Datenschutzpolitik bei PROTEKTOR-POLSKA Sp. z o.o.

I. Allgemeine Bestimmungen

§1

Der Zweck der Datenschutzpolitik in Bezug auf Personenbezogene Daten PROTEKTOR-POLSKA Sp. z o. o. (nachstehend SICHERHEITSPOLITIK genannt) ist es, eine optimale und mit den Anforderungen der geltenden Rechtsakte übereinstimmende Art und Weise der Verarbeitung von Informationen mit personenbezogenen Daten zu erreichen.

§2

Die Datenschutzpolitik wurde auf der Grundlage der Anforderungen entwickelt, die u.a. in folgenden Vorschriften festgeschrieben sind:
(a) 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 / Amtsblatt der EU.L Nr.119, S.1/,
b) das Gesetz vom 10. Mai 2018 über den Schutz personenbezogener Daten (GBl. 2018, Pos. 1000).

§3

Der Schutz personenbezogener Daten wird durch physische, organisatorische, Systemsoftware-, Anwendungs- und Benutzergarantien umgesetzt, die in einem angemessenen Verhältnis zu dem Risiko einer Sicherheitsverletzung der im Rahmen der Geschäftstätigkeit verarbeiteten personenbezogenen Daten stehen.

§4

Der Schutz der bei PROTEKTOR-POLSKA Sp. z o.o. verarbeiteten personenbezogenen Daten ist als Gewährleistung ihrer Vertraulichkeit, Integrität, Verantwortlichkeit und Verfügbarkeit auf einem angemessenen Niveau zu verstehen. Das Maß der Sicherheit ist das akzeptierbare Risiko in Bezug auf den Schutz personenbezogener Daten.
2. Die angewandten Schutzmaßnahmen sollen die oben genannten Ziele erreichen und gewährleisten:
a) Datenvertraulichkeit - die Daten dürfen Unbefugten nicht zugänglich gemacht werden,
b) Datenintegrität - personenbezogene Daten dürfen nicht auf unbefugte Weise verändert oder zerstört werden,
c) Verantwortlichkeit der Daten - die Handlungen einer Person können eindeutig nur dieser Person zugeordnet werden,
d) Systemintegrität - die Integrität des Systems, die Unmöglichkeit jeglicher Manipulation, ob absichtlich oder versehentlich,
e) Informationsverfügbarkeit - die Gewährleistung, dass befugte Personen bei Bedarf Zugang zu Informationen und zugehörigen Ressourcen haben,
f) Risikomanagement - der Prozess der Identifizierung, Kontrolle und Minimierung oder Beseitigung von Sicherheitsrisiken, die sich auf Informationssysteme zur Verarbeitung personenbezogener Daten auswirken können.

§5

Der Datenschutzbeauftragte bei PROTEKTOR-POLSKA Sp. z o.o. ist Herr Sebastian Piórkowski.

II. Begriffsbestimmungen

§6

Die folgenden in der Datenschutzpolitik verwendeten Begriffe sind zu verstehen als:
a) Datenschutzbeauftragter - eine natürliche oder juristische Person, Behörde, Einheit oder sonstige Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet;
b) Gesetz - das Gesetz vom 10. Mai 2018 über den Schutz personenbezogener Daten (Gesetzblatt 2018, Pos. 1000),
c) Datenschutzgesetz- Verordnung des Europäischen Parlaments und des Rates /EU/ 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG /Amtsblatt der EU.L Nr. 119, S. 1/,
d) personenbezogene Daten - alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen,
e) Datei mit personenbezogenen Daten - ein strukturierter Satz personenbezogener Daten, der nach bestimmten Kriterien zugänglich ist,
f) Datenverarbeitung - ein mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder eine Reihe von Vorgängen im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Aufbewahrung, die Verarbeitung, die Verknüpfung, die Übermittlung, die Veränderung, der Zugang und die Löschung, die Vernichtung usw.
g) Computersystem - eine Gesamtheit von zusammenwirkenden Geräten, Programmen, Informationsverarbeitungsverfahren und Softwaretools, die zur Verarbeitung personenbezogener Daten verwendet werden,
h) traditionelles System - eine Gesamtheit von organisatorischen Verfahren, die sich auf die mechanische Verarbeitung von Informationen beziehen, sowie von Geräten und festen Einrichtungen, die für die Verarbeitung personenbezogener Daten auf Papier verwendet werden,
i) Datensicherheit im EDV-System - Umsetzung und Betrieb geeigneter technischer und organisatorischer Maßnahmen, die den Schutz der Daten vor unbefugter Verarbeitung gewährleisten,
j) für das EDV-System Verantwortlicher - eine oder mehrere Personen, die von dem für die Verarbeitung Verantwortlichen ermächtigt sind, die EDV-Systeme zu verwalten und zu betreiben,
k) Empfänger - eine natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, der personenbezogene Daten unter anderem auf der Grundlage einer Betrauungsvereinbarung mitgeteilt werden,
l) Dritter - eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle außer der betroffenen Person, die personenbezogene Daten unter der Aufsicht des für die Verarbeitung Verantwortlichen verarbeiten darf,
m) Benutzerkennung (Login) - eine Folge von Buchstaben, Ziffern oder anderen Zeichen, die die zur Verarbeitung personenbezogener Daten im Computersystem berechtigte Person eindeutig identifiziert,
n) Passwort - eine Abfolge von Buchstaben, Ziffern oder anderen Zeichen, die der Benutzerkennung zugeordnet ist und die der betroffenen Person bekannt ist.

