Unternehmensrichtlinie Datenschutz

CSG Clinische Studien Gesellschaft mbH

Stand 09.05.2018

CSG Clinische Studien Gesellschaft mbH
Friedrichstraße 180
10117 Berlin

www.csg-germany.com

1. Bedeutung, Ziel, Zugänglichkeit

(1) Diese Unternehmensrichtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten im Unternehmen.
(2) Mit dieser Unternehmensrichtlinie sollen die Persönlichkeitsrechte von Betroffenen gewahrt und geschützt werden.
(3) Die Unternehmensrichtlinie muss für alle Beschäftigten und leitenden Angestellten jederzeit leicht zugänglich sein.

2. Geltungsbereich

(1) Diese Richtlinie gilt persönlich für alle Beschäftigten sowie leitenden Angestellten der CSG Clinische Studien Gesellschaft mbH.
(2) Die Gebote und Verbote dieser Unternehmensrichtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob dieser elektronisch oder in Papierform vonstattengeht. Ebenso beziehen sie alle Kategorien von betroffenen Personen (Kunden, Beschäftigte, Lieferanten etc.) in ihren Geltungsbereich ein.

3. Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (betroffene Person). Kundendaten gehören dabei ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie seine E-Mail-Adresse. Es genügt, wenn die jeweilige Information mit dem Namen der betroffenen Person verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z. B. beim Autokennzeichen. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.
(2) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, genetische oder biometrische Daten sowie Angaben über eine eventuelle Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben.
(3) Erheben ist das Beschaffen von Daten über eine betroffene Person.
(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist
    - Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,

- Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
- Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
- die Daten an den Dritten weitergegeben werden oder
- der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
- Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken (z. B. durch einen Vermerk oder die Entnahme aus einer Zugriffsberechtigung),
- Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt (z. B. die Auswertung bzw. Selektion personenbezogener Daten zur werblichen Ansprache).

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(7) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(8) Verantwortlicher ist die juristische Person, einschließlich sämtlicher Untergliederungen und unselbständiger Zweigstellen, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Wer im Einzelfall als Verantwortlicher anzusehen ist, richtet sich danach, wer über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(9) Dritter ist jede Person oder Stelle neben dem Verantwortlichen, so auch andere konzernangehörige juristische Personen.

(10) Auftragsverarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch einen Auftragnehmer für einen Auftraggeber. Der Auftragnehmer darf die personenbezogenen Daten nur nach Weisung des Auftraggebers erheben, verarbeiten oder nutzen. Die Verantwortung für den Datenumgang verbleibt beim Auftraggeber als Verantwortlichem.

4. Datenschutzorganisation

(1) Die CSG Clinische Studien Gesellschaft mbH hat einen Datenschutzbeauftragten nach Maßgabe des Bundesdatenschutzgesetzes (BDSG) bzw. der Datenschutz-Grundverordnung (DSGVO) bestellt. Diesen erreichen Sie unter folgenden Kontaktdaten:

Dr. Uwe Schläger
datenschutz nord GmbH
Konsul-Smidt-Str. 88

28217 Bremen

Ansprechpartnerin:
Linda Dannenberg
ldannenberg@datenschutz-nord.de
Telefon: +49 30 308 77 49 14
Fax: +49 30 308 77 49 11

(2) Der Datenschutzbeauftragte überwacht und gewährleistet die Einhaltung der gesetzlichen Vorgaben sowie die der Richtlinie. Der Datenschutzbeauftragte berät die Unternehmensleitung zu Fragen des Datenschutzes, ist zuständig bei der Kommunikation mit Betroffenen und Aufsichtsbehörden und berichtet regelmäßig der Unternehmensleitung über die Umsetzung des Datenschutzes im Unternehmen.
(3) Der Datenschutzbeauftragte nimmt seine Aufgaben weisungsfrei und unter Anwendung seiner Fachkunde wahr. Er ist der Geschäftsleitung unmittelbar unterstellt.
(4) Das Unternehmen bzw. seine Mitarbeiter haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen.

5. Umgang mit personenbezogenen Daten

(1) Die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, es sei denn eine gesetzliche Norm erlaubt explizit den Datenumgang. Personenbezogene Daten dürfen nach dem BDSG bzw. der DSGVO grundsätzlich verarbeitet werden:
- Bei einem bestehenden Vertragsverhältnis mit der betroffenen Person.
- Im Zuge der Vertragsanbahnung oder -abwicklung mit der betroffenen Person.
- Wenn und soweit die betroffene Person eingewilligt hat.
- Wenn eine spezielle Rechtsvorschrift außerhalb des BDSG bzw. der DSGVO die Verarbeitung erfordert.
- Wenn weitere Erlaubnistatbestände des BDSG bzw. der DSGVO vorliegen.

