creo concept®

PERFECT WALL

Datenschutzerklärung bei CreoConcept

creo concept®

PERFECT WALL

Einleitung

CreoConcept Sp. z o.o. Sp. k. ist der Verantwortliche der personenbezogenen Daten und die Tätigkeiten im Bereich des Schutzes personenbezogener Daten werden vom Vorstandsvorsitzenden Tomasz Rybka durchgeführt. Er ist verpflichtet, alle erforderlichen Maßnahmen zu ergreifen, um Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten vorzubeugen.

Die Datenschutzerklärung ist ein Dokument, das die Grundsätze des Schutzes personenbezogener Daten beschreibt, die der Verantwortliche verwendet, 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 und zum freien Datenverkehr sowie zur Aufhebung der Richtlinie 95/46/EG und des Gesetzes vom 10. Mai 2018 zum Schutz personenbezogener Daten (polnisches Gesetzblatt 2018 pos. 1000) zu erfüllen.

Zweck dieser Datenschutzerklärung ist es, 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 (Datenschutz-Grundverordnung, im Folgenden RODO) zu erfüllen Es handelt sich um eine Reihe von Anforderungen, Regeln und Vorschriften zum Schutz personenbezogener Daten durch den Verantwortlichen der personenbezogenen Daten.

Kapitel I

Allgemeine Bestimmungen

§ 1

Für die Zwecke dieses Dokuments werden die folgenden Definitionen eingeführt:

1. Richtlinie – Datenschutzerklärung bei CreoConcept Sp. z o.o. z o.o. Sp. k.,
2. Personenbezogene Daten – alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine identifizierbare Person ist eine Person, die direkt oder indirekt, insbesondere anhand einer Identifikationsnummer oder eines oder mehrerer spezifischer Faktoren, die ihre physischen, physiologischen, mentalen, wirtschaftlichen, kulturellen oder sozialen Merkmale bestimmen, identifiziert werden kann.
3. Datensatz – ein geordneter Satz personenbezogener Daten, der nach bestimmten Kriterien verfügbar ist, unabhängig davon, ob dieser Satz zentral, dezentral oder funktional oder geografisch verteilt ist.
4. Verantwortlicher – eine natürliche oder juristische Person, Behörde, Organisationseinheit oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Methoden der Verarbeitung personenbezogener Daten entscheidet.
5. Verarbeitende Einheit – eine natürliche oder juristische Person, Behörde, Organisationseinheit oder andere juristische Person, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
6. Risiko – ein Indikator für einen Zustand oder ein Ereignis, das zu Verlusten führen kann. Es ist proportional zur Eintrittswahrscheinlichkeit dieses Ereignisses und zur Höhe des Schadens, den es verursachen kann.
7. Verarbeitung – ein Vorgang oder eine Reihe von Vorgängen, die mit personenbezogenen Daten oder Sätzen personenbezogener Daten auf automatisierte oder nicht automatisierte Weise ausgeführt werden, z. B. das Sammeln, Aufzeichnen, Organisieren, Strukturieren, Speichern, Anpassen oder Modifizieren, Herunterladen, Durchsuchen, Verwenden, Offenlegen durch Senden , Verbreiten oder sonstiges Bereitstellen, Abgleichen oder Zusammenführen, Einschränken, Löschen, Vernichten.
8. Empfänger - ist eine natürliche oder juristische Person, Behörde, Organisationseinheit oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt. Öffentliche Behörden, die im Rahmen laufender Verfahren nach dem Recht der EU oder der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten nicht als Empfänger.
9. Einwilligung der betroffenen Person - eine ohne Zwang, für den konkreten Fall, in Kenntnis der Sachlage und unmissverständlich abgegebene Willensbekundung, mit der die betroffene Person durch eine schriftliche Erklärung oder eine eindeutige bestätigende Handlung in die Verarbeitung der sie betreffenden personenbezogenen Daten einwilligt.
10. Verstoß gegen den Schutz personenbezogener Daten (Vorfall) – ein Sicherheitsverstoß, der zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unbefugten Offenlegung oder zum unbefugten Zugriff auf übertragene, gespeicherte oder anderweitig verarbeitete personenbezogene Daten führt.

