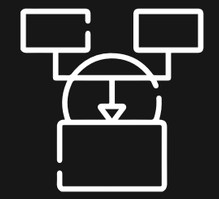
Datenschutzerklärung von Vitrintec Sp. z o.o.

VITRINTEC®
wall solutions

Vorwort

Vitrintec Sp. z o.o. ist der für die Datenverarbeitung Verantwortliche und der Vorstandsvorsitzende, Tomasz Rybka, ist für den Schutz der personenbezogenen Daten zuständig. Er ist verpflichtet, alle notwendigen Maßnahmen zu ergreifen, um Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten zu vermeiden.
Die Datenschutzerklärung ist ein Dokument, das die Grundsätze des Schutzes personenbezogener Daten beschreibt, die der Verantwortliche anwendet, um die Anforderungen der 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 sowie des Gesetzes vom 10. Mai 2018 zum Schutz personenbezogener Daten (Gesetzblatt 2018, Punkt 1000) zu erfüllen.

Mit dieser Datenschutzerklärung sollen die Ziele der 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 (Allgemeine Datenschutzverordnung, im Folgenden DSGVO) erfüllt werden. Sie stellt eine Reihe von Anforderungen, Regeln und Vorschriften zum Schutz personenbezogener Daten bei der Verantwortlichen für die Datenverarbeitung.



KAPITEL 1

Allgemeine Bestimmungen

§ 1

Für die Zwecke dieses Dokuments werden die folgenden Definitionen eingeführt:

1. Richtlinie – Datenschutzerklärung von Vitrintec Sp. z o.o.

2. Personenbezogene Daten – alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine Person betrachtet, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Merkmalen, die sich auf ihre physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Eigenschaften beziehen.

3. Datensatz – ein strukturierter Satz personenbezogener Daten, der nach bestimmten Kriterien zugänglich ist, unabhängig davon, ob der Satz zentral, dezentral oder funktional bzw. geografisch verstreut ist.

4. Verantwortlicher – eine natürliche oder juristische Person, Behörde, organisatorische Einheit oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

5. Auftragsverarbeiter – eine natürliche oder juristische Person, Behörde, Organisationseinheit oder sonstige Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet;

6. Risiko – ein Indikator für einen Zustand oder ein Ereignis, das zu einem Verlust führen kann. Es ist proportional zu der Wahrscheinlichkeit, dass dieses Ereignis eintritt, und zu der Höhe des Verlustes, den es verursachen kann.

7. Verarbeitung – ein Vorgang oder eine Reihe von Vorgängen, die mit personenbezogenen Daten oder einer Reihe von personenbezogenen Daten in automatisierter oder nicht automatisierter Weise durchgeführt werden, z. B. Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Abrufen, Abfragen, Verwenden, Offenlegen, Verbreiten oder sonstiges Bereitstellen, Abgleichen oder Verknüpfen, Einschränken, Löschen, Vernichten.

8. Empfänger – eine natürliche oder juristische Person, Behörde, Organisationseinheit oder sonstige Stelle, an die personenbezogene Daten weitergegeben werden, unabhängig davon, ob es sich um einen Dritten handelt oder nicht. Die Behörden, die im Rahmen eines Verfahrens nach EU-Recht oder dem Recht der Mitgliedstaaten personenbezogene Daten erhalten können, gelten nicht als Empfänger.

9. Einwilligung der betroffenen Person – eine freiwillige, spezifische, bewusste und eindeutige Willenserklärung, mit der die betroffene Person durch eine schriftliche Erklärung oder eine klare bestätigende Handlung ihre Zustimmung zur Verarbeitung der sie betreffenden personenbezogenen Daten erteilt.

10. Verletzung des Schutzes personenbezogener Daten (Vorfall) – eine Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe oder zum unbefugten Zugriff auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt.

