

Na osnovu člana 41. Zakona o zaštiti podataka o ličnosti („Službeni glasnik RS”, broj 87/2018), (u daljem tekstu: Zakon) i člana 198. stav 4. Zakona o privrednim društvima ("Sl. glasnik RS", br. 36/2011, 99/2011, 83/2014 - dr. zakon, 5/2015, 44/2018, 95/2018 i 91/2019) VINAVER MEDICAL DOO NOVI SAD, Fruškogorska 1, MB: 21934151, PIB: 113843476, (u daljem tekstu: Rukovalac), dana 17.05.2024. godine donosi:

## **PRAVILNIK O ZAŠTITI PODATAKA O LIČNOSTI**

### **Uvod**

VINAVER MEDICAL DOO NOVI SAD je specijalizovan za razvoj softverskih rešenja zasnovanih na sistemima veštačke inteligencije (u daljem tekstu: AI Rešenja) za kvantifikaciju materijala korišćenjem spektralnog rendgenskog snimanja u cilju poboljšanja medicinske dijagnostike i radioterapije korisnika usluga posebno:

- Softverska rešenje na bazi veštačke inteligencije koji generiše kvantitativnu reprezentaciju CT slike iz spektralnih podataka radi poboljšane detekcije oboljenja kao i povećanja preciznosti u planiranju svih vrsta radioterapije
- Softverska rešenje na bazi veštačke inteligencije za detekciju oboljenja prilikom svih vrsta endoskopskih ispitivanja u medicini

Ovaj pravilnik se primenjuje na sve aktivnosti obrade podataka o ličnosti koje sprovodi VINAVER MEDICAL DOO NOVI SAD, uključujući pre svega prikupljanje, skladištenje i korišćenje anonimizovanih zdravstvenih podataka u svrhu obučavanja algoritama veštačke inteligencije i mašinskog učenja (u daljem tekstu: **AI algoritama**).

Ovaj pravilnik predstavlja našu posvećenost usklađenosti sa Zakonom o zaštiti podataka o ličnosti (u daljem tekstu: **ZZPL**), Opštom uredbom o zaštiti podataka Evropske unije (u daljem tekstu: **GDPR**), detaljno opisujući naše aktivnosti obrade podataka, mere zaštite podataka i politike koje su na snazi radi zaštite ličnih podataka uz poštovanje principa Akta (Opšte uredbе) o veštačkoj inteligenciji (u daljem tekstu: **AI Act**).

## **Osnovne odredbe**

### **Član 1.**

Pravilnik o zaštiti podataka o ličnosti (u daljem tekstu: Pravilnik) je osnovni interni opšti akt kojim se uređuje

Based on Article 41 of the Law on Personal Data Protection ("Official Gazette of RS", No. 87/2018), (hereinafter: the Law) and Article 198, paragraph 4 of the Law on Companies ("Official Gazette of RS", No. 36/2011, 99/2011, 83/2014 - other law, 5/2015, 44/2018, 95/2018 and 91/2019) VINAVER MEDICAL DOO NOVI SAD, Fruškogorska 1, MB: 21934151, PIB: 113843476, (hereinafter: the Controller), on 17.05.2024. adopts:

## **RULEBOOK ON PERSONAL DATA PROTECTION**

### **Introduction**

VINAVER MEDICAL DOO NOVI SAD is specialized in the development of AI solutions for material quantification using spectral X-ray imaging to improve medical diagnostics and radiotherapy for users of service especially:

- Software solution based on artificial intelligence that generates a quantitative representation of a CT image from spectral data for improved disease detection as well as increased precision in the planning of all types of radiotherapy
- Software solution based on artificial intelligence for disease detection during all types of endoscopic examinations in medicine

This Rulebook applies to all personal data processing activities carried out by VINAVER MEDICAL DOO NOVI SAD, including primarily the collection, storage and use of anonymized health data for the purpose of training Artificial intelligence and machine learning I algorithms (hereinafter: **AI algorithms**).

This Rulebook represents our commitment to compliance with the Law on Personal Data Protection (hereinafter: **LPDP**), the General Data Protection Regulation of the European Union (hereinafter: **GDPR**), detailing our data processing activities, data protection measures and policies in force to protect personal data while respecting the principles of the Artificial Intelligence Act (hereinafter: **AI Act**).