III. Anwendungsbereich

§7

1. In der Firma PROTEKTOR-POLSKA Sp. z o. o. werden personenbezogene Daten in Personendateien gesammelt und verarbeitet:
a) Mitarbeiter,
b) Bewerbern,
c) Kunden,
d) Auftragnehmer.
Die oben genannten Informationen werden sowohl in Form von traditionellen als auch von elektronischen Unterlagen verarbeitet.

2. Das Sicherheitskonzept enthält Regelungen zu den implementierten technischen und organisatorischen Sicherheitsmaßnahmen, um den Schutz der verarbeiteten personenbezogenen Daten zu gewährleisten.

3. Die Firma PROTEKTOR-POLSKA Sp. z o.o. führt ein Verzeichnis der Personen, die zur Verarbeitung personenbezogener Daten berechtigt sind, sowie ein Verzeichnis der Tätigkeiten zur Verarbeitung personenbezogener Daten und der Verfahren, die im Falle einer Verletzung des Schutzes personenbezogener Daten anzuwenden sind.

§8

Die Datenschutzpolitik gilt insbesondere für:
a) personenbezogene Daten, die im System verarbeitet werden: Invoice iBiznes, Open Office, Symfonia, Payer,
b) Alle Informationen über Daten von Mitarbeitern, Bewerbern, Kunden und Auftragnehmern,
c) Empfänger von personenbezogenen Daten, denen personenbezogene Daten zur Verarbeitung auf der Grundlage von Betrauungsverträgen übermittelt wurden, z. B. Buchhaltungsbüro, Anwaltskanzlei, IT-Spezialist,
d) Informationen über die Sicherheit personenbezogener Daten, einschließlich insbesondere der Kontonamen und Passwörter in Systemen zur Verarbeitung personenbezogener Daten,
e) ein Verzeichnis der Dritten, z. B. Mitarbeiter, externe Unternehmen, Wirtschaftsprüfungsgesellschaften, die von dem für die Verarbeitung Verantwortlichen zur Verarbeitung personenbezogener Daten ermächtigt wurden,
f) sonstige Dokumente, die personenbezogene Daten enthalten.

§9

1. Die in der Datenschutzpolitik und anderen damit zusammenhängenden Dokumenten festgelegten Bereiche des Schutzes personenbezogener Daten gelten für:
a) alle bestehenden, derzeit implementierten oder künftigen IT- und papiergestützten Systeme, in denen geschützte personenbezogene Daten verarbeitet werden,
b) alle Standorte, Gebäude und Räumlichkeiten, an denen geschützte Daten verarbeitet werden oder werden sollen,
c) alle Mitarbeiter, Auszubildenden und sonstigen Personen mit Zugang zu geschützten Daten.

2. Alle Beschäftigten, Auszubildenden und sonstigen Personen mit Zugang zu geschützten personenbezogenen Daten sind verpflichtet, die in der Datenschutzpolitik sowie in anderen damit zusammenhängenden Dokumenten dargelegten Grundsätze anzuwenden.