§ 2

1. Die Datenschutzerklärung dient folgendem:

a) Gewährleistung des Schutzes der bei CreoConcept Sp. z o.o. Sp. k.,

b) Festlegung einheitlicher Verhaltensregeln für die Verarbeitung personenbezogener Daten,

c) Umsetzung organisatorischer und technischer Maßnahmen, die eine rechtskonforme Verarbeitung personenbezogener Daten, insbesondere der DSGVO, gewährleisten und die Möglichkeit zum Nachweis dieser Einhaltung bieten.

2. Die detailierten Ziele der Richtlinie sind:

a) Gewährleistung der Umsetzung der Rechte der Personen, auf die sich personenbezogene Daten beziehen,

b) Festlegung der Pflichten und Verantwortlichkeiten der Personen, die zur Erfüllung der in der Richtlinie festgelegten Aufgaben verpflichtet sind,

c) Gewährleistung der Datenschutz-Folgenabschätzungen,

d) Umgang mit Verstößen gegen den Schutz personenbezogener Daten und Begrenzung ihrer Auswirkungen,

e) Art und Weise, wie die Mitarbeiter über Änderungen der Vorschriften informiert werden betrifft personenbezogene Daten.

3. Geltungsbereich der Datenschutzerklärung

a) Die Datenschutzerklärung legt die Art der Verarbeitung personenbezogener Daten und die Verwaltung von Prozessen im Zusammenhang mit der Verarbeitung personenbezogener Daten fest, um einen angemessenen Schutz der Daten zu sichern, für die der Verantwortliche oder Co-Verantwortliche der Vorstandsvorsitzende des Unternehmens ist.

b) Die Datenschutzerklärung definiert auch die Art und Weise der Verarbeitung personenbezogener Daten und die Verwaltung der mit der Verarbeitung personenbezogener Daten verbundenen Prozesse, um einen angemessenen Schutz dieser Daten zu gewährleisten.

c) Die Datenschutzerklärung legt die Pflichten und Verantwortlichkeiten der Personen fest, die für die Ausführung von Aufgaben im Zusammenhang mit den genannten Prozessen verantwortlich sind.

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

1. der Art der Verarbeitung (vollautomatisiert, teilautomatisiert oder nicht automatisiert),
2. der Form oder Weise der Verarbeitung (Papier, elektronisch oder auf andere Weise)
3. den Kanäle für den Fluss personenbezogener Daten,
4. der IT-Tools zur Verarbeitung personenbezogener Daten (Systeme, Apps, Programme),
5. des Verarbeitungszwecks,
6. der Quelle der personenbezogenen Daten,
7. der Kategorien personenbezogener Daten,
8. Die Richtlinie wird von allen Personen angewendet, die auf Wunsch des Verantwortlichen an der Verarbeitung personenbezogener Daten teilnehmen.

Kapitel II

Dateninventur. Grundsätze der Verarbeitung personenbezogener Daten. Verantwortung. Informationspflicht. Vereinbarungen und Kontakte mit externen Parteien.

§ 3

1. Die zu schützenden personenbezogenen Daten sind im Anhang dieser Datenschutzerklärung aufgeführt (Anhang Nr. 1 – Liste der Dateien mit personenbezogenen Daten).
2. Die Liste umfasst Datensätze, bei denen ein potenzielles Risiko einer Verletzung der Rechte und Freiheiten natürlicher Personen besteht.
3. Jeder Satz wird so beschrieben, dass eine Risikoanalyse möglich ist.
4. Die Beschreibung der Sätze enthält folgende Informationen:
   a) Satzname,
   b) Beschreibung der Verarbeitungszwecke,
   c) Art, Umfang, Kontext, dokumentierte personenbezogene Daten,
   d) Empfänger,
   e) Funktionsbeschreibung der Verarbeitungsvorgänge,
   f) für die Verarbeitung personenbezogener Daten,
   g) Informationen über die Notwendigkeit, eine Folgenabschätzung für den Satz durchzuführen,
   h) Kategorie der betroffenen Personen,
   i) Daten des Verantwortlichen – der Person, die für die gesammelten Daten verantwortlich ist,
   j) geplante Termine für die Datenlöschung,
   k) Rechtsgrundlage für die Verarbeitung.

