Odobreno od strane / Approved by: _____

Dragana Davidović, direktor / director of DPM Avala doo Beograd,
DPM Crni Vrh d.o.o. Beograd, Dunav Minerals doo Beograd

Dana: 25.11.2025. godine
Date: 25th November 2025

Privacy Standard *Standard privatnosti*

Document Number: GRP-ST-LEG-19 V.1.1

Broj dokumenta: GRP-ST-LEG-19 V.1.1

Vlasnik Politike: Potpisano

Policy Document Owner: Signed

Politiku odobrio: Potpisano

Policy Document Approver: Signed

DPM METALS

Privacy Standard / Standard privatnosti

Document Administration / Administracija dokumenta

Document Management / Upravljanje dokumentom

Document Owner (Name, Title) / Vlasnik dokumenta (Ime, funkcija)	Kelly Stark-Anderson, Executive Vice President, Corporate Affairs, General Counsel and Corporate Secretary / Kelly Stark-Anderson, izvršni potpredsednik za korporativne poslove, generalni savetnik i korporativni sekretar
Document Administrator (Name,Title) / Administror dokumenta (Ime, funkcija)	Petya Dombalova, Director Legal & Compliance / Petya Dombalova, direktor službe za pravna pitanja i usklađenost
Document Approver (Group or Name, Title) / Dokument odobrava (Grupa ili ime, funkcija)	David Rae, President and Chief Executive Officer / David Rae, predsednik i glavni izvršni direktor
Adoption Date / Datum usvajanja	May 1, 2025 / 1. maj 2025.
Initial Effective Date / Inicijalni datum stupanja na snagu	June 1, 2025 / 1. jun 2025.
Last Amended Date / Datum poslednje izmene	September 12, 2025 / 12. septembar 2025.
Effective Date of the Last Amendment / Datum stupanja na snagu poslednje izmene	September 12, 2025 / 12. septembar 2025.
Next Review Date / Datum naredne revizije	May 1, 2027 / 1. maj 2027. godine

Version History / Pregled izmena

Version / Verzija	Description of Version Changes/ Opis izmene
1.0	Initial / Prvo izdanje
1.1	Revised (2025: company name and logo changes) / Revidirano (2025: promena naziva i logotipa kompanije)

Related Documents / Povezani dokumenti

Document Number / Broj dokumenta	Document Title / Naziv dokumenta
GRP-PO-LEG-01 V.10	*Code of Business Conduct and Ethics / Kodeks poslovnog ponašanja i poslovne etike*
GRP-PO-IT-01 V.3.1	*Information Protection Policy / Politika zaštite informacija*

GRP-ST-IT-06 V.2.0	*Information Categorization Standard / Standard za kategorizaciju informacija*
GRP-ST-IT-05 V.1.0	*Data Loss Prevention Standard (under Revision) / Standard za prevenciju gubitka podataka (u fazi revizije)*
GRP-ST-IT-04 V.2.0	*Information Retention, Recovery and Sanitization Standard / Standard za čuvanje, oporavak i brisanje/uništavanje informacija*
GRP-ST-LEG-17 V.1.1	*Subsidiary Governance Standard / Standard korporativnog upravljanja podružnicama*
GRP-PR-IT-12 V.2.0	*Acceptable Mobile Device Use Procedure / Procedura za prihvatljivo korišćenje mobilnih uređaja*
GRP-PR-IT-09 V.2.1	*Acceptable Email Use Procedure / Procedura za prihvatljivo korišćenje elektronske pošte*
GRP-PR-IT-11 V.2.0	*Internet Acceptable Use Procedure / Procedura za prihvatljivo korišćenje interneta*

Table of Contents / Sadržaj

1. Defined Terms / Definicije pojmova

The following terms and acronyms are integral to the understanding of this Standard and have the meanings assigned within this Section or as referenced herein:

Sledeći pojmovi i skraćenice su neophodni za razumevanje ovog Standarda i imaju značenje dodeljeno u okviru ovog dela ili kako je ovde navedeno:

Term / Pojam	Definition / Definicija
Board Member(s) / Član(ovi) Borda	As a group or individually, any member of the DPM Board or any member of the board of directors of any DPM subsidiary or any individual delegated equivalent authority by the shareholder(s) of such entity. / Kao grupa ili pojedinac, svaki član borda DPM-a ili neki član borda direktora iz bilo koje podružnice DPM-a ili pojedinci sa ekvivalentnim ovlašćenjima od strane akcionara takvog entiteta.
Business Function and Business Function Head / Poslovna funkcija i rukovodilac poslovne funkcije	A team of Employees with a designated cost centre, or multiple cost centres, accountable for establishing and maintaining business systems, including through Policy Documents, internal controls, and applications; managing or supporting implementation; and providing ongoing support to other Employees and relevant Third Parties. The Business Function Head thereof is the individual accountable for the Business Function. / Tim zaposlenih sa određenim troškovnim centrom, ili sa više njih, odgovorni za uspostavljanje i održavanje poslovnih sistema, uključujući strateške dokumente, interne kontrole i primene; upravljanje i pružanje podrške implementaciji; pružanje tekuće podrške drugim zaposlenima i relevantnim Trećim licima. Rukovodilac poslovne funkcije je pojedinac odgovoran za poslovnu funkciju.
Business Unit and Business Unit Head / Poslovna jedinica i rukovodilac poslovne jedinice	DPM and each of its Subsidiaries, individually. The Business Unit Head is the individual accountable for the Business Unit. / DPM i svaka od njegovih Podružnica, pojedinačno. Rukovodilac poslovne jedinice je lice odgovorno za poslovnu jedinicu.
Collect, Collected or Collection / Prikupiti, prikupio ili prikupljanje	The gathering, acquiring or otherwise obtaining, recording, and / or compiling of Personal Information. / Prikupljanje, sticanje ili drugo dobijanje, evidentiranje i/ili sastavljanje Podataka o ličnosti.
Company or Group / Kompanija ili Grupa	DPM and all its directly and indirectly owned Subsidiaries, collectively. / DPM i sve njene podružnice u direktnom i indirektnom vlasništvu, zajedno.