§ 2

1. Die Richtlinie dient dazu:

a) den Schutz der bei Vitrintec Sp. z o.o. verarbeiteten personenbezogenen Daten zu gewährleisten

b) einheitliche Verhaltensregeln für die Verarbeitung von personenbezogenen Daten festzulegen,

c) organisatorische und technische Maßnahmen zu ergreifen, die eine gesetzeskonforme Verarbeitung personenbezogener Daten, insbesondere der DSGVO, gewährleisten, und dies nachweisen zu können.

2. Die spezifischen Ziele der Richtlinie sind:

a) sicherzustellen, dass die Rechte der betroffenen Personen ausgeübt werden,

b) die Pflichten und Verantwortlichkeiten der Personen festzulegen, die verpflichtet sind, die in der Richtlinie festgelegten Aufgaben auszuüben,

c) sicherzustellen, dass Folgenabschätzungen zum Datenschutz durchgeführt werden,

d) Verstöße gegen den Schutz personenbezogener Daten zu verwalten und zu reduzieren,

e) die Art und Weise, wie die Mitarbeiter/innen mit den Änderungen der Vorschriften zu personenbezogenen Daten vertraut gemacht werden.

3. Anwendungsbereich der Richtlinie

a) Die Richtlinie regelt die Art und Weise der Verarbeitung personenbezogener Daten und die Verwaltung von Vorgängen im Zusammenhang mit der Verarbeitung personenbezogener Daten, um einen angemessenen Schutz der Daten zu gewährleisten, für die der Geschäftsführer verantwortlich oder mitverantwortlich ist,

b) Die Richtlinie legt auch fest, wie personenbezogene Daten verarbeitet werden und wie Prozesse im Zusammenhang mit der Verarbeitung personenbezogener Daten verwaltet werden, um einen angemessenen Schutz dieser Daten zu gewährleisten,

c) Die Richtlinie legt die Pflichten und Verantwortlichkeiten der Personen fest, die verpflichtet sind, die Aufgaben im Zusammenhang mit den fraglichen Prozessen auszuüben,

d) Die Richtlinie gilt für die Verarbeitung der betreffenden personenbezogenen Daten unabhängig von:

1) der Art der Verarbeitung (voll automatisiert, teilautomatisiert oder nicht automatisiert),

2) der Form oder der Art der Verarbeitung (auf Papier, elektronisch oder auf andere Weise),

3) den Kanälen, über die personenbezogene Daten übermittelt werden,

4) der für die Verarbeitung personenbezogener Daten verwendeten IT-Tools (Systeme, Anwendungen, Programme),

5) dem Zweck der Verarbeitung,

6) der Quelle der personenbezogenen Daten,

7) den Kategorien von personenbezogenen Daten,

KAPITEL 2

Datenbestand.

Grundsätze der Verarbeitung personenbezogener Daten.

Verantwortung Informationspflicht.

Vereinbarungen und Kontakte

mit externen Parteien.

§ 3

1. Die zu schützenden personenbezogenen Daten sind im Anhang zu dieser Richtlinie aufgeführt (Anhang Nr. 1 - Liste der Kategorien personenbezogener Daten).
2. Die Liste enthält Datensätze, bei denen ein potenzielles Risiko für die Verletzung der Rechte oder Freiheiten von Personen festgestellt wurde.
3. Jeder Datensatz wird so beschrieben, dass eine Risikoanalyse durchgeführt werden kann.
4. Die Beschreibung der Datensätze enthält u.a. folgende Informationen

a) den Namen des Datensatzes,
b) die Beschreibung der Zwecke der Verarbeitung,
c) die Art, den Umfang, den Kontext, die dokumentierten personenbezogenen Daten,
d) die Empfänger,
e) die funktionale Beschreibung der Verarbeitungsvorgänge,
f) die zur Verarbeitung der personenbezogenen Daten verwendeten Mittel,
g) die Information über die Notwendigkeit der Durchführung einer Folgenabschätzung für den Datensatz,
h) die Kategorie der betroffenen Personen,
i) die Daten des Verantwortlichen – der Person, die für die erhobenen Daten verantwortlich ist,
j) geplante Termine für die Löschung,
k) Rechtsgrundlage der Verarbeitung.