§ 4

1. Der Verantwortliche und die verarbeitende Einheit stellen sicher, dass personenbezogene Daten gemäß den folgenden Regeln verarbeitet werden:
   a) gesetzeskonform und zuverlässig sowie für den Betroffenen transparent (Rechtskonformität, Verlässlichkeit und Transparenz),
   b) die Daten werden nur für bestimmte, eindeutige und legitime Zwecke erhoben (Zweckbindung),
   c) angemessen, relevant und nicht übermäßig für die Zwecke, für die sie verarbeitet werden (Datenminimierung),
   d) korrekt und ggf. aktualisiert (Korrektheit),
   e) in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht, und zwar nicht länger, als es für die Zwecke der Verarbeitung erforderlich ist, mit den in der Verordnung genannten Ausnahmen (Einschränkung der Aufbewahrung),
   f) in einer Weise, die eine angemessene Sicherheit personenbezogener Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Beschädigung, und zwar durch technische und organisatorische Maßnahmen, die den Risiken und der Kategorie der zu schützenden Daten angemessen sind und insbesondere den Schutz vor unbefugtem Zugriff oder unbefugtem Besitz (Integrität und Vertraulichkeit) gewährleisten,
   g) Die so genannte Informationspflicht - das Recht auf Auskunft, Datenübertragbarkeit, Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch - wurde gegenüber den betroffenen Personen ausgeübt.
2. Der Verantwortliche führt ein Verzeichnis der Verarbeitungstätigkeiten. Das Register ist auch eine Liste der vom Verantwortlichen verarbeiteten Dateien mit personenbezogenen Daten (Anhang Nr. 1).
3. Die verarbeitende Einheit führt ein Verzeichnis der Kategorien von Verarbeitungstätigkeiten.

§ 5

1. Die in diesem Dokument dargelegten Grundsätze sind alle Mitarbeiter von CreoConcept Sp.. z o.o. Sp. k., unabhängig von der Grundlage ihres Beschäftigungsverhältnisses, sowie Personen, die Tätigkeiten im Rahmen zivilrechtlicher Verträge ausüben und im Rahmen ihrer dienstlichen Aufgaben personenbezogene Daten verarbeiten, verpflichtet.
2. Jede Person, die Zugang zu persönlichen Daten bei CreoConcept Sp. z o.o. Sp. k. hat, ist verpflichtet, dieses Dokument zu lesen.

§ 6

1. Der Verantwortliche/Die verarbeitende Einheit ist für die Erteilung und Aufhebung von Berechtigungen zur Verarbeitung personenbezogener Daten in Papiersätzen und IT-Systemen verantwortlich.
2. Die verarbeitende Einheit und jede Person, die unter der Autorität des Verantwortlichen oder der verarbeitenden Einheit handelt und Zugriff auf personenbezogene Daten hat, verarbeitet diese nur auf Anweisung des Verantwortlichen, sofern dies nicht gesetzlich vorgeschrieben ist.
3. Satzgenehmigungen werden auf Antrag von Vorgesetzten (Abteilungsleiter/Direktoren) erteilt. Die Leiter der Organisationseinheiten legen den Umfang der Kompetenzen für die Verarbeitung personenbezogener Daten fest.
4. Berechtigungen definieren den Umfang von Datenoperationen.
5. Die Vollmachten sollten in den Personalakten der Mitarbeiter (bzw. in den Unterlagen der zuständigen Kommission) aufbewahrt, nur autorisierten Personen zugänglich gemacht und bei einer Änderung des Aufgabenbereichs aktualisiert werden.
6. Genehmigungen können ausnahmsweise auch in Form von Anordnungen erteilt werden, z. B. die Genehmigung zur Durchführung von Inspektionen, Audits oder zur Wahrnehmung behördlicher Aufgaben.
7. Der Verantwortliche führt Aufzeichnungen über autorisierte Personen, um den ordnungsgemäßen Zugriff auf Daten autorisierter Personen zu kontrollieren. Die Evidenz stellt einen Anhang zu dieser Richtlinie dar (Anhang Nr. 2 – Vorlage für Evidenz autorisierter Personen). Die Evidenz wird in elektronischer Form geführt.