Consent / Saglasnost	An agreement to the Collection, Use, and / or Disclosure of Personal Information. / Saglasnost za prikupljanje, korišćenjem i/ili otkrivanjem Podataka o ličnosti.
Corporate Compliance Officer / Službenik za korporativnu usklađenost	The Corporate Director Legal & Compliance or any other Employee appointed as Corporate Compliance Officer by the DPM Board. / Direktor Sektora za pravne poslove i usklađenost ili bilo koji drugi Zaposleni kojeg Bord DPM-a imenuje za Službenika za korporativnu usklađenost.
Data Processing Agreement or DPA / Ugovor o obradi podataka ili DPA	A legally binding document that outlines the terms and conditions under which Personal Information is Processed by a Third-Party Processor on behalf of the Company including but not limited to the rights and obligations of both the Third-Party Processor and the Company. / Pravno obavezujući dokument koji definiše uslove pod kojima Podatke o ličnosti obrađuje Treća strana Obrađivač u ime Kompanije, uključujući, ali ne ograničavajući se na prava i obaveze kako Treće strane Obrađivača, tako i Kompanije.
Disclose, Disclosed or Disclosure / Otkriti, otkrio ili otkrivanje	The transmission, dissemination, or otherwise making available of Personal Information. / Prenos, distribucija ili stavljanje na raspolaganje Podataka o ličnosti
DPM	DPM Metals Inc. (the parent company incorporated in Canada). / DPM Metals Inc. (matična kompanija sa sedištem u Kanadi).
Employee / Zaposleni	An individual engaged by the Company on a full-time or part-time permanent, fixed term, or temporary basis, as well as a secondment employee, student, intern, or apprentice. For clarity, Employees also include Company Officers. For the definition of "Company Officer", refer to the *Subsidiary Governance Standard.* / Lice koje zapošljava Kompanija na puno ili skraćeno radno vreme za stalno, na određeno ili na privremenoj osnovi, kao i privremeno premešteni zaposleni, student, lice na praksi ili pripravnik. Radi izbegavanja nedoumice, zaposleni takođe podrazumevaju službenike. Definiciju *službenika* pogledati u *Standardu korporativnog upravljanja podružnicama.*
Group Privacy Officer / Službenik za privatnost Grupe	The Corporate Compliance Officer or any other person designated by DPM's Chief Executive Officer. / Službenik za korporativnu usklađenost ili bilo koja druga osoba koju imenuje Izvršni direktor DPM-a.
Information Subject / Subjekt podataka	The identified or identifiable living individual to whom Personal Information relates. / Identifikovano ili prepoznatljivo živo fizičko lice na koje se odnose Podaci o ličnosti.

IT Privacy Coordinator / IT koordinator za privatnost	A member of the Company's Technology Function, designated by the VP Supply Chain & Technology, to carry out the Privacy-related accountabilities set out in this Standard. / Član Sektora za tehnologiju Kompanije, kojeg imenuje Potpredsednik za lanac snabdevanja i tehnologiju, za vršenje odgovornosti u vezi sa privatnošću, definisanih u ovom Standardu.
Personal Information / Podaci o ličnosti	Any information that identifies an Information Subject, or information relating to an Information Subject, that the Company can directly or indirectly identify from the information alone or combined with other identifiers that the Company possesses or can reasonably access. This includes identifiers such as name, identification number, location data, online identifier, factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that Information Subject. / Bilo koja informacija koja identifikuje Subjekta podataka, ili informacija koja se odnosi na Subjekta podataka, a kojeg Kompanija može direktno ili indirektno da identifikuje iz same informacije ili u kombinaciji sa drugim identifikatorima koje Kompanija poseduje ili kojima može razumno pristupiti. Ovo uključuje identifikatore kao što su ime, identifikacioni broj, podaci o lokaciji, onlajn identifikator, faktore specifične za fizički, fiziološki, genetski, mentalni, ekonomski, kulturološki ili društveni identitet tog Subjekta podataka.
Personal Information Breach / Povreda podataka o ličnosti	Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Information or the physical, technical, administrative or organizational safeguards that the Company or its Third-Party Processor put in place to protect it. The loss, or unauthorized access, disclosure or acquisition, of Personal Information is a Personal Information Breach. / Bilo koja radnja ili propust koji ugrožava bezbednost, poverljivost, integritet ili dostupnost Podataka o ličnosti, ili fizičke, tehničke, administrativne ili organizacione mere zaštite koje su Kompanija ili Treća strana Obrađivač uspostavili za njihovu zaštitu. Gubitak, ili neovlašćeni pristup, otkrivanje ili sticanje Podataka o ličnosti predstavlja Povredu podataka o ličnosti.
Policy Document / Politika (dokument)	Each or any of a Policy, Standard, Procedure or Guideline created by or for the Company or one or more of its Business Units. / Politika, Standard, Procedura ili Smernica koju je kreirala Kompanija ili su kreirani za Kompaniju ili jednu ili više njenih Poslovnih jedinica.

Privacy / Privatnost	The protection of Personal Information Processed by or on behalf of the Company. / Zaštita Podataka o ličnosti koje obrađuje Kompanija ili se obrađuju u njeno ime.
Privacy Laws / Zakoni o privatnosti	All laws and regulations pertaining to Personal Information protection, that are applicable to the Company, including but not limited to the *Canadian Personal Information Protection and Electronic Documents Act* (PIPEDA) and the European Union *General Data Protection Regulation* (GDPR). / Svi zakoni i uredbe koji se odnose na zaštitu Podataka o ličnosti, a koji su primenjivi na Kompaniju, uključujući, između ostalog, kanadski Zakon o zaštiti podataka o ličnosti i elektronskim dokumentima (PIPEDA) i Opštu uredbu Evropske unije o zaštiti podataka (GDPR).
Privacy Liaison / Saradnik za privatnost	The Head of, or an Employee designated by the Head of, the Business Function Collecting or otherwise Processing Personal Information to carry out the Privacy - related accountabilities set out in this Standard. / Rukovodilac, ili Zaposleni kojeg imenuje Rukovodilac, Poslovne funkcije koja prikuplja ili na drugi način obrađuje Podatke o ličnosti u cilju vršenja odgovornosti u vezi sa privatnošću definisanih u ovom Standardu.
Privacy Professionals / Stručnjaci za privatnost	A member of the Legal & Compliance Function at each respective Business Unit, who has been assigned Privacy accountabilities for the Business Unit by the Business Unit Head. / Član Sektora za pravne poslove i usklađenost u svakoj relevantnoj Poslovnoj jedinici, kome je Rukovodilac Poslovne jedinice dodelio odgovornosti u vezi sa privatnošću za tu Poslovnu jedinicu.
Process, Processed or Processing / Obrađivati, obradio ili obrada	In the context of Personal Information, the verb "to process" includes any activity that involves the use of Personal Information (whether through manual or automated means) such as the Collection, recording, storage, retrieval, use (i.e., organization, adaption, alteration, consultation, alignment, or combination), Disclosure and destruction of Personal Information. Processing also includes transmitting or transferring Personal Data to Third Parties. / U kontekstu Podataka o ličnosti, glagol „obrađivati" uključuje svaku aktivnost koja podrazumeva korišćenje Podataka o ličnosti (bilo ručnim ili automatizovanim sredstvima), kao što su prikupljanje, evidentiranje, skladištenje, preuzimanje, korišćenje (tj. organizovanje, prilagođavanje, izmena, konsultovanje, usklađivanje ili kombinovanje), otkrivanje i uništavanje Podataka o ličnosti. Obrada takođe uključuje prenos Podataka o ličnosti Trećim stranama.