§ 4

1. Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass personenbezogene Daten in Übereinstimmung mit den folgenden Regeln verarbeitet werden:

a) rechtmäßig, fair und transparent für die betroffene Person (Rechtmäßigkeit, Fairness und Transparenz),

b) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden (Zweckbindung),

c) den Zwecken, für die sie verarbeitet werden, angemessen, relevant und nicht übermäßig sind (Datenminimierung),

d) zutreffend sind und, soweit erforderlich, aktualisiert werden (Richtigkeit),

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, und zwar nicht länger, als es für die Zwecke der Verarbeitung erforderlich ist, abgesehen von den in der Verordnung genannten Ausnahmen (Speicherbegrenzung),

f) in einer Weise, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor zufälligem Verlust, zufälliger Zerstörung oder zufälliger Beschädigung durch technische und organisatorische Maßnahmen, die den Risiken und der Kategorie der zu schützenden Daten angemessen sind, und insbesondere den Schutz vor Weitergabe an Unbefugte oder vor dem Zugriff durch Unbefugte (Integrität und Vertraulichkeit),

g) Die sogenannte Informationspflicht - das Recht auf Auskunft über die Daten, Datenübertragbarkeit, Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch - gegenüber den betroffenen Personen, deren Daten verarbeitet werden, ausgeübt wurde.

2. Der Verantwortliche führt ein Register der Verarbeitungstätigkeiten. Das Register ist gleichzeitig ein Verzeichnis der von dem Verantwortlichen verarbeiteten personenbezogenen Datensätze (Anhang 1).

3. Der Auftragsverarbeiter führt ein Verzeichnis der Kategorien von Verarbeitungstätigkeiten.

§ 5

1. All employees of Vitrintec Sp. z o.o., irrespective of their basis of employment and persons carrying out activities on the basis of civil law contracts, who process personal data as part of their duties, are obliged to apply the principles set out by this document.
2. Any person with access to personal data processed at Vitrintec Sp. z o.o. is required to read this document.

§ 6

1. Der Verantwortliche/Verarbeiter ist für die Erteilung und Aufhebung von Genehmigungen zur Verarbeitung personenbezogener Daten in Papierform und IT-Systemen verantwortlich.

2. Der Auftragsverarbeiter und jede Person, die im Auftrag des Verantwortlichen oder des Auftragsverarbeiters handelt und Zugang zu personenbezogenen Daten hat, darf personenbezogene Daten nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, dies ist gesetzlich vorgeschrieben.

3. Die Berechtigungen für Datensätze werden auf Antrag der Vorgesetzten (Leiter/Abteilungsleiter) erteilt. Die Leiter von Organisationseinheiten legen den Umfang der Befugnisse für die Verarbeitung personenbezogener Daten fest.

4. Die Genehmigungen legen den Umfang der Datenverarbeitung fest.

5. Die Genehmigungen sollten in den Personalakten der Mitarbeiter aufbewahrt werden (ggf. in den Akten der zuständigen Ausschüsse), nur befugten Personen zugänglich gemacht werden und bei Änderungen des Aufgabenbereichs aktualisiert werden.

6. In Ausnahmefällen können die Genehmigungen in Form von Anordnungen erteilt werden, z. B. die Genehmigung zur Durchführung von Inspektionen, Audits, behördlichen Tätigkeiten.

7. Der Verantwortliche führt ein Register der bevollmächtigten Personen, um den ordnungsgemäßen Zugriff auf die Daten zu kontrollieren. Das Register ist dieser Richtlinie beigefügt (Anhang Nr. 2 – Musterregister der befugten Personen). Die Daten werden in elektronischer Form aufbewahrt.