§ 7

1. Die Berechtigung zur Verarbeitung personenbezogener Daten im IT-System wird auf Antrag der Vorgesetzten (Leiter/Abteilungsdirektoren) der mit der Datenverarbeitung beauftragten Personen erteilt. Wenn die Situation es erfordert, können auch Mitarbeiter einen solchen Antrag stellen. Eine Anfrage zur Bereitstellung einer Ressource im Zusammenhang mit personenbezogenen Daten wird per E-Mail an einen IT-Spezialisten innerhalb der Organisation gesendet und der Vorgesetzte wird ebenfalls darüber informiert (E-Mail DW).
2. Abteilungsleiter von Organisationseinheiten legen fest, auf welche IT-Systeme die Mitarbeiter ihrer Abteilungen Zugriff und welchen Kompetenzumfang sie haben.
3. Der in Abs. 1 genannte Anspruch erlischt mit der Einstellung der Verarbeitung personenbezogener Daten durch die Person, der der Anspruch gewährt wurde, oder mit der Beendigung des Beschäftigungsverhältnisses.

§ 8

1. Bei der Erhebung personenbezogener Daten von der betroffenen Person ist der Verantwortliche verpflichtet, folgende Informationen bereitzustellen:
   a) seine Identität und Kontaktdaten,
   b) Zwecke der Datenverarbeitung und Rechtsgrundlage der Verarbeitung,
   c) wenn die Verarbeitung personenbezogener Daten mit der Umsetzung rechtlich berechtigter Interessen des Verantwortlichen oder eines Dritten zusammenhängt, sind rechtlich berechtigte Interessen anzugeben.
   d) Informationen über die Empfänger personenbezogener Daten oder Kategorien von Empfängern,
   e) gegebenenfalls Informationen über die Absicht, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln,
   f) die Dauer, für die personenbezogene Daten gespeichert werden, und, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
   g) Informationen über das Recht, vom Verantwortlichen Zugang zu den personenbezogenen Daten der betroffenen Person zu verlangen, Berichtigung, Löschung oder Einschränkung der Verarbeitung oder das Recht, der Verarbeitung zu widersprechen, sowie das Recht auf Datenübertragung,
   h) Informationen über das Recht, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung vor dem Widerruf erfolgten Verarbeitung berührt wird (diese Regel gilt für die Verarbeitung von Daten aufgrund der Einwilligung für einen oder mehrere Zwecke und für die Verarbeitung besonderer Datenkategorien aufgrund der Einwilligung der betroffenen Person),
   i) Information über das Recht, eine Beschwerde bei der Aufsichtsbehörde einzureichen
   j) Informationen darüber, ob die Bereitstellung der Daten ein gesetzliches oder vertragliches Erfordernis oder eine Bedingung für den Abschluss eines Vertrags ist und ob die betroffene Person verpflichtet ist, die Daten bereitzustellen, und welche Folgen es haben kann, wenn sie dies nicht tut,
   k) Informationen zur automatisierten Entscheidungsfindung.
2. Erhält der für die Verarbeitung Verantwortliche personenbezogene Daten von einer anderen Quelle als der betroffenen Person, so ist er verpflichtet, der betroffenen Person alle unter Punkt. 1 aufgeführten Informationen zur Verfügung zu stellen, und zusätzlich: Informationen über die Quelle der personenbezogenen Daten zu geben.
3. Die Informationen, auf die in Punkt. 2 sind von dem für die Verarbeitung Verantwortlichen innerhalb einer angemessenen Frist nach Erhalt der Daten, spätestens jedoch innerhalb eines Monats unter Berücksichtigung der besonderen Umstände der Verarbeitung der personenbezogenen Daten zu erteilen. Sollen personenbezogene Daten zur Kommunikation mit der betroffenen Person verwendet werden, stellt der Verantwortliche die Daten spätestens zum Zeitpunkt der ersten Kommunikation bereit. Wenn geplant ist, personenbezogene Daten an einen anderen Empfänger weiterzugeben, spätestens dann, wenn sie erstmals weitergegeben werden.