IV. Liste der Ablagesysteme für personenbezogene Daten

§ 10

Personenbezogene Daten werden in Gruppen gesammelt:
1. Verzeichnis von Personen, die berechtigt sind, personenbezogene Daten zu verarbeiten,
2. Personalakten der Mitarbeiter,
3. Register der Krankschreibungen,
4. Ärztliche Überweisungen ,
5. Urlaubskarteien, Arbeitszeitkonten, Freistellungen,
6. Dienstreisenkarteien,
7. Lohn- und Gehaltsabrechnungen der Mitarbeiter.
8. Versicherungserklärungen der Arbeitnehmer,
9. Sozialversicherungserklärungen und -nachweise für Arbeitnehmer,
10. Steuererklärungen der Arbeitnehmer,
11. Unfallregister,
12. Zivilrechtliche Verträge,
13.Verträge mit Kontrahenten,
14. Kundenregister,
15. Archivdokumente.
Die vorgenannten personenbezogenen Daten werden auf herkömmliche Weise und mit Hilfe eines IT-Systems verarbeitet.

V. Verzeichnis der Gebäude und Räumlichkeiten, in denen die Verarbeitung personenbezogener Daten erfolgt

§ 11

Die personenbezogenen Daten werden in einem Gebäude in Bydgoszcz in der ul. Kościuszki 27/ 610 und in Żnin in der ul. Dworcowa 27A verarbeitet.

VI. Organisatorische und technische Garantien für personenbezogene Daten

§ 12

1. Organisatorische Schutzmaßnahmen:
a) Es wurde ein Sicherheitskonzept für die Verarbeitung personenbezogener Daten ausgearbeitet und umgesetzt,
b) eine Anweisung für die Verwaltung des für die Verarbeitung personenbezogener Daten in der Organisation verwendeten IT-Systems - die Anlage Nr. 1 bildet - erstellt und umgesetzt worden ist,
c) ein Verfahren für den Umgang mit einer Verletzung des Schutzes personenbezogener Daten geschaffen wurde - als Anlage 2 beigefügt,
d) nur Personen, die von dem für die Verarbeitung personenbezogener Daten Verantwortlichen oder einer von dem für die Verarbeitung Verantwortlichen beauftragten Person ermächtigt wurden, dürfen die Daten verarbeiten,
e) die mit der Verarbeitung der Daten beauftragten Personen mit den Vorschriften über den Schutz personenbezogener Daten und den Vorschriften über die Sicherheit des IT-Systems vertraut gemacht worden sind,
f) Die mit der Verarbeitung personenbezogener Daten befassten Personen sind verpflichtet, diese vertraulich zu behandeln,
g) Die Verarbeitung personenbezogener Daten erfolgt unter Bedingungen, die die Daten vor unbefugtem Zugriff schützen,
h) Unbefugten ist der Aufenthalt in den Räumen, in denen personenbezogene Daten verarbeitet werden, nur in Anwesenheit einer mit der Verarbeitung von personenbezogenen Daten beauftragten Person und unter Bedingungen gestattet, die die Datensicherheit gewährleisten,

i) Dokumente und Informationsträger, die personenbezogene Daten enthalten und vernichtet werden sollen, sind mit dafür vorgesehenen Geräten zu neutralisieren oder so zu verändern, dass ihr Inhalt nicht rekonstruiert werden kann.

2. Technische Sicherheitsvorkehrungen
a) Die Computerarbeitsplätze sind mit einem individuellen Virenschutz ausgestattet,
b) die Computer sind durch eine individuelle Benutzerkennung und zyklische Änderung des Passworts gegen die Nutzung durch Personen geschützt, die nicht zur Verarbeitung personenbezogener Daten berechtigt sind,

3. Physische Schutzmaßnahmen:
a) Der Bereich, in dem personenbezogene Daten verarbeitet werden, wird rund um die Uhr überwacht,
b) der Bereich, in dem personenbezogene Daten verarbeitet werden, wird rund um die Uhr durch eine physische Sicherung des Gebäudes abgedeckt,
c) Geräte, die zur Verarbeitung personenbezogener Daten verwendet werden, sind in verschließbaren Räumen unterzubringen,
d) Dokumente, die personenbezogene Daten enthalten, werden in verschließbaren Schränken aufbewahrt.