§ 7

8. Die Berechtigung zur Verarbeitung personenbezogener Daten im IT-System wird auf Antrag der Vorgesetzten (Abteilungsleiter) der Personen, die die Daten verarbeiten sollen, erteilt. In bestimmten Fällen kann ein solcher Antrag auch von den Beschäftigten gestellt werden. Der Antrag auf eine Ressource, die sich auf personenbezogene Daten bezieht, ist per E-Mail an den IT-Spezialisten innerhalb der Organisation zu richten, wobei auch der Vorgesetzte zu informieren ist (E-Mail zur Kenntnis).

8. Die Leiter der Organisationseinheiten der Abteilungen legen fest, zu welchen IT-Systemen die Beschäftigten ihrer Abteilungen Zugang und welchen Umfang die Berechtigungen haben.

8. Die in Abs. 1 genannte Berechtigung erlischt mit der Beendigung der Verarbeitung personenbezogener Daten durch die Person, der die Berechtigung erteilt wurde, oder mit der Beendigung des Arbeitsverhältnisses.

§ 8

1. Wenn der Verantwortliche personenbezogene Daten von einer betroffenen Person erhält, ist er verpflichtet, ihr die folgenden Informationen zur Verfügung zu stellen:

a) seine/ihre Identität und Kontaktangaben,

b) die Zwecke der Datenverarbeitung und die Rechtsgrundlage der Verarbeitung

c) wenn die Verarbeitung personenbezogener Daten mit der Ausübung eines berechtigten Interesses verbunden ist, das von dem Verantwortlichen oder von einem Dritten verfolgt wird – das berechtigte Interesse muss angegeben werden,

d) Angaben zu den Empfängern oder Kategorien von Empfängern der personenbezogenen Daten

e) ggf. Informationen über die Absicht, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln,

f) den Zeitraum, für den die personenbezogenen Daten gespeichert werden, und, falls dies nicht möglich ist, die Kriterien für die Festlegung dieses Zeitraums,

g) Informationen über das Recht, von dem Verantwortlichen Zugang zu den personenbezogenen Daten der betroffenen Person, deren Berichtigung, Löschung oder Einschränkung der Verarbeitung zu verlangen, oder das Recht, der Verarbeitung zu widersprechen, sowie das Recht auf Datenübertragbarkeit,

h) Informationen über das Recht, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit, der auf der Grundlage der Einwilligung vor dem Widerruf erfolgten Verarbeitung berührt wird (diese Regelung gilt für die Verarbeitung von Daten auf der Grundlage einer für einen oder mehrere Zwecke erteilten Einwilligung und für die Verarbeitung besonderer Datenkategorien auf der Grundlage der Einwilligung der betroffenen Person),

i) Informationen über das Recht, eine Beschwerde bei der Aufsichtsbehörde einzureichen

j) Informationen darüber, ob die Daten zur Verfügung zu stellen ein gesetzliches oder vertragliches Erfordernis oder eine Bedingung für den Abschluss eines Vertrages ist und ob die betroffene Person verpflichtet ist, die Daten zur Verfügung zu stellen und welche Folgen es haben kann, wenn sie dies nicht tut,

k) Informationen zur automatisierten Entscheidungsfindung.

2. Wenn der Verantwortliche personenbezogene Daten von einer anderen Quelle als der betroffenen Person erhält, ist er verpflichtet, der betroffenen Person alle in Abs. 1 genannten Informationen zur Verfügung zu stellen, und zusätzlich: Informationen über die Quelle der personenbezogenen Daten zu geben.