## **Basic Provisions**

### **Article 1**

The Rulebook on Personal Data Protection (hereinafter: **Rulebook**) is the basic internal general act regulating the

zaštita podataka o ličnosti svih lica koja stupaju u kontakt sa Rukovaocem a naročito: zaposlenih i radno angažovanih lica, spoljnih saradnika i drugih lica koja stupaju u ugovorne i druge pravne odnose sa Rukovaocem, kao i drugih lica čije podatke Rukovalac obrađuje bilo da se radi o kandidatima koji konkurišu za posao, korisnicima usluga/klijentima, poslovnim partnerima kao i licima čije podatke obrađujemo kao Obrađivači, u skladu sa Zakonom, Opštom uredbom o zaštiti podataka Evropske unije (Uredba (EU) 2016/679 Evropskog Parlamenta i Saveta od 27. aprila 2016.godine o zaštiti fizičkih lica u pogledu obrade ličnih podataka i o slobodnom kretanju takvih podataka i ukidanju Direktive 95/46/EC - GDPR.), uz poštovanje Akta (Opšte uredbe) o veštačkoj inteligenciji (AI Act) i drugih propisa u oblasti zaštite podataka o ličnosti.

Cilj ovog Pravilnika je da se obezbedi pravna sigurnost i transparentnost u obradi podataka o ličnosti lica čiji se podaci obrađuju, kao i da se utvrdi pravni osnov, svrha obrade, vrste podataka koje se obrađuju, prava lica u pogledu obrade podataka o ličnosti, mere zaštite podataka, obaveze zaposlenih u pogledu zaštite podataka i druga pitanja od značaja.

Na pitanja koja nisu regulisana ovim Pravilnikom, neposredno će se primenjivati odredbe Zakona i drugih relevantnih propisa koji regulišu oblast zaštite podataka o ličnosti.

## Značenje pojedinih izraza Član 2.

Pojedini izrazi u ovom Pravilniku imaju sledeće značenje:

„**podatak o ličnosti**“ je svaki podatak koji se odnosi na fizičko lice čiji je identitet određen ili odrediv, neposredno ili posredno, posebno na osnovu oznake identiteta, kao što je ime i identifikacioni broj, podataka o lokaciji, identifikatora u elektronskim komunikacionim mrežama ili jednog, odnosno više obeležja njegovog fizičkog, fiziološkog, genetskog, mentalnog, ekonomskog, kulturnog i društvenog identiteta;

„**posebne vrste podataka o ličnosti**“ su podaci kojim se otkriva rasno ili etničko poreklo, političko mišljenje, versko ili filozofsko uverenje ili članstvo u sindikatu, genetski podaci, biometrijski podaci, podaci o zdravstvenom stanju, seksualnom životu ili seksualnoj orijentaciji fizičkog lica;

protection of personal data of all persons who come into contact with the Controller, in particular: employees and persons engaged to work, external associates and other persons entering into contractual and other legal relations with the Controller, as well as other persons whose data the Controller processes, whether they are job applicants, service users/clients, business partners or persons whose data we process as Processors, in accordance with the Law, the General Data Protection Regulation of the European Union (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - GDPR), while respecting the Artificial Intelligence Act (AI Act) and other regulations in the field of personal data protection.

The aim of this Rulebook is to ensure legal certainty and transparency in the processing of personal data of persons whose data is processed, as well as to establish the legal basis, purpose of processing, types of data processed, rights of persons regarding personal data processing, data protection measures, obligations of employees regarding data protection and other relevant issues.

For issues not regulated by this Rulebook, the provisions of the Law and other relevant regulations governing the field of personal data protection shall apply directly.