Subsidiary/Podružnica	Includes each entity in which DPM holds, directly or indirectly, over 50% ownership of the voting shares or an interest which allows DPM to exert direct or indirect control over the entity (collectively referred to as Subsidiaries). For clarity, the Private English Language Secondary School Chelopech EOOD is not included in this definition as it is subject to the *Bulgarian Education Act*. / Uključuje svaki entitet u kojem DPM poseduje, direktno ili indirektno, više od 50% vlasništva nad akcijama sa pravom glasa ili udeo koji DPM-u omogućava direktnu ili indirektnu kontrolu nad entitetom (zajednički Podružnice). Radi jasnoće, Privatna srednja škola engleskog jezika Čelopeč EOOD nije uključena u ovu definiciju jer podleže Bugarskom zakonu o obrazovanju.
Third Party / Treće lice	An individual, company, or other entity, that is interested in entering or has an existing business relationship with the Company. Third Parties include, but are not limited to, suppliers, contractors, advisors, consultants, agents, brokers, lobbyists, donation and sponsorship beneficiaries, customers, and joint venture, merger, and acquisition partners. / Lice, kompanija ili drugi entitet, koji je zainteresovan za zasnivanje ili ima postojeći poslovni odnos sa Kompanijom. Treća lica uključuju, ali nisu ograničena na, dobavljače, izvođače, savetnike, konsultante, agente, brokere, lobiste, korisnike donacija i sponzorstava, klijente, kao i partnere u zajedničkim ulaganjima, spajanjima i pripajanjima.
Third-Party Processor / Treća strana Obrađivač	Third-Party Processors are Third Parties engaged by the Company to Process the Personal Information as further set out in Section 4.7. / Treće strane Obrađivači su Treća lica koje Kompanija angažuje da obrađuju Podatke o ličnosti kao što je dalje navedeno u Odeljku 4.7.

2. Purpose and Scope / Svrha i područje primene

The purpose of this Privacy Standard (this Standard) is to facilitate the protection of Personal Information the Company Collects and otherwise Processes (including the Personal Information of Employees, Board Members, and Third-Party Information Subjects) in accordance with applicable legal requirements.

Svrha ovog Standarda o privatnosti (u daljem tekstu: Standard) je da omogući zaštitu Podataka o ličnosti koje Kompanija prikuplja i na drugi način obrađuje (uključujući Podatke o ličnosti Zaposlenih, Članova Borda i Subjekte podataka treća lica) u skladu sa važećim zakonskim zahtevima.

This Standard sets out the Company's approach to using, managing and protecting Personal Information, regardless of the medium on which that information is stored, and is applicable to Board Members, Employees and Third Parties, who Process Personal Information at the request and/or on behalf the Company.

Ovaj Standard utvrđuje pristup Kompanije korišćenju, upravljanju i zaštiti Podataka o ličnosti, bez obzira na medij na kojem su te informacije sačuvane, i primenjiv je na Članove Borda, Zaposlene i Treća lica koja Obrađuju Podatke o ličnosti na zahtev i/ili u ime Kompanije.

3. Overarching Requirements / Sveobuhvatni zahtevi

The Company operates across different jurisdictions, each with its own set of Privacy Law requirements. It is committed to complying with all applicable Privacy Laws and adhering to the principles outlined in the Information Protection Policy. This Standard establishes the requirements that will be uniformly applied across all jurisdictions where the Company conducts business. In instances where local Privacy Laws impose additional or more stringent standards, those higher requirements must be observed.

Kompanija posluje u različitim jurisdikcijama, od kojih svaka ima sopstveni skup zahteva iz Zakona o privatnosti. Kompanija je posvećena poštovanju svih važećih Zakona o privatnosti i pridržavanju principa navedenih u Politici zaštite informacija. Ovim Standardom uspostavljaju se zahtevi koji će se ujednačeno primenjivati u svim jurisdikcijama u kojima Kompanija posluje. U slučajevima gde lokalni Zakoni o privatnosti nameću dodatne ili strože standarde, ti stroži zahtevi se moraju poštovati.

A fundamental principle of this Standard is the recognition that Personal Information is owned by the Information Subject, not by the Company. Consequently, the Company is dedicated to respecting and safeguarding the

Fundamentalni princip ovog Standarda je priznavanje da su Podaci o ličnosti u vlasništvu Subjekta podataka, a ne Kompanije. Iz tog razloga, Kompanija je posvećena poštovanju i zaštiti Podataka o ličnosti Zaposlenih i Trećih

Personal Information of Employees and Third Parties, which it Processes. This commitment is paramount to maintaining the trust and confidence of all Company's stakeholders. A failure to protect Personal Information can also result in legal and reputational risk to the Company.

lica, koje obrađuje. Ova posvećenost je od suštinske važnosti za održavanje poverenja svih zainteresovanih strana Kompanije. Nepostojanje zaštite Podataka o ličnosti takođe može dovesti do pravnog i reputacionog rizika za Kompaniju.

This Standard must be read in conjunction with the Policy Documents listed in the Related Documents Section.

Ovaj Standard se mora tumačiti u vezi sa Politikama (dokumentima) navedenim u delu Povezani dokumenti.

4. Performance Requirements / Zahtevi za performansama

4.1. Permissibility of Personal Information Processing / Dopuštenost obrade Podataka o ličnosti

The Processing of Personal Information is allowed only if the Information Subject has given their Consent or if it is otherwise permitted by applicable Privacy Laws.

Obrada Podataka o ličnosti dozvoljena je samo ukoliko je Subjekt podataka dao svoju Saglasnost ili ukoliko je to na drugi način dopušteno važećim Zakonima o privatnosti.

When relying on Consent for Processing, such Consent must be obtained in writing or through other legally permissible means. Prior to seeking Consent, the Information Subject must be informed about the purpose of the Processing and any potential transfer of their Personal Information. The declaration of Consent must be clearly highlighted when included within other statements to ensure it is fully understood by the Information Subject.

Kada se Obrada zasniva na Saglasnosti, takva Saglasnost mora biti pribavljena u pisanoj formi ili drugim zakonski dozvoljenim sredstvima. Pre traženja Saglasnosti, Subjekt podataka mora biti informisan o svrsi Obrade i svakom potencijalnom prenosu njihovih Podataka o ličnosti. Izjava o Saglasnosti mora biti jasno istaknuta ukoliko je uključena u okviru drugih izjava, kako bi se osiguralo da je Subjekt podataka u potpunosti razume.

Privacy Liaisons must keep records of all Consents related to their respective Business Functions. This ensures that the Information Subject can, if they choose, withdraw their Consent in accordance with applicable Privacy Laws.

Saradnik za privatnost mora voditi evidenciju o svim Saglasnostima povezanim sa njihovim Poslovnim funkcijama. Ovo osigurava da Subjekt podataka može, ukoliko tako odluči, povući svoju Saglasnost u skladu sa važećim Zakonima o privatnosti.