3. Die in Abs. 2 genannten Informationen sind von dem Verantwortlichen für die Verarbeitung innerhalb einer angemessenen Frist nach Erhalt der Daten zu erteilen, spätestens jedoch innerhalb eines Monats unter Berücksichtigung der besonderen Umstände der Verarbeitung personenbezogener Daten. Sollen personenbezogene Daten für die Kommunikation mit der betroffenen Person verwendet werden, muss der Verantwortliche die Daten spätestens bei der ersten solchen Kommunikation zur Verfügung stellen. Wenn geplant ist, personenbezogene Daten an einen anderen Empfänger weiterzugeben, spätestens bei der ersten Weitergabe.

§ 9

1. Personenbezogene Daten dürfen nur für die Ziele verwendet werden, für die sie erhoben wurden, werden oder werden sollen, und nur so lange verarbeitet werden, wie es für die Erreichung der Ziele, für die die Daten verarbeitet werden, erforderlich ist. Personenbezogene Daten dürfen länger gespeichert werden, wenn sie ausschließlich zu Archivierungszwecken im öffentlichen Interesse, zu wissenschaftlichen oder historischen Zwecken oder zu statistischen Zwecken verarbeitet werden.

2. Personenbezogene Daten sollten in einer Form gespeichert werden, die eine Identifizierung der betroffenen Person nicht zulässt.

3. Die betroffene Person hat das Recht, von dem Verantwortlichen die Berichtigung sie betreffender Daten zu verlangen, falls sie unrichtig sind.

4. Die betroffene Person hat das Recht, von dem Verantwortlichen die unverzügliche Löschung der sie betreffenden personenbezogenen Daten zu verlangen, und der Verantwortliche ist verpflichtet, die Daten unverzüglich zu löschen, wenn eine der Voraussetzungen gegeben ist:

a) die personenbezogenen Daten sind für die Ziele, für die sie erhoben wurden, nicht mehr erforderlich,

b) die betroffene Person hat die Einwilligung, auf die sich die Verarbeitung stützt, zurückgezogen und es gibt keine andere Rechtsgrundlage für die Verarbeitung,

c) die betroffene Person legt nach dem Gesetz Widerspruch ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor,

d) die personenbezogenen Daten unrechtmäßig verarbeitet worden sind,

e) die personenbezogenen Daten gelöscht werden müssen, um einer rechtlichen Verpflichtung nachzukommen,

f) die personenbezogenen Daten im Zusammenhang mit dem Angebot von Diensten der Informationsgesellschaft erhoben wurden.

5. Die betroffene Person hat das Recht, die Einschränkung der Verarbeitung in folgenden Fällen zu verlangen:

a) die betroffene Person bestreitet die Richtigkeit der Daten,

b) die Daten werden unrechtmäßig verarbeitet, und die betroffene Person widerspricht der Löschung der Daten,

c) Der Verantwortliche benötigt die personenbezogenen Daten nicht mehr für die Ziele der Verarbeitung, aber die Daten werden von der betroffenen Person zur Feststellung, Geltendmachung oder Verteidigung eines Anspruchs benötigt,

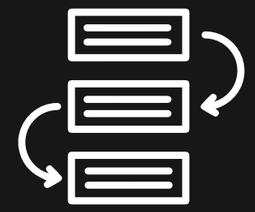
d) Die betroffene Person hat gegen die Verarbeitung Widerspruch eingelegt.

6. Die betroffene Person hat das Recht, die dem Verantwortlichen zur Verfügung gestellten sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und diese personenbezogenen Daten einem anderen Verantwortlichen zu übermitteln.

7. Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung, einschließlich Profiling, beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Folgen nach sich zieht oder sie in ähnlicher Weise erheblich beeinträchtigt.

§ 10

1. Wenn die Daten im Auftrag des Verantwortlichen verarbeitet werden sollen, dürfen nur solche Auftragsverarbeiter eingesetzt werden, die ausreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Verarbeitung den Anforderungen dieser Verordnung entspricht und die Rechte der betroffenen Personen geschützt werden.
2. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen rechtsverbindlichen Rechtsinstruments, das zwischen dem Auftragsverarbeiter und dem Verantwortlichen geschlossen wird und in dem der Gegenstand und die Dauer der Verarbeitung, ihre Art und ihr Zweck, die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen sowie die Pflichten und Rechte des Verantwortlichen festgelegt sind.
3. Bei der Beauftragung von externen Unternehmen, die sich auf den Betrieb von Schlüsselelementen des IT-Sicherheitsmanagementsystems auswirken, wird es empfohlen, einen Vertrag über die Beauftragung abzuschließen.