## Meaning of Certain Terms Article 2

Certain terms in this Rulebook have the following meaning:

„**Personal data**“ means any information relating to an identified or identifiable natural person, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

„**Special categories of personal data**“ means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

„**lice na koje se podaci odnose**“ je fizičko lice čiji se podaci o ličnosti obrađuju;

„**obrada podataka o ličnosti**“ je svaka radnja ili skup radnji koje se vrše automatizovano ili neautomatizovano sa podacima o ličnosti ili njihovim skupovima, kao što su prikupljanje, beleženje, razvrstavanje, grupisanje, odnosno strukturiranje, pohranjivanje, upodobljavanje ili menjanje, otkrivanje, uvid, upotreba, otkrivanje prenosom, odnosno dostavljanjem, umnožavanje, širenje ili na drugi način činjenje dostupnim, upoređivanje, ograničavanje, brisanje ili uništavanje (u daljem tekstu: obrada);

„**ograničavanje obrade**“ je označavanje pohranjenih podataka o ličnosti u cilju ograničenja njihove obrade u budućnosti;

„**profilisanje**“ je svaki oblik automatizovane obrade koji se koristi da bi se ocenilo određeno svojstvo ličnosti, posebno u cilju analize ili predviđanja radnog učinka fizičkog lica, njegovog ekonomskog položaja, zdravstvenog stanja, ličnih sklonosti, interesa, pouzdanosti, ponašanja, lokacije ili kretanja;

„**pseudonimizacija**“ je obrada na način koji onemogućava pripisivanje podataka o ličnosti određenom licu bez korišćenja dodatnih podataka, pod uslovom da se ovi dodatni podaci čuvaju posebno i da su preduzete tehničke, organizacione i kadrovske mere koje obezbeđuju da se podatak o ličnosti ne može pripisati određenom ili odredivom licu;

„**rukovalac**“ je fizičko ili pravno lice, odnosno organ vlasti koji samostalno ili zajedno sa drugima određuje svrhu i način obrade. Zakonom kojim se određuje svrha i način obrade, može se odrediti i rukovalac ili propisati uslovi za njegovo određivanje;

„**obrađivač**“ je fizičko ili pravno lice, odnosno organ vlasti koji obrađuje podatke o ličnosti u ime rukovaoca;

„**primalac**“ je fizičko ili pravno lice, odnosno organ vlasti kome su podaci o ličnosti otkriveni, bez obzira da li se radi o trećoj strani ili ne, osim ako se radi o organima vlasti koji u skladu sa zakonom primaju podatke o ličnosti u okviru istraživanja određenog slučaja i obrađuju ove podatke u skladu sa pravilima o zaštiti podataka o ličnosti koja se odnose na svrhu obrade;

"**Data subject**" means a natural person whose personal data is processed;

"**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"**Restriction of processing**" means the marking of stored personal data with the aim of limiting its processing in the future;

"**Profiling**" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements;

"**Pseudonymization**" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

"**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

"**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"**Recipient**" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not, unless it is a matter of authorities that, in accordance with the law, receive personal data within the framework of the investigation of a specific case and process this data in

„**treća strana**“ je fizičko ili pravno lice, odnosno organ vlasti, koji nije lice na koje se podaci odnose, rukovalac ili obrađivač, kao ni lice koje je ovlašćeno da obrađuje podatke o ličnosti pod neposrednim nadzorom rukovoca ili obrađivača;

„**genetski podatak**“ je podatak o ličnosti koji se odnosi na nasleđena ili stečena genetska obeležja fizičkog lica koja pružaju jedinstvenu informaciju o fiziologiji ili zdravlju tog lica, a naročito oni koji su dobijeni analizom iz uzorka biološkog porekla;

„**biometrijski podatak**“ je podatak o ličnosti dobijen posebnom tehničkom obradom u vezi sa fizičkim obeležjima, fiziološkim obeležjima ili obeležjima ponašanja fizičkog lica, koja omogućava ili potvrđuje jedinstvenu identifikaciju tog lica, kao što je slika njegovog lica ili njegovi daktiloskopski podaci;

„**podaci o zdravlju**“ su podaci o fizičkom ili mentalnom zdravlju fizičkog lica, uključujući i one o pružanju zdravstvenih usluga, kojima se otkrivaju informacije o njegovom zdravstvenom stanju;

„**Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti**“ (u daljem tekstu: Poverenik) je nezavisan i samostalni organ vlasti ustanovljen na osnovu zakona, koji je nadležan za nadzor nad sprovođenjem ovog zakona i obavljanje drugih poslova propisanih zakonom;

„**organ vlasti**“ je državni organ, organ teritorijalne autonomije i jedinice lokalne samouprave, javno preduzeće, ustanova i druga javna služba, organizacija i drugo pravno ili fizičko lice koje vrši javna ovlašćenja; Na sve ostale pojmove koji nisu izričito navedeni u ovom članu, primenjuju se definicije iz Zakona za zaštitu podataka o ličnosti.