§ 9

1. Personenbezogene Daten dürfen nur für die Zwecke verwendet werden, für die sie erhoben und verarbeitet wurden, und zwar für einen Zeitraum, der nicht länger ist, als es zur Erreichung der Zwecke, für die die Daten verarbeitet werden, erforderlich ist. Personenbezogene Daten können länger gespeichert werden, wenn sie ausschließlich für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Zwecke oder für statistische Zwecke verarbeitet werden.
2. Personenbezogene Daten sollten in einer Form gespeichert werden, die eine Identifizierung der betroffenen Personen unmöglich macht.
3. Die betroffene Person hat das Recht, vom Verantwortlichen die Berichtigung der sie betreffenden unrichtigen Daten zu verlangen.
4. Die betroffene Person hat das Recht, vom Verantwortlichen die sofortige Löschung der sie betreffenden personenbezogenen Daten zu verlangen, und der Verantwortliche ist verpflichtet, die Daten unverzüglich zu löschen, wenn eine der folgenden Bedingungen eintritt:
   a) personenbezogene Daten sind für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich,
   b) die betroffene Person hat ihre Einwilligung zur Verarbeitung widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
   c) die betroffene Person legt Widerspruch gegen das Gesetz ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor,
   d) personenbezogene Daten wurden unrechtmäßig verarbeitet,
   e) die Löschung personenbezogener Daten ist zur Erfüllung einer gesetzlichen Verpflichtung erforderlich,
   f) die personenbezogenen Daten wurden im Zusammenhang mit der Bereitstellung von Diensten der Informationsgesellschaft erhoben.
5. Die betroffene Person hat das Recht, in folgenden Fällen eine Einschränkung der Verarbeitung zu verlangen:
   a) die betroffene Person bestreitet deren Richtigkeit,
   b) die Verarbeitung ist unrechtmäßig und die betroffene Person widerspricht der Datenlöschung,
   c) Der für die Verarbeitung Verantwortliche benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht mehr, die betroffene Person benötigt sie jedoch zur Begründung, Geltendmachung oder Verteidigung von Rechtsansprüchen, Verteidigung von Ansprüchen.
   d) Die betroffene Person hat Widerspruch gegen die Verarbeitung eingelegt.
6. Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie dem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese personenbezogenen Daten einem anderen Verantwortlichen zu übermitteln ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden.
7. Die betroffene Person hat das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruht und ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

§ 10

1. Soll die Verarbeitung im Auftrag des Verantwortlichen erfolgen, darf dieser nur die Dienste von verarbeitenden Einheiten in Anspruch nehmen, die ausreichende Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen bieten, damit die Verarbeitung den Anforderungen dieser Verordnung entspricht und die Rechte der betroffenen Personen schützt.
2. Die Verarbeitung durch die verarbeitende Einheit erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments, das die verarbeitende Einheit und den Verantwortlichen bindet und den Gegenstand und die Dauer der Verarbeitung, ihre Art und ihren Zweck, die Art der personenbezogenen Daten und die Kategorien der betroffenen Personen, Pflichten usw. des Verantwortlichen festlegt.
3. Beim Abschluss von Verträgen mit externen Unternehmen, die Einfluss auf die Funktion wesentlicher Elemente des Informationssicherheitsmanagementsystems haben, empfiehlt sich der Abschluss eines Betrauungsvertrages.