KAPITEL 3

Umgang mit Risiken für die Sicherheit personenbezogener Daten.

Leitfaden für den Umgang mit Vorfällen.

§ 11

Das Verfahren definiert einen Katalog von Sicherheitslücken und -vorfällen bei personenbezogenen Daten und beschreibt, wie darauf zu reagieren ist. Sein Zweck ist es, die Folgen von Vorfällen im Bereich der Sicherheit zu minimieren und das Risiko von Bedrohungen und Vorfällen in der Zukunft zu verringern.

1. Jeder Mitarbeiter des Unternehmens ist verpflichtet, seinen direkten Vorgesetzten unverzüglich, spätestens innerhalb von 24 Stunden, zu benachrichtigen, wenn eine Sicherheitslücke festgestellt wird oder ein Vorfall eintritt. Wenn der Vorfall den Verlust von digitalen Daten betrifft, sollte auch die IT-Abteilung informiert werden.
2. Zu den typischen Schwachstellen im Zusammenhang mit der Sicherheit personenbezogener Daten gehören insbesondere:

a. unzureichende physische Sicherheit von Räumen, Geräten und Dokumenten,

b. unzureichender Schutz von IT-Hardware und -Software gegen Lecks, Diebstahl und Verlust von personenbezogenen Daten,

c. Nichteinhaltung der Grundsätze zum Schutz personenbezogener Daten durch die Beschäftigten (z. B. Nichtanwendung des Prinzips des sauberen Schreibtischs/Bildschirms, Passwortschutz, fehlendes Abschließen von Räumen, Schränken und Schreibtischen).

3. Zu den typischen Vorfällen im Zusammenhang mit der Sicherheit personenbezogener Daten gehören insbesondere:

a. externe zufällige Ereignisse (Brand im Gebäude/Raum, Überschwemmung, Stromausfall, Kommunikationsausfall),

b. interne zufällige Ereignisse (Ausfälle von Servern, Computern, Festplatten, Software, Fehler von IT-Mitarbeitern und Nutzern, Datenverluste),

c. vorsätzliche Vorfälle (Hacken des IT-Systems oder der Räume, Diebstahl von Daten oder Geräten, Weitergabe von Informationen, Offenlegung von Daten an Unbefugte, vorsätzliche Zerstörung von Dokumenten oder Daten, Viren oder andere Malware).

4. Wenn ein Vorfall festgestellt wird, führt der Verantwortliche (im Falle digitaler Daten unter Mitwirkung der IT-Abteilung) eine Untersuchung durch, bei der die folgenden Aspekte ermittelt werden:

a. der Umfang und die Ursachen des Vorfalls und seine möglichen Folgen,

b. mögliche disziplinarische Maßnahmen,

c. Maßnahmen zur Wiederherstellung des Betriebs der Organisation nach dem Vorfall,

d. präventive (vorsorgliche) Maßnahmen, die darauf abzielen, ähnliche Vorfälle in Zukunft zu vermeiden oder Verluste zu verringern.