4.2. Sensitive Personal Information and other Special Categories / Osetljivi podaci o ličnosti i druge posebne kategorije

Information that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, or data concerning health, sex life or sexual orientation is considered sensitive Personal Information. Other types of Personal Information may also be deemed sensitive based on the context, volume and intended usage, as determined through a Privacy Impact Assessment (see Section 4.11 below).

Informacije koje otkrivaju rasno ili etničko poreklo, politička mišljenja, verska ili filozofska uverenja, članstvo u sindikatu, genetski podaci, biometrijski podaci ili podaci koji se odnose na zdravstveno stanje, seksualni život ili seksualnu orijentaciju smatraju se osetljivim Podacima o ličnosti. Druge vrste Podataka o ličnosti takođe se mogu smatrati osetljivim na osnovu konteksta, obima i predviđene upotrebe, kako je utvrđeno Procenom uticaja na privatnost (videti deo 4.11 u nastavku).

Sensitive Personal Information is subject to heightened security measures and can only be Processed with explicit consent except where required or permitted by law, such as for regulatory compliance, legal proceedings, or the protection of rights and safety.

Osetljivi Podaci o ličnosti podležu pojačanim merama bezbednosti i mogu se obrađivati samo uz izričitu saglasnost, osim kada je to zahtevano ili dozvoljeno zakonom, npr. za potrebe regulatorne usklađenosti, pravnih postupaka ili zaštite prava i bezbednosti.

To ensure that sensitive Personal Information is properly Processed, Privacy Liaisons must always consult with Privacy Professionals before collecting such Personal Information. Additionally, Privacy Professionals must be consulted whenever there is uncertainty whether the Personal Information to be Processed qualifies as sensitive.

Kako bi se osiguralo da se osetljivi Podaci o ličnosti pravilno obrađuju, Saradnici za privatnost moraju se uvek konsultovati sa Stručnjacima za privatnost pre prikupljanja takvih Podataka o ličnosti. Pored toga, Stručnjaci za privatnost se moraju konsultovati kad god postoji neizvesnost da li Podaci o ličnosti koji se obrađuju ispunjavaju uslove da se smatraju osetljivim.

4.3. Purpose Limitation / Ograničenje svrhe

Personal Information must be Collected solely for specified, explicit and legitimate purposes. Privacy Liaisons, in consultation with the respective Privacy Professional, must define these purposes and ensure they are appropriately documented. Processing Personal Information for purposes other than

Podaci o ličnosti se moraju Prikupiti isključivo za navedene, izričite i legitimne svrhe. Saradnik za privatnost u konsultaciji sa odgovarajućim Stručnjakom za privatnost, moraju definisati ove svrhe i osigurati da su one adekvatno dokumentovane. Obrada Podataka o ličnosti u svrhe koje su drugačije

those for which it was initially Collected is permissible only with the Information Subject's Consent or if otherwise allowed by applicable Privacy Laws.

od onih za koje su prvobitno Prikupljene dozvoljena je samo uz Saglasnost Subjekta podataka ili ukoliko je drugačije dopušteno važećim Zakonima o privatnosti.

4.4. Accuracy / Tačnost

To ensure the integrity of Personal Information and protect the rights of Information Subjects, the Personal Information Processed by the Company must be accurate and up to date. The accuracy of any Personal Information Collected by the Company must be verified at the point of Collection and at regular intervals thereafter. Privacy Liaisons must also ensure that reasonable steps are taken to amend or destroy any inaccurate or outdated Personal Information Processed by their Business Function in accordance with the *Information Retention, Recovery and Sanitization Standard.*

Da bi se osigurao integritet Podataka o ličnosti i zaštitila prava Subjekta podataka, Podaci o ličnosti koje Kompanija obrađuje moraju biti tačni i ažurni. Tačnost svih Podataka o ličnosti koje Kompanija Prikuplja mora se proveriti u trenutku Prikupljanja i u redovnim intervalima nakon toga. Saradnici za privatnost takođe moraju osigurati preduzimanje razumnih koraka za izmenu ili uništavanje svih netačnih ili zastarelih Podataka o ličnosti koje obrađuje njihova Poslovna funkcija, u skladu sa *Standardom za čuvanje, oporavak i brisanje/uništavanje informacija.*

4.5. Reduced Data Retention / Smanjeni period čuvanja podataka o ličnosti

The longer Personal Information is retained, the greater the risk of a Personal Information Breach or the information becoming inaccurate. The Company must ensure that Personal Information is retained only for the duration necessary to fulfill the business purpose or to comply with legal requirements.

Što se Podaci o ličnosti duže čuvaju, veći je rizik od Povrede Podataka o ličnosti ili od toga da podaci postanu netačni. Kompanija mora osigurati da se Podaci o ličnosti čuvaju samo onoliko dugo koliko je neophodno za ispunjavanje poslovne svrhe ili za usklađenost sa zakonskim zahtevima.

Once Personal Information is no longer needed by a Business Function for its specified purposes, it must be deleted, anonymized or otherwise managed in accordance with the *Information Retention, Recovery and Sanitization Standard.*

Kada Poslovnoj funkciji više nisu potrebni Podaci o ličnosti za navedene svrhe, isti moraju biti izbrisani, anonimizovani ili se mora postupiti na drugi način u skladu sa *Standardom za čuvanje, oporavak i brisanje/uništavanje informacija.*

4.6. Personal Information Communications and Notices / Komunikacija i obaveštenja o podacima o ličnosti

In certain jurisdictions where the Company operates, when Personal Information is Collected, Information Subjects have specific rights. Therefore, before Collecting any Personal Information, the Privacy Liaisons must consult with the respective Privacy Professional to determine what communication or formal notice, if any, must be provided to the Information Subject.

U određenim jurisdikcijama u kojima Kompanija posluje, Subjekti podataka imaju specifična prava prilikom Prikupljanja Podataka o ličnosti. Iz tog razloga, pre Prikupljanja bilo kakvih Podataka o ličnosti, Saradnici za privatnost moraju se konsultovati sa odgovarajućim Stručnjakom za privatnost kako bi se utvrdilo koje obaveštenje ili formalno saopštenje, ako je potrebno, mora biti dostavljeno Subjektu podataka.

If applicable Privacy Laws require a privacy notice to be given to Information Subjects, such notice must be developed in consultation with the respective Privacy Professional to ensure it includes all necessary information and is delivered to the Information Subject within the timeframe required by applicable Privacy Laws.

Ako važeći Zakoni o privatnosti zahtevaju da se obaveštenje o privatnosti dostavi Subjektima podataka, takvo obaveštenje mora biti pripremljeno u konsultaciji sa odgovarajućim Stručnjakom za privatnost kako bi se osiguralo da uključuje sve neophodne informacije i da je dostavljeno Subjektu podataka u roku koji propisuju važeći Zakoni o privatnosti.