Kapitel III

Vorgehensweise bei Gefährdung der Sicherheit personenbezogener Daten. Anweisungen zum Umgang mit Vorfällen.

§ 11

Das Verfahren definiert einen Katalog von Schwachstellen und Vorfällen, die die Sicherheit personenbezogener Daten gefährden, und beschreibt, wie darauf reagiert werden soll. Ziel ist es, die Auswirkungen von Sicherheitsvorfällen zu minimieren und das Risiko zukünftiger Bedrohungen und Vorfälle zu verringern.

1. Jeder Mitarbeiter des Unternehmens ist verpflichtet, jede Schwachstelle oder jeden Vorfall unverzüglich, spätestens jedoch innerhalb von 24 Stunden, seinem direkten Vorgesetzten zu melden. Handelt es sich bei dem Vorfall um ein Leck digitaler Daten, sollte auch die IT-Abteilung informiert werden.
2. Zu den typischen Sicherheitslücken im Bereich personenbezogener Daten zählen insbesondere:
   a) unzureichende physische Sicherung von Räumen, Geräten und Dokumenten,
   b) unsachgemäßer Schutz von IT-Geräten und Software vor Leckage, Diebstahl und Verlust personenbezogener Daten,
   c) Nichteinhaltung der Grundsätze des Schutzes personenbezogener Daten durch Mitarbeiter (z. B. Nichtbeachtung der Regel für einen sauberen Schreibtisch/Bildschirm, Passwortschutz, Nichtabschließung von Räumen, Schränken, Schreibtischen).
3. Zu den typischen Vorfällen im Bereich der Sicherheit personenbezogener Daten zählen insbesondere:
   a) Externe zufällige Ereignisse (Brand in einem Gebäude/Raum, Überschwemmung mit Wasser, Stromausfall, Kommunikationsverlust),
   b) Interne zufällige Ereignisse (Ausfälle von Servern, Computern, Festplatten, Software, Fehler von IT-Spezialisten und Benutzern, Datenverlust,
   c) Vorsätzliche Vorfälle (Einbruch in das IT-System oder die Räumlichkeiten, Diebstahl von Daten oder Geräten, Informationslecks, Weitergabe von Daten an Unbefugte, vorsätzliche Zerstörung von Dokumenten oder Daten, Einsatz von Viren und anderer schädlicher Software).
4. Wenn ein Vorfall festgestellt wird, führt der Verantwortliche (im Fall digitaler Daten einschließlich der IT-Abteilung) ein Untersuchungsverfahren durch, bei dem:
   a) er den Umfang und die Ursachen des Vorfalls sowie seine möglichen Folgen ermittelt,
   b) mögliche Disziplinarmaßnahmen einleitet,
   c) er daran arbeitet, den Betrieb der Organisation nach einem Vorfall wiederherzustellen,
   d) vorbeugende Maßnahmen empfiehlt, die darauf abzielen, ähnliche Vorfälle in der Zukunft zu verhindern oder Verluste zu reduzieren, wenn sie auftreten.
5. Der Verantwortliche dokumentiert alle oben genannten Verstöße gegen den Schutz personenbezogener Daten, einschließlich der Umstände des Verstoßes gegen den Schutz personenbezogener Daten, seiner Auswirkungen und der ergriffenen Abhilfemaßnahmen (Anhang Nr. 3 – Meldung eines Verstoßes gegen den Schutz personenbezogener Daten).

6. Es ist verboten, durch zur Datenverarbeitung berechtigte Personen bewusst oder unabsichtlich Vorfälle herbeizuführen.
7. Im Falle einer Verletzung des Schutzes personenbezogener Daten, die zu einer Verletzung der Rechte und Freiheiten natürlicher Personen führt, muss der Verantwortliche dies den Aufsichtsorganen unverzüglich – möglichst spätestens 72 Stunden nach Feststellung der Verletzung – melden.
8. Im Falle eines Vorfalls benachrichtigt der Verantwortliche die betroffenen Personen über den Vorfall.