5. Der Verantwortliche muss alle oben genannten Verstöße gegen den Schutz personenbezogener Daten dokumentieren, einschließlich ihre Umstände, Folgen und ergriffenen Maßnahmen (Anhang Nr. 3 – Meldung eines Verstoßes gegen den Schutz personenbezogener Daten),
6. Es ist verboten, bewusst oder unbewusst Vorfälle durch Personen zu verursachen, die berechtigt sind, Daten zu verarbeiten.
7. Im Falle einer Verletzung des Schutzes personenbezogener Daten, die das Risiko einer Verletzung der Rechte oder Freiheiten natürlicher Personen mit sich bringt, muss der Verantwortliche dies unverzüglich - nach Möglichkeit spätestens 72 Stunden nach Feststellung der Verletzung - der Aufsichtsbehörde melden.
8. Bei einem Vorfall benachrichtigt der Verantwortliche die betroffenen Personen darüber.

KAPITEL 4

Datenschutzbestimmungen,
wichtige Richtlinien.

§ 12

1. Die Bestimmungen legen die grundlegenden Verpflichtungen von Arbeitnehmern, Mitarbeitern, Mitarbeitern von Dritten, die Zugang zu personenbezogenen Daten haben, die von dem Verantwortlichen verarbeitet werden, und Nutzern von IT-Systemen mit Zugang zu personenbezogenen Daten, die von dem Verantwortlichen verarbeitet werden, fest.

2. Nachdem sie sich mit den Grundsätzen des Schutzes personenbezogener Daten vertraut gemacht haben, sind die Personen verpflichtet, ihre Kenntnis dieser Grundsätze zu bestätigen und zu erklären, dass sie sie anwenden (Anhang Nr. 5 - Erklärung über die vertrauliche Behandlung personenbezogener Daten am Arbeitsplatz).

KAPITEL 5

Schulung/Audit

§ 13

1. Jeder Nutzer ist verpflichtet, sich mit den Vorschriften in diesem Bereich vertraut zu machen und die damit verbundenen Aufgaben und Verantwortlichkeiten zu verstehen, bevor er personenbezogene Daten verarbeiten darf.
2. Alle Nutzer müssen regelmäßig an internen Schulungen teilnehmen.
3. Der Verantwortliche ist für die Durchführung der Schulungen verantwortlich.
4. Wenn eine interne Schulung zu den Grundsätzen des Schutzes personenbezogener Daten durchgeführt wird, ist es ratsam, diese zu dokumentieren.
5. Nach der Schulung zu den Grundsätzen des Schutzes personenbezogener Daten sind die Teilnehmer verpflichtet, ihre Kenntnis dieser Grundsätze zu bestätigen und ihre Anwendung zu erklären.
6. Gemäß Artikel 32 der DSGVO muss der Verantwortliche die Wirksamkeit der technischen und organisatorischen Maßnahmen, die die Sicherheit der Verarbeitung gewährleisten sollen, regelmäßig prüfen, messen und bewerten.

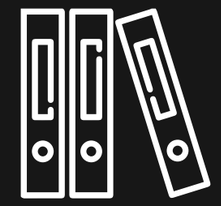
KAPITEL 6

Technische und organisatorische
Maßnahmen zum Schutz

§ 14

1. Gemäß Artikel 32 der DSGVO muss der Verantwortliche sicherstellen, dass die Verfügbarkeit von und der Zugang zu personenbezogenen Daten schnell wiederhergestellt werden kann. Im Falle eines physischen oder technischen Vorfalls.

2. Die Verfahren zur Wiederherstellung der Verfügbarkeit von und des Zugriffs auf personenbezogene Daten wurden in einem Anhang festgelegt (Anhang 10 - Geschäftskontinuitätsplan).



KAPITEL 7

Liste der Räume, in denen Dokumente mit personenbezogenen Daten bei Vitrintec Sp. z o.o.

§ 15

Die Liste der Räume, die der Vitrintec Sp. z o.o. gehören und in denen personenbezogene Daten verarbeitet werden, einschließlich der besonders geschützten Räume, ist dieser Richtlinie beigefügt: Anhang 4 - Liste der Räume.

VITRINTEC®
wall solutions

Die Datenschutzerklärung für Vitrintec Sp. z o.o. wurde
am 1. Juli 2024 in Kraft gesetzt.