VII. Aufgaben des für die Verarbeitung personenbezogener Daten Verantwortlichen.

§ 14

1. Die wichtigsten Aufgaben des für die Verarbeitung personenbezogener Daten Verantwortlichen sind:
a) die Organisation der Sicherheit und des Schutzes personenbezogener Daten gemäß den Anforderungen des Datenschutzgesetzes und des Gesetzes zum Schutz personenbezogener Daten,
b) Gewährleistung der Datenverarbeitung gemäß den Bestimmungen des Sicherheitskonzepts und anderer interner Dokumente,
c) Führung eines Verzeichnisses der zur Verarbeitung personenbezogener Daten befugten Personen,
d) Durchführung von Untersuchungen im Falle von Verletzungen des Schutzes personenbezogener Daten, e) Überwachung der Sicherheit personenbezogener Daten,
f) die Einleitung und Durchführung von Maßnahmen zur Verbesserung des Schutzes personenbezogener Daten.

2 Der Verantwortliche für Personendaten ist verantwortlich für:
a) die laufende Überwachung und Sicherstellung der Kontinuität des Betriebs des IT-Systems und der Datenbanken, b) die Optimierung der Leistung des IT-Systems, der Installationen und Konfigurationen der Netzwerk- und Serverhardware,
c) die Installation und Konfiguration der System- und Netzsoftware,
d) Konfiguration und Verwaltung von System-, Netz- und Datensicherheitssoftware zur Verhinderung von unberechtigtem Zugriff,
e) die Überwachung der Notstromversorgung von Computern und anderen Geräten, die die Sicherheit der Datenverarbeitung beeinträchtigen,
f) Zusammenarbeit mit den Lieferanten von Dienstleistungen und Netz- und Serverausrüstungen und Sicherstellung von Aufzeichnungen über den Schutz personenbezogener Daten,
g) Verwaltung von Notkopien von System- und Netzsoftwarekonfigurationen,
h) Verwaltung von Sicherungskopien personenbezogener Daten und von Ressourcen, die deren Verarbeitung ermöglichen,
i) Abwehr von Versuchen, die Informationssicherheit zu verletzen,
j) Gewährung streng definierter Zugriffsrechte auf Informationen in einem bestimmten System,

k) Änderung oder Verbesserung von Sicherheitsverfahren und Sicherheitsstandards,
l) Verwaltung von Lizenzen und der damit verbundenen Verfahren,
m) Durchführung von Antivirenmaßnahmen.

VIII. Betrauung mit der Verarbeitung personenbezogener Daten

§ 15 1.

1. Der Datenschutzbeauftragte kann die Verarbeitung personenbezogener Daten nur durch einen schriftlich abgeschlossenen Vertrag unter Einhaltung der in Artikel 28 des Datenschutzgesetzes für solche Verträge genannten Anforderungen an eine andere Stelle übertragen.

Bevor er die Verarbeitung personenbezogener Daten in Auftrag gibt, holt der für die Verarbeitung Verantwortliche so weit wie möglich Informationen über die bisherige Praxis der mit der Verarbeitung personenbezogener Daten betrauten Person in Bezug auf die Sicherheit personenbezogener Daten ein.

IX. Schlussbestimmungen

§ 16 1.

1. Jeder Benutzer muss, bevor er mit IT-Systemen, die personenbezogene Daten verarbeiten, oder mit Dateien mit personenbezogenen Daten in Papierform arbeiten darf, im Bereich des Schutzes personenbezogener Daten in elektronischen und Papierdateien geschult werden.

2. Die Schulung liegt in der Verantwortung des für die Verarbeitung personenbezogener Daten Verantwortlichen.

3. Der Umfang der Schulung umfasst die Inkenntnissetzung des Benutzers mit den Bestimmungen des Gesetzes über den Schutz personenbezogener Daten und der auf seiner Grundlage erlassenen Durchführungsbestimmungen sowie mit der Sicherheitspolitik und anderen damit zusammenhängenden Dokumenten, die bei dem für die Verarbeitung personenbezogener Daten Verantwortlichen gelten,

4. Die Schulung wird mit der Unterzeichnung einer Erklärung durch den Schulungsteilnehmer abgeschlossen, in der er erklärt, dass er an der Schulung teilgenommen und sie verstanden hat und dass er sich verpflichtet, die während der Schulung vorgestellten Grundsätze des Schutzes personenbezogener Daten einzuhalten.