When an Information Subject inquires with the Company about their Personal Information, or otherwise seeks to exercise any related rights, the Employee receiving the inquiry must promptly notify the Privacy Liaison for the respective Business Function. The Privacy Liaison must verify the identity of the requestor and refer the inquiry to the respective Privacy Professional for handling.

Kada Subjekt podataka uputi Kompaniji upit o svojim Podacima o ličnosti, ili na drugi način želi da ostvari bilo koje povezano pravo, Zaposleni koji primi upit mora bez odlaganja obavestiti Saradnika za privatnost za odgovarajuću Poslovnu funkciju. Saradnik za privatnost mora proveriti identitet podnosioca zahteva i proslediti upit odgovarajućem Stručnjaku za privatnost na rešavanje.

4.7. Transfer Limitation / Ograničenje prenosa

The Company may engage Third-Parties Processors for various services, such as hosting and storage cloud computing, contract management, background and due diligence screening, reporting and assurance,

Kompanija može angažovati Treće strane Obrađivače za razne usluge, kao što su hostovanje i skladištenje u oblaku, upravljanje ugovorima, provera prošlosti i dubinska analiza (*due diligence*), izveštavanje i kontrola,

risk analysis and mitigation, payroll and benefits management, as well as speak-up and incident reporting services.

When engaging Third Party Processors, the Company remains accountable for the Personal Information Processed by these entities. Therefore, a Data Processing Agreement must be entered into before any transfer of Personal Information occurs. Privacy Liaisons are accountable for ensuring that a Data Processing Agreement is in place, in consultation with the IT Privacy Coordinator and the respective Privacy Professional.

The Data Processing Agreement must require the Third Party to adhere to the relevant Company Policy Documents related to the protection of Personal Information, unless the Privacy Professional determines that the Third-Party Processor has its own policy documents consistent with the principles set out in this Standard.

Additionally, the Data Processing Agreement must clearly define the scope of the Third-Party Processor's activities, stipulating that Processing may not be undertaken for any other purpose.

Privacy Liaisons must assess whether Processing of Personal Information by their respective Business Functions will involve transferring Personal Information outside of the country of Collection. Since Privacy Laws may restrict such transfers to certain jurisdictions, the respective Business Unit's Privacy Professional must be notified before any transfer occurs to evaluate potential restrictions.

analiza i ublažavanje rizika, upravljanje zaradama i naknadama zarada, kao i usluge prijavljivanja nepravilnosti i incidenata.

Prilikom angažovanja Treće strane Obrađivača, Kompanija ostaje odgovorna za Podatke o ličnosti koje ti entiteti Obrađuju. Iz tog razloga, pre nego što dođe do bilo kakvog prenosa Podataka o ličnosti mora se potpisati Ugovor o obradi podataka. Saradnici za privatnost su odgovorni da osiguraju da je Ugovor o obradi podataka na snazi, u konsultaciji sa IT koordinatorom za privatnost i odgovarajućim Stručnjakom za privatnost.

Ugovor o obradi podataka mora zahtevati od Trećeg lica da se pridržava relevantnih Politike Kompanije u vezi sa zaštitom Podataka o ličnosti, osim ako Stručnjak za privatnost ne utvrdi da Treća strana Obrađivač ima sopstvene dokumente politike koji su usaglašeni sa principima utvrđenim u ovom Standardu.

Pored toga, Ugovor o obradi podataka mora jasno definisati obim aktivnosti Treće strane Obrađivača, propisujući da se Obrada ne sme vršiti u druge svrhe.

Saradnici za privatnost moraju proceniti da li će Obrada Podataka o ličnosti od strane njihovih odgovarajućih Poslovnih funkcija uključivati prenos Podataka o ličnosti van zemlje prikupljanja. Budući da Zakoni o privatnosti mogu ograničiti takve prenose na određene jurisdikcije, Stručnjak za privatnost odgovarajuće Poslovne jedinice mora biti obavešten pre nego što se izvrši bilo kakav prenos, kako bi se procenila potencijalna ograničenja.

4.8. Confidentiality and Authorization / Poverljivost i autorizacija

Only authorized Employees are permitted to engage in the Processing of Personal Information. These Employees are strictly prohibited from using such Personal Information for personal purposes, transferring it or making it accessible in any manner to unauthorized Employees, Third Parties or any other external stakeholder. Within the context of this Standard, "unauthorized" also refers to the use of Personal Information by Employees for purposes unrelated to their employment duties.

Samo ovlašćenim Zaposlenima je dozvoljeno da vrše Obradu Podataka o ličnosti. Ovim Zaposlenima je strogo zabranjeno da koriste takve Podatke o ličnosti u lične svrhe, da ih prenose ili da ih na bilo koji način čine dostupnim neovlašćenim Zaposlenima, Trećim licima ili bilo kojoj drugoj eksternoj zainteresovanoj strani. U kontekstu ovog Standarda, „neovlašćeno" se takođe odnosi na korišćenje Podataka o ličnosti od strane Zaposlenih u svrhe koje nisu povezane sa njihovim radnim dužnostima.

4.9. Reporting Personal Information Breaches / Prijavljivanje povreda podataka o ličnosti

Preventing Personal Information Breaches is the accountability of all Employees and Third Parties. All actual or suspected Personal Information Breaches must be reported immediately to a Privacy Liaison or to the Privacy Professional of the respective Business Unit.

In the event of a Personal Information Breach, Privacy Professionals will coordinate an investigation in close collaboration with the IT Privacy Coordinator. The Company will promptly take steps to contain and assess the breach, ensuring that measures are implemented to minimize harm. Depending on the nature of the Personal Information Breach, affected Information Subjects and relevant regulatory authorities may need to be notified.

Sprečavanje Povreda podataka o ličnosti je odgovornost svih Zaposlenih i Trećih lica. Sve stvarne ili sumnjive Povrede podataka o ličnosti moraju biti odmah prijavljene Saradniku za privatnost ili Stručnjaku za privatnost odgovarajuće Poslovne jedinice.

U slučaju Povrede podataka o ličnosti, Stručnjaci za privatnost će koordinisati istragu u bliskoj saradnji sa IT koordinatorom za privatnost. Kompanija će bez odlaganja preduzeti korake za suzbijanje i procenu povrede, osiguravajući primenu mera koje imaju za cilj minimiziranje štete. U zavisnosti od prirode Povrede podataka o ličnosti, možda će biti potrebno obavestiti Subjekte podataka na koje je povreda uticala, kao i relevantne regulatorne organe.

4.10. Data Protection Measures and Privacy by Design / Mere zaštite podataka i privatnost po dizajnu

To safeguard the confidentiality, integrity and security of the Personal Information it Collects, the Company, with the support of the IT Department, must implement physical, technical and administrative security measures. Examples of these measures are provided in Appendix A.