(2) Personenbezogene Daten sind für einen zuvor festgelegten Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit dem ursprünglich festgelegten Zweck vereinbar ist. Eine Datenhaltung ohne Zweck, so beispielsweise die Vorratsdatenspeicherung, ist unzulässig.
(3) Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist ebenfalls nur mit einer gesetzlichen Erlaubnisnorm oder der Einwilligung der betroffenen Person zulässig.

(4) Personenbezogene Daten sollen grundsätzlich direkt bei der betroffenen Person erhoben werden. Eine Erhebung aus anderen Quellen (Internet, Warndienste, Auskunfteien) ist ohne ein zwingendes gesetzliches Erfordernis unzulässig. Besteht ein gesetzliches Erfordernis, ist die betroffene Person unverzüglich über die Datenerhebung zu informieren, soweit eine gesetzliche Regelung dem nicht entgegensteht.
(5) Die betroffene Person ist bei der Erhebung seiner personenbezogenen Daten über die Zweckbestimmung, die Identität des Verantwortlichen sowie die Empfänger seiner personenbezogenen Daten zu informieren.
(6) Personenbezogene Daten müssen sachlich richtig und, wenn nötig, auf dem neusten Stand sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Die jeweilige Fachabteilung hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmäßig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen.
(7) Falls möglich, sollte auf einen personenbezogenen Datenumgang verzichtet werden. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen. Beispielsweise kann es im Rahmen einer statistischen Auswertung von Daten nicht notwendig sein, den Vollnamen einer betroffenen Person zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrundeliegenden Information ebenfalls gewährleisten kann.

6. Besondere personenbezogene Daten

Besondere personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung der betroffenen Person oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben, verarbeitet oder genutzt werden. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z. B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

7. Datenübermittlung/Datenweitergabe

(1) Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung der betroffenen Person zulässig.
(2) Befindet sich der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen betroffener Personen. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann.

8. Externe Dienstleister

(1) Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist der Datenschutzbeauftragte vorab zu informieren.

(2) Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang
- Technisch-organisatorische Sicherheitsmaßnahmen
- Erfahrung des Anbieters im Markt
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.)

(3) Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung. Hierin sind Datenschutz- und IT-Sicherheitsaspekte zu regeln.

(4) Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

9. Datenvermeidung, Datensparsamkeit, Privacy by design and by default

(1) Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einer betroffenen Person zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist.

(2) Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen. Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern („Privacy by design“).

10. Rechte von betroffenen Personen

(1) Betroffene Personen haben das Recht auf Auskunft über die im Unternehmen über ihre Person gespeicherten personenbezogenen Daten.

(2) Bei der Bearbeitung von Anträgen ist die Identität der betroffenen Person zweifelsfrei festzustellen.

(3) Die Auskunftserteilung erfolgt auf schriftlichem Weg und beinhaltet, neben den zur Person vorhandenen Daten, auch die Empfänger von Daten sowie den Zweck der Verarbeitung und, soweit möglich, die geplante Dauer, für

die die personenbezogenen Daten gespeichert werden. Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung, soweit dies nicht Rechte und Freiheiten anderer Personen beeinträchtigt.

(4) Der Datenschutzbeauftragte steht bei der Bearbeitung von Auskunftsbegehren beratend zur Verfügung.

(5) Betroffene Personen haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen.

(6) Personenbezogene Daten sind insbesondere unter den folgenden Voraussetzungen zu löschen:
- personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig oder
- , die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung. oder
- die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor oder
- personenbezogenen Daten wurden unrechtmäßig verarbeitet.

(7) An die Stelle einer Löschung kann eine Einschränkung der Verarbeitung von Daten treten, wenn
- eine Kenntnis der Daten für die Erfüllung des Zwecks der Speicherung zwar nicht mehr erforderlich ist, jedoch gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, oder
- schutzwürdige Interessen der betroffenen Person beeinträchtigt würden, oder
- die personenbezogenen Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt

(8) Widerspricht die betroffene Person der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung ist eine weitere Verarbeitung oder Nutzung für diese Zwecke unzulässig.