Kapitel IV

Datenschutzbestimmungen, Schlüsselpolitik.

§ 12

1. Die Bestimmungen enthalten die grundlegenden Verpflichtungen zur Einhaltung der Grundsätze des Schutzes personenbezogener Daten gemäß den Bestimmungen für: Angestellte, Mitarbeiter, Angestellte von Dritten mit Zugang zu personenbezogenen Daten, die von dem für die Verarbeitung Verantwortlichen verarbeitet werden, Nutzer von IT-Systemen mit Zugang zu personenbezogenen Daten, die von dem für die Verarbeitung Verantwortlichen verarbeitet werden.
2. Nach der Unterrichtung über die Datenschutzgrundsätze müssen die Mitarbeiter ihre Kenntnis dieser Grundsätze bestätigen und erklären, dass sie sie anwenden (Anhang 5 - Erklärung über die Vertraulichkeit personenbezogener Daten, die im Rahmen ihrer Arbeit erhoben werden).

Kapitel V
Schulung/Audit

§ 13

1. Bevor die Verarbeitung personenbezogener Daten gestattet wird, ist jeder Nutzer verpflichtet, sich mit den diesbezüglichen Regelungen vertraut zu machen und sich über die sich daraus ergebenden Aufgaben und Pflichten zu informieren.
2. Alle Benutzer unterliegen regelmäßigen internen Schulungen.
3. Der Verantwortliche für personenbezogene Daten ist für die Durchführung der Schulung verantwortlich.
4. Im Falle einer internen Schulung zu den Grundsätzen des Schutzes personenbezogener Daten empfiehlt es sich, den Abschluss dieser Schulung zu dokumentieren.
5. Im Anschluss an die Schulung über die Datenschutzgrundsätze müssen die Teilnehmer ihre Kenntnis dieser Grundsätze bestätigen und erklären, dass sie sie anwenden.
6. Gemäß Art. 32 DSGVO hat der Verantwortliche die Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung regelmäßig zu prüfen, zu messen und zu bewerten.

Kapitel VI

Organisatorische und technische Maßnahmen zum Schutz personenbezogener Daten

§ 14

1. Gemäß Artikel 32 der DSGVO muss der Verantwortliche sicherstellen, dass die Verfügbarkeit und der Zugriff auf personenbezogene Daten schnell wiederhergestellt werden können. Im Falle eines physischen oder technischen Vorfalls.
2. Als Anhang wurden Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugriffs darauf entwickelt (Anhang Nr. 10 – Geschäftskontinuitätsplan).

Kapitel VII

Liste der Räumlichkeiten, in denen Dokumente mit personenbezogenen Daten bei CreoConcept Sp. z o.o. Sp. k.

§ 15

Die Liste der Räumlichkeiten von CreoConcept Sp. z o.o. Sp. k. in denen Vorgänge mit personenbezogenen Daten durchgeführt werden, einschließlich besonders geschützter Räume, ist eine Anlage zu dieser Richtlinie:

Anlage Nr. 4 – Liste der Räumlichkeiten.

Anhang Nr. 1 – Liste der vom Verantwortlichen erfassten personenbezogenen Datensätzen
Anlage Nr. 2 – Muster der Evidenz der automatisierten Personen
Anhang Nr. 3 – Meldung der Verletzung des Schutzes personenbezogener Daten
Anhang Nr. 4 - Liste der Räumlichkeiten
Anlage Nr. 5 – Erklärung zur Geheimhaltung der im Rahmen der Arbeit erhobenen personenbezogenen Daten

creo concept®

PERFECT WALL

Datenschutzerklärung bei CreoConcept Sp. z o.o. Sp. k. wurde am 8. Dezember 2023 verabschiedet.

THINK CREO