Kako bi osigurala poverljivost, integritet i bezbednost Podataka o ličnosti koje Prikuplja, Kompanija, uz podršku IT Sektora, mora primeniti fizičke, tehničke i administrativne bezbednosne mere. Primeri ovih mera dati su u Prilogu A.

When implementing new applications and services, the Company is committed to embedding privacy into their design and operation from the outset, adhering to the principle of "privacy by design".

Prilikom uvođenja novih aplikacija i usluga, Kompanija je posvećena ugrađivanju privatnosti u njihov dizajn i rad od samog početka, pridržavajući se principa „privatnost po dizajnu".

4.11. Privacy Impact Assessment and Risk / Procena uticaja na privatnost i rizik

To uphold its commitment to protecting Personal Information and to enable transparency and control, the Company will conduct "Privacy Impact Assessments" where appropriate. A Privacy Impact Assessment is a systematic process designed to evaluate how Personal Information is Collected, used, disclosed and managed within the Company's operations. This process helps the Company identify potential Privacy risks and implement measures to mitigate them, especially when introducing new technologies, systems, or processes that involve Personal Information.

Da bi podržala svoju posvećenost zaštiti Podataka o ličnosti i omogućila transparentnost i kontrolu, Kompanija će, gde je to prikladno, sprovoditi „Procene uticaja na privatnost". Procena uticaja na privatnost je sistematski proces osmišljen da proceni kako se Podaci o ličnosti prikupljaju, koriste, otkrivaju i kako se istima upravlja u okviru operacija Kompanije. Ovaj proces pomaže Kompaniji da identifikuje potencijalne rizike po privatnost i primeni mere za njihovo ublažavanje, naročito prilikom uvođenja novih tehnologija, sistema ili procesa koji uključuju Podatke o ličnosti.

The Company will conduct Privacy Impact Assessments in the following scenarios:

- When new projects or systems are introduced that Collect or otherwise Process Personal Information;

Kompanija će sprovoditi Procene uticaja na privatnost u sledećim scenarijima:

- Kada se uvode novi projekti ili sistemi koji prikupljaju ili na drugi način obrađuju Podatke o ličnosti;

- When existing Processing activities undergo significant changes; and
- When legal requirements mandate such assessment (e.g., in response to regulatory changes).

- Kada postojeće aktivnosti obrade podležu značajnim promenama; i
- Kada zakonski zahtevi nalažu takvu procenu (npr. kao odgovor na regulatorne promene).

Privacy Impact Assessments are carried out by the respective Privacy Liaisons under the oversight of the respective Privacy Professionals and in consultation with the IT Privacy Coordinator and the Group Privacy Officer, when necessary.

Procene uticaja na privatnost sprovode odgovarajući Saradnici za privatnost pod nadzorom odgovarajućih Stručnjaka za privatnost i u konsultaciji sa IT koordinatorom za privatnost i Službenikom za privatnost Grupe, kada je to potrebno.

4.12. Mobile Device, Email and Internet Usage / Korišćenje mobilnih uređaja, elektronske pošte i internet

Employees must exercise special caution when sharing or otherwise Processing Personal Information via mobile devices such as smartphones, tablets and notebooks as well as through email and internet use. Detailed requirements can be found in the *Acceptable Mobile Device Use Procedure, Acceptable Email Use Procedure* and the *Internet Acceptable Use Procedure*.

Zaposleni moraju biti posebno oprezni prilikom deljenja ili druge obrade Podataka o ličnosti putem mobilnih uređaja, kao što su pametni telefoni, tableti i laptopovi, kao i putem korišćenja elektronske pošte i interneta. Detaljni zahtevi se mogu naći u Proceduri za prihvatljivo korišćenje mobilnih uređaja, Proceduri za prihvatljivo korišćenje elektronske pošte i Proceduri za prihvatljivo korišćenje interneta.

5. Role Relationships, Authorities and Accountabilities / Odnosi uloga, ovlašćenja i odgovornosti

To facilitate compliance with this Standard, certain roles, relationships, and accountabilities are prescribed herein.

Da bi se olakšalo poštovanje ovog standarda, ovde su utvrđene određene uloge, odnosi i odgovornosti.

5.1. Group Privacy Officer / Službenik za privatnost Grupe

The Group Privacy Officer is accountable for overseeing compliance with this Standard,

Službenik za privatnost Grupe je odgovoran za nadgledanje usklađenosti sa ovim

and reporting to DPMs senior management, with the support of designated Privacy Professionals. To fulfill these accountabilities, the Group Privacy Officer may request information from the Privacy Professionals, who are obligated to provide the requested information within a reasonable timeframe.

In the absence of a designated Privacy Professional for DPM, the accountabilities outlined in Section 5.2 below will be assumed by the Group Privacy Officer.

Standardom i izveštavanje višeg menadžmenta DPM-a, uz podršku imenovanih Stručnjaka za privatnost. U cilju ispunjavanja ovih odgovornosti, Službenik za privatnost Grupe može zatražiti informacije od Stručnjaka za privatnost, koji su obavezni da tražene informacije dostave u razumnom roku.

U odsustvu imenovanog Stručnjaka za privatnost za DPM, odgovornosti navedene u delu 5.2 u nastavku preuzima Službenik za privatnost Grupe.

5.2. Privacy Professionals / Stručnjaci za privatnost

Privacy Professionals are accountable for ensuring that applicable Privacy Laws are understood, communicated and integrated into the practices of their respective Business Unit.

The key accountabilities of Privacy Professionals include, but are not limited to:

- Maintaining up-to-date knowledge of applicable Privacy Laws and notifying Group Privacy Officer of any significant changes;
- Developing and updating Privacy policy documents for their respective Business Unit;
- Creating and delivering Privacy training programs for Employees for their respective Business Unit;
- Assisting and advising Privacy Liaisons in establishing Data Processing Agreements when engaging Third Party Processors;
- Notifying the Group Privacy Officer of any Privacy Data Breaches and coordinating the investigation and response to such beaches;
- Overseeing Privacy Impact Assessments conducted by Privacy Liaisons within their respective Business Unit; and
- Acting as the primary point of contact with Privacy authorities for their respective Business Units.

Stručnjaci za privatnost su odgovorni za osiguravanje da se važeći Zakoni o privatnosti razumeju, prenose i integrišu u praksu njihovih odgovarajućih Poslovnih jedinica.