11. Auskunftsersuchen Dritter über betroffene Personen

Sollte eine Stelle Informationen über Betroffene fordern, so beispielsweise Kunden oder Beschäftigte dieses Unternehmens, ist eine Weitergabe von Informationen nur zulässig, wenn

- die Auskunft gebende Stelle ein berechtigtes Interesse hierfür darlegen kann, und
- eine gesetzliche Norm zur Auskunft verpflichtet, sowie
- –die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

12. Verfahrensmeldung, Verzeichnis von Verarbeitungstätigkeiten

(1) Dem Datenschutzbeauftragten sind vor Einführung eines Verfahrens, das den Umgang mit personenbezogenen Daten zum Inhalt hat, durch die jeweils fachlich verantwortliche Person alle notwendigen Informationen zur Ausgestaltung dieses Verfahrens zur Verfügung zu stellen.
(2) Der Datenschutzbeauftragte führt eine Übersicht über gemeldete Verfahren zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten (Verzeichnis von Verarbeitungstätigkeiten).

13. Werbung

(1) Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax, oder E-Mail ist grundsätzlich nur zulässig, wenn der Betroffene zuvor in die Verwendung seiner Daten zu Werbezwecken eingewilligt hat.
(2) Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm zulässig. Bitte konsultieren Sie diesbezüglich den Datenschutzbeauftragten.

14. Schulung

Beschäftigte, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen.

15. Datengeheimnis

Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Sie sind vor Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Die Verpflichtung erfolgt durch die Geschäftsleitung unter Verwendung des hierzu vorgesehenen Formulars.

16. Beschwerden

(1) Jeder Betroffene hat das Recht, sich über eine Verarbeitung seiner Daten zu beschweren, sollte er sich hierdurch in seinen Rechten verletzt fühlen. Ebenso können Beschäftigte Verstöße gegen diese Unternehmensrichtlinie jederzeit anzeigen.
(2) Die zuständige Stelle für die oben genannten Beschwerden ist der Datenschutzbeauftragte als interne unabhängige und weisungsfreie Instanz.

17. Interne Ermittlungen

(1) Maßnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis sind unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchzuführen. Insbesondere müssen die dabei erhobenen und verwendeten Daten zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen der Betroffenen verhältnismäßig sein.

(2) Die betroffene Person ist so bald wie möglich über die zu seiner Person durchgeführten Maßnahmen zu informieren.

(3) Bei allen Formen der internen Ermittlungen ist der Datenschutzbeauftragte hinsichtlich der Auswahl und Ausgestaltung der Maßnahmen vorab einzubeziehen.

18. Verfügbarkeit, Vertraulichkeit und Integrität von Daten

(1) In Abhängigkeit der Art der Daten und deren Schutzbedürftigkeit hat für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Risikoanalyse zu erfolgen. Dies gilt insbesondere für besondere personenbezogene Daten gem. § 3 Abs.2 dieser Richtlinie.

(2) Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird ein allgemeines Sicherheitskonzept erstellt, das für alle Verfahren verbindlich ist. Hierin sind insbesondere Mittel und Maßnahmen zur Verschlüsselung und Datensicherung vorzusehen.

(3) Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Türen unbesetzter Räume sind zu verschließen. Wirksame Maßnahmen zur Zugangskontrolle an Geräten müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit stets zu sperren.

(4) Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und sind nicht übertragbar. Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten werden. Passwörter müssen eine minimale Länge von zehn Zeichen aufweisen und aus einem Zeichenmix bestehen. Passwörter dürfen nicht in einem Wörterbuch vorkommen oder aus leicht zu erratenden Begriffen gebildet werden, insbesondere nicht Begriffe, die im Zusammenhang mit dem Unternehmen stehen.

(5) Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-to-know-Prinzip“). Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein.

(6) Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung17 hat zwingend zu erfolgen, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.

(7) Zu unterschiedlichen Zwecken erhobene personenbezogene Daten sind getrennt voneinander zu verarbeiten. Die Trennung von Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.
(8) Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

19. Unrechtmäßige Kenntniserlangung von Daten („Datenpanne“)

(1) Sollten Unternehmensdaten unrechtmäßig Dritten offenbart worden sein, ist darüber unverzüglich der Datenschutzbeauftragte zu informieren.
(2) Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

20. Folgen von Verstößen

Ein fahrlässiger oder gar mutwilliger Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

21. Aktualisierung der Richtlinie

(1) Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.
(2) Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten und leitenden Angestellten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.