, das Recht der EU oder eines Mitgliedstaates schreibt die Speicherung der **personenbezogenen Daten** vor;

k) unterstützen den Verantwortlichen bei der Erfüllung seiner Verpflichtungen gemäß den geltenden Datenschutzgesetzen.

5.4 Durch **technische und organisatorische Maßnahmen (TOMs)** ist ein angemessener Schutz aller **personenbezogenen Daten**, insbesondere die im Rahmen der Zertifizierung, der Webseiten und Veranstaltungen verarbeitet werden, sicherzustellen und zu dokumentieren.

5.5 Auf Verlangen der **betroffenen Person** erteilen die Verantwortlichen jederzeit Auskunft über die zu ihrer Person gespeicherten Daten und Übergeben eine Kopie dieser Daten.

5.6 Darüber hinaus erhält die **betroffene Person** unaufgefordert Zugang zu den folgenden Informationen:

a) Die Zwecke der **Verarbeitung**;

b) Die Kategorien der betroffenen **personenbezogenen Daten**;

c) Die Empfänger oder Kategorien von Empfängern, an die die **personenbezogenen Daten** weitergegeben wurden oder werden;

d) Wenn möglich, die vorgesehene Dauer der Speicherung der **personenbezogenen Daten** oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) Informationen darüber, ob **personenbezogene Daten** in ein Drittland oder an eine internationale Organisation übermittelt werden;

f) Das Bestehen des Rechts, von dem für die **Verarbeitung** Verantwortlichen die Berichtigung oder Löschung **personenbezogener Daten** oder die Einschränkung der **Verarbeitung personenbezogener Daten**, die die **betroffene Person** betreffen, zu verlangen oder gegen eine solche **Verarbeitung** Widerspruch einzulegen;

g) Das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

h) Falls die **personenbezogenen Daten** nicht bei der **betroffenen Person** erhoben wurden, alle verfügbaren Informationen über ihre Herkunft;

i) Das Bestehen des Rechts der Einwilligung zur **Verarbeitung** ihrer **personenbezogenen Daten** jederzeit zu widerrufen.

5.7 Daraus hervorgehend ist von den betroffenen Stellen ein angemessenes Sicherheitskonzepts inkl. eines Informationssicherheitsmanagementsystems, **technische und organisatorische Maßnahmen (TOMs)** und die generelle Sorgfalt hinsichtlich Persönlichkeitsrechten Betroffener, Datensparsamkeit, Vertraulichkeit bereitzustellen.

6. Vorgaben zum Schutz vertraulicher Informationen

6.1 Grundsätzlich ist jede festgestellte (signifikante) Information ein schützenswertes Gut. Eine Inventarisierung der Informationen zum Anwendungsbereich (einschließlich tangierender Bereiche) ist daher unabdingbar, so dass die Sicherheitsmaßnahmen angemessen erfolgen müssen, insbesondere wenn der Inhaber des **Geschäftsgeheimnisses** den Schutz von **Geschäftsgeheimnissen** nach dem GeschGehG in Anspruch nehmen will. Informationen müssen nach ihrem Wert, gesetzlichen Vorschriften, Betriebswichtigkeit uns Sensibilität im Hinblick auf unbefugte Offenlegung oder Veränderung klassifiziert werden.

6.2 Die gesammelten Informationen, die teilweise auch nicht öffentlich zugänglich sind, werden grundsätzlich als schützenswerte Informationen betrachtet. Sie werden wie vertraglich und im **ENplus-Handbuch** vorgesehen an **beteiligte Stellen** weitergegeben.

6.3 Alle gesammelten Informationen, die nicht öffentlich zugänglich sind, müssen als **vertrauliche Informationen** behandelt und dürfen nicht an Dritte weitergegeben werden. **Vertrauliche Informationen** im Sinne dieses Dokuments sind

a) alle **Geschäftsgeheimnisse**,

b) alle betrieblichen Angelegenheiten vertraulicher Natur, deren Geheimhaltung durch das **für Deutschland zuständige ENplus-Management (DEPI)**) angeordnet oder deren Geheimhaltungsbedürftigkeit offensichtlich ist,

c) alle betrieblichen Informationen vertraulicher Natur, die für ein berufliches Spezialgebiet fachfremd sind (z. B. bei einem Informatiker Daten zu einem chemischen Prozess),

d) alle nicht offenkundigen betrieblichen Informationen vertraulicher Natur, die im Rahmen des Arbeitsverhältnisses direkt oder von Dritten, insbesondere von **Unternehmen** oder Kooperationspartnern, erhalten wurden und deren Vertraulichkeit entweder offenkundig ist oder mitgeteilt wurde.

6.4 Die Maßnahmen zur Umsetzung der Sicherheitskriterien und das Erreichen der Sicherheitsziele sind in erster Linie nicht technischer, sondern organisatorischer Natur.

Die maßgeblichen Sicherheitskriterien sind Verfügbarkeit, Vertraulichkeit und Integrität:

a) Vertraulichkeit bedeutet: Informationen werden gegenüber Unberechtigten nicht offengelegt.

b) Integrität bedeutet: Die Vollständigkeit und Korrektheit/Unverfälschtheit von Informationswerten wird geschützt.

c) Zugreifbarkeit/Verfügbarkeit bedeutet: Berechtigte können auf Informationen zugreifen und diese nutzen, wann immer dies erforderlich ist.

6.5 Informationen müssen nach Ihrem Wert, gesetzlichen Vorschriften, Betriebswichtigkeit uns Sensibilität im Hinblick auf unbefugte Offenlegung oder Veränderung klassifiziert werden.

6.6 Das Personal, das Zugang zu **vertraulichen Informationen** hat, wird ordnungsgemäß autorisiert. Das autorisierte Personal muss:

a) ordnungsgemäß im Schutz **vertraulicher Informationen** geschult sein;

b) Vertraulichkeitsformulare oder Vertraulichkeitsvereinbarungen unterzeichnen.

c) Bei Verstößen im Umgang mit **vertraulichen Informationen** sind disziplinarische Maßnahmen zu ergreifen

6.7 **Vertrauliche Informationen** auf Papierdokumenten sind durch die Sicherung der Informationen in einzelnen Akten zu schützen, die unter Verschluss zu halten sind.

6.8 **Vertrauliche Informationen**, die digitalisiert oder auf andere Weise in elektronischen Medien dargestellt werden, müssen in gesicherten Formaten gespeichert werden. Jede elektronische Datenbank mit sensiblen Informationen muss ausreichend gegen unbefugten Zugriff geschützt sein.

6.9 Dritte, die spezifische Dienstleistungen im Zusammenhang mit der Verwaltung des ENplus-Programms erbringen und Zugang zu den sensiblen Informationen haben, müssen eine Geheimhaltungsvereinbarung oder ähnliche Vereinbarungen unterzeichnen.

Das weltweit führende
Zertifizierungsprogramm
für Holzpellets

Wir sind ein weltweit führendes, transparentes und unabhängiges Zertifizierungsprogramm für Holzpellets. Wir garantieren die Qualität und bekämpfen Markenmissbrauch entlang der gesamten Bereitstellungskette, von der Produktion bis zur Auslieferung.

Deutsches Pelletinstitut GmbH
Neustädtische Kirchstraße 8
10117 Berlin, Deutschland
Tel.: + 49 30 688 1599 55
E-Mail: info@enplus-pellets.de