Ključne odgovornosti Stručnjaka za privatnost uključuju, između ostalog:

- Održavanje ažurnog znanja o važećim Zakonima o privatnosti i obaveštavanje Službenika za privatnost Grupe o svim značajnim promenama;
- Izrada i ažuriranje dokumenata Politike privatnosti za odgovarajuće Poslovne jedinice;
- Kreiranje i sprovođenje programa obuke o Privatnosti za Zaposlene u odgovarajućoj Poslovnoj jedinici;
- Pružanje pomoći i saveta Saradnicima za privatnost prilikom zaključivanja Ugovora o obradi podataka tokom angažovanja Treće strane Obrađivača;
- Obaveštavanje Službenika za privatnost Grupe o svim Povredama podataka o ličnost i koordinacija istrage i odgovora na takve povrede;
- Nadgledanje Procena uticaja na privatnost koje sprovode Saradnici za privatnost u okviru njihovih odgovarajućih Poslovnih jedinica; i
- Delovanje kao primarna kontakt tačka sa nadležnim Organima za privatnost za odgovarajuće Poslovne jedinice.

5.3. Privacy Liaison / Saradnik za privatnost

Each Business Function Head whose Business Functions Processes Personal Information, must designate an Employee within the

Svaki Rukovodilac Poslovne funkcije čije Poslovne funkcije Obrađuju Podatke o ličnosti, mora imenovati Zaposlenog unutar Poslovne

Business Function to serve as a Privacy Liaison and facilitate the adherence to this Standard.

The key accountabilities of the Privacy Liaisons include, but are not limited to:

- Ensuring that Privacy considerations are integrated into the business processes and projects of their respective Business Function;
- Ensuring that Personal Information Processed by their respective Business Function is Collected, used and stored in compliance with this Standard;
- Ensuring a Data Processing Agreement is executed after consulting the respective Business Unit's Privacy Professional and the IT Privacy Coordinator;
- Reporting privacy concerns and Personal Information Breaches to the Privacy Professionals; and
- Conducting Privacy Impact Assessments, as required.

funkcije da služi kao Saradnik za privatnost i olakšava poštovanje ovog Standarda.

Ključne odgovornosti Saradnika za privatnost uključuju, između ostalog:

- Osiguravanje da su pitanja Privatnosti integrisana u poslovne procese i projekte njihove odgovarajuće Poslovne funkcije;
- Osiguravanje da se Podaci o ličnosti koje obrađuje njihova odgovarajuća Poslovna funkcija Prikupljaju, koriste i čuvaju u skladu sa ovim Standardom;
- Osiguravanje da se Ugovor o obradi podataka izvršava nakon konsultacija sa Stručnjakom za privatnost odgovarajuće Poslovne jedinice i IT koordinatorom za privatnost;
- Prijavljivanje zabrinutosti u vezi sa Privatnošću kao i Povreda podataka o ličnosti Stručnjacima za privatnost; i
- Sprovođenje Procena uticaja na privatnost, po potrebi.

5.4. IT Privacy Coordinator / IT koordinator za privatnost

The IT Privacy Coordinator is accountable for supporting the Group Privacy Officer and Privacy Professionals and ensuring the implementation of the Company technological controls designed to protect Personal Information.

The key accountabilities of the IT Privacy Coordinator include, but are not limited to:

- Reviewing, managing, and conducting regular testing and assessments to

IT koordinator za privatnost je odgovoran za podršku Službeniku za privatnost Grupe i Stručnjacima za privatnost i za osiguravanje primene tehničkih kontrola Kompanije predviđenih za zaštitu Podataka o ličnosti.

Ključne odgovornosti IT koordinatora za privatnost uključuju, između ostalog:

- Pregled, upravljanje i sprovođenje redovnog testiranja i procena u cilju

evaluate the effectiveness of technical and organizational measures for ensuring the security of Personal Information.

- Assisting Privacy Professionals in responding to Information Subject requests or requests from Privacy authorities within the timeframes prescribed by Privacy Laws.
- Reviewing data security documents to ensure appropriate security controls, both prior to the onboarding of Third Party – Processors and as part of ongoing interactions with them.
- Assisting in identifying, managing and mitigating Personal Information Breaches through technological support.
- Supporting Privacy Professionals in the execution of other accountabilities set out in this Standard, as needed.

evaluacije efikasnosti tehničkih i organizacionih mera za osiguravanje bezbednosti Podataka o ličnosti.

- Pomaganje Stručnjacima za privatnost u odgovaranju na zahteve Subjekata podataka ili zahteve nadležnih Organa za privatnost u rokovima propisanim Zakonima o privatnosti.
- Pregled dokumenata o bezbednosti podataka kako bi se osigurale odgovarajuće bezbednosne kontrole, kako pre angažovanja Treće strane Obrađivača, tako i u okviru tekuće saradnje sa njima.
- Pomoć u identifikaciji, upravljanju i ublažavanju Povreda podataka o ličnosti kroz tehnološku podršku.
- Podrška Stručnjacima za privatnost u izvršavanju drugih odgovornosti navedenih u ovom Standardu, po potrebi.

6. Effective Date and Review / Datum stupanja na snagu i revizije

This Standard must be reviewed once every two years.

Ovaj Standard se mora revidirati svake dve godine.

7. Compliance / Poštovanje ovog standard

Any violation of this Standard must be reported through the speak-up channels specified in the *Code of Business Conduct and Ethics*.

Svako kršenje ovog Standarda mora se prijaviti putem kanala za prijavljivanje nepravilnosti navedenih u Kodeksu poslovnog ponašanja i poslovne etike.

Non-compliance with this Standard may subject a person to whom this Standard applies to corrective action by the Company as

Nepoštovanje ovog Standarda može podrazumevati primenu korektivnih mera Kompanije protiv lica na koja se ovaj Standard

described in the *Code of Business Conduct and Ethics.*

primenjuje, kako je opisano u Kodeksu poslovnog ponašanja i poslovne etike.

8. Appendices / Prilozi

Appendix A: Examples of Safeguard Measures

Prilog A: Primeri mera zaštite

Appendix A: Examples of Safeguard Measures / Prilog A: Primeri mera zaštite

(a) Physical Security Measures

These measures protect the physical locations and devices where Personal Information is stored or accessed. Some examples include:

- **Controlled Access to Facilities**: Only authorized Employees may access the Company's buildings or areas where Personal Information is stored.
- **Secure Storage**: Hard copies of Personal Information (e.g., employee records, contracts) must be kept in locked cabinets, safes, or secure filing rooms that are only accessible to authorized Employees.
- **Environmental Controls**: Protecting server rooms from environmental risks such as fire, floods, or overheating by using climate control, fire suppression systems, and uninterruptible power supplies.
- **Visitor Control**: Implementing a strict visitor management system, including strict visitor protocols in secure areas.

The Company may also adopt surveillance and monitoring techniques (such as the use of CCTV cameras and alarms to monitor access to facilities, data centers, and sensitive areas) after consulting with the Group Privacy Professional.

(b) Technical Security Measures

These are measures designed to protect digital systems and networks from cyber

(a) Fizičke mere bezbednosti

Ove mere štite fizičke lokacije i uređaje na kojima se Podaci o ličnosti čuvaju ili preko kojih se Podacima o ličnosti pristupa. Neki primeri su:

- **Kontrolisan pristup objektima**: Samo ovlašćeni Zaposleni mogu pristupiti objektima ili područjima Kompanije gde se Podaci o ličnosti čuvaju.
- **Bezbedno skladištenje**: Štampane kopije Podataka o ličnosti (npr. evidencija zaposlenih, ugovori) moraju se čuvati u zaključanim ormarima, sefovima ili obezbeđenim arhivama kojima mogu pristupiti samo ovlašćeni Zaposleni.
- **Kontrole okruženja**: Zaštita serverskih soba od rizika iz okruženja kao što su požar, poplave ili pregrevanje, korišćenjem kontrole klime, sistema za gašenje požara i neprekidnog napajanja (UPS).
- **Kontrola posetilaca**: Primena strogog sistema za upravljanje posetiocima, uključujući stroge protokole za posetioce u bezbednim područjima.

Kompanija takođe može primeniti tehnike nadzora i monitoringa (kao što je upotreba CCTV kamera i alarma za praćenje pristupa objektima, data centrima i osetljivim područjima) nakon konsultacija sa Službenikom za privatnost Grupe.

(b) Tehničke mere bezbednosti

Ovo su mere osmišljene za zaštitu digitalnih sistema i mreža od sajber pretnji i

threats and unauthorized access. Some specific examples include:

- **Data Encryption**: Encrypting sensitive Personal Information both at rest (in storage) and in transit (when being transmitted over networks) to prevent unauthorized access.
- **Firewalls and Intrusion Detection Systems**: Using firewalls and intrusion detection/prevention systems to monitor and filter network traffic
- **Multi-Factor Authentication:** Requiring multiple forms of verification for accessing sensitive systems or information.
- **Role-Based Access Controls**: Limiting access to Personal Information based on an Employee's role or job accountabilities.
- **Regular Security Audits and Vulnerability Assessments**: Regularly assessing and testing the company's IT infrastructure to identify and address potential treats.
- **Anti-virus and Anti-malware Software**: Deploying and regularly updating anti-virus and anti-malware software on all Company systems to detect and remove malicious software.
- **Backup Systems**: Implementing automatic backups of important information, stored in secure, off-site locations or in the cloud.

neovlašćenog pristupa. Neki konkretni primeri su:

- **Šifrovanje (enkripcija) podataka:** Šifrovanje osetljivih Podataka o ličnosti u mirovanju (u skladištu) i u tranzitu (prilikom prenosa preko mreža) radi sprečavanja neovlašćenog pristupa.
- **Firewall-ovi i sistemi za detekciju upada:** Korišćenje firewall-ova i sistema za detekciju/prevenciju upada za praćenje i filtriranje mrežnog saobraćaja.
- **Višefaktorska autentifikacija (MFA):** Zahtevanje višestrukih oblika verifikacije za pristup osetljivim sistemima ili informacijama.
- **Kontrole pristupa zasnovane na ulogama:** Ograničavanje pristupa Podacima o ličnosti na osnovu uloge ili radnih odgovornosti Zaposlenog.
- **Redovne bezbednosne provere i procene ranjivosti:** Redovna procena i testiranje IT infrastrukture Kompanije u cilju identifikovanja i rešavanja potencijalnih pretnji.
- **Anti-virus i anti-malware softver:** Instaliranje i redovno ažuriranje anti-virus i anti-malware softvera na svim sistemima Kompanije u cilju otkrivanja i uklanjanja zlonamernog softvera.
- **Sistemi za izradu rezervnih kopija (Backup):** Implementacija automatske izrade rezervnih kopija važnih informacija, koje se čuvaju na bezbednim, udaljenim lokacijama ili u oblaku.

- **Web filtering:** Blocking access to malicious and unauthorized websites, reducing the risk of malware, phishing, and data breaches.

- **Patch Management**: Regularly updating software with the latest security software updates (i.e. patches) to mitigate vulnerabilities.
- **Security Incident and Event Management**: Implementing tools, which provide centralized monitoring, analysis, and real-time alerting of security events across the Company's network.

- **Security Incident Response Plan:** Quickly identifying and mitigating security breaches to minimize damage and information loss
- **Disaster Recovery Plan:** Focusing on restoring IT systems and information access after disruptions to ensure business continuity.

(c) Administrative Security Measures

Administrative measures ensure that policies, procedures, and employee behavior contribute to the protection of Personal Information. These include:

- **Privacy Policies and Procedures**: Developing and communicating clear policies for handling, access, retention, and deletion of Personal Information.
- **Employee Training and Awareness**: Providing regular training to Employees on best practices for data

- **Web filtriranje:** Blokiranje pristupa zlonamernim i neovlašćenim veb lokacijama, čime se smanjuje rizik od malvera, phishing-a i povreda podataka.
- **Upravljanje zakrpama:** Redovno ažuriranje softvera najnovijim bezbednosnim zakrpama sa ciljem ublažavanja ranjivosti.
- **Upravljanje bezbednosnim incidentima i događajima:** Implementacija alata koji omogućavaju centralizovano praćenje, analizu i upozoravanje u realnom vremenu na bezbednosne događaje širom mreže Kompanije.
- **Plan reagovanja na bezbednosne incidente:** Brzo identifikovanje i ublažavanje povreda bezbednosti s ciljem minimiziranja štete i gubitka informacija.
- **Plan oporavka od katastrofe:** Fokusiranje na obnavljanje IT sistema i pristupa informacijama nakon prekida, kako bi se osigurao kontinuitet poslovanja.

(c) Administrativne mere bezbednosti

Administrativne mere obezbeđuju da politike, procedure i ponašanje zaposlenih doprinose zaštiti Podataka o ličnosti. One uključuju:

- **Politike i procedure privatnosti:** Priprema i obaveštavanje o jasnim politikama za rukovanje, pristup, čuvanje i brisanje Podataka o ličnosti.
- **Obuka i podizanje svesti zaposlenih:** Pružanje redovne obuke Zaposlenima o najboljim praksama za bezbednost

security, phishing awareness, password management, and how to report suspicious activity.

- **Third-Party Processor Vendor Management**: Ensuring that Third-Party Processors comply with the Company's privacy and security standards.
- **Regular Audits and Compliance Checks**: Conducting internal and external audits to ensure compliance with Privacy Laws and Company policies.

podataka, svesti o phishing-u, upravljanju lozinkama i kako prijaviti sumnjive aktivnosti.

- **Upravljanje Trećim stranama Obrađivačima:** Osiguravanje da se Treće strane Obrađivači pridržavaju standarda privatnosti i bezbednosti Kompanije.
- **Redovne provere i kontrole usklađenosti:** Sprovođenje internih i eksternih revizija s ciljem osiguravanja poštovanja Zakona o privatnosti i politika Kompanije.