### Načela obrade podataka o ličnosti Član 3.

Prilikom obrade podataka o ličnosti Rukovalac će postupati u skladu sa sledećim načelima:

„**Zakornost, poštenje i transparentnost**“ podaci o ličnosti će se obrađivati zakonito, pošteno i transparentno

accordance with the rules on the protection of personal data related to the purpose of processing;

„**Third party**“ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

„**Genetic data**“ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person;

„**Biometric data**“ means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person;

„**Data concerning health**“ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

„**Commissioner for Information of Public Importance and Personal Data Protection**“ (hereinafter: the Commissioner) is an independent state authority established by law, which is competent to supervise the implementation of this law and perform other duties prescribed by law;

„**Public authority**“ means a state authority, territorial autonomy authority and local self-government unit, public enterprise, institution and other public service, organization and other legal or natural person exercising public authority; For all other terms not explicitly stated in this Article, the definitions from the Law on Personal Data Protection shall apply.

### Principles of Personal Data Processing Article 3

When processing personal data, the Controller shall act in accordance with the following principles:

„**Lawfulness, fairness and transparency**“ - personal data shall be processed lawfully, fairly and in a transparent

u odnosu na lice na koje se podaci odnose. Zakonita obrada je obrada koja se vrši u skladu sa Zakonom, odnosno drugim zakonom kojim se uređuje obrada;

**„Ograničenje u odnosu na svrhu obrade“** podaci o ličnosti se prikupljati u svrhe koje su konkretno određene, izričite, opravdane i zakonite i dalje se ne mogu obrađivati na način koji nije u skladu sa tim svrhama;

**„Minimizacija podataka“** podaci o ličnosti će biti primereni, bitni i ograničeni na ono što je neophodno u odnosu na svrhu obrade;

**„Tačnost“** podaci o ličnosti će biti tačni i, ako je to neophodno, ažurirani. Uzimajući u obzir svrhu obrade, moraju se preduzeti sve razumne mere kojima se obezbeđuje da se netačni podaci o ličnosti bez odlaganja izbrišu ili isprave;

**„Ograničenje čuvanja“** podaci o ličnosti će se čuvati u obliku koji omogućava identifikaciju lica samo u roku koji je neophodan za ostvarivanje svrhe obrade;

**„Načelo bezbednosti“** Rukovalac sprovodi odgovarajuće tehničke, organizacione i kadrovske mere kako bi dostigao odgovarajući nivo bezbednosti u odnosu na rizik, a i skladu sa nivoom tehnoloških dostignuća i troškovima njihove primene, prirodom, obimom, okolnostima i svrhom obrade, kao i verovatnoćom nastupanja rizika i nivoom rizika za prava i slobode fizičkih lica, i organi koji, u skladu sa zakonom, primaju podatke o ličnosti u okviru istrage o konkretnom slučaju i obrađuju te podatke u skladu sa pravilima o zaštiti podataka o ličnosti u vezi sa svrhom obrade;

**„Integritet i poverljivost“** podaci o ličnosti će se obrađivati na način koji obezbeđuje odgovarajuću zaštitu podataka o ličnosti, uključujući zaštitu od neovlašćene ili nezakonite obrade, kao i od slučajnog gubitka, uništenja ili oštećenja primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera.

**„Odgovornost za postupanje“** Rukovalac je odgovoran za primenu odredaba ovog člana i mora biti u mogućnosti da predoči njihovu primenu.

**Podaci o ličnosti koji se obrađuju**

manner in relation to the data subject. Lawful processing is processing performed in accordance with the Law or other law governing the processing;

**"Purpose limitation"** - personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

**"Data minimization"** - personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

**"Accuracy"** - personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

**"Storage limitation"** - personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

**"Principle of security"** The operator implements appropriate technical, organizational and personnel measures in order to reach the appropriate level of security in relation to the risk, and in accordance with the level of technological achievements and the costs of their application, the nature, scope, circumstances and purpose of the processing, as well as the probability of the occurrence of the risk and the level of risk for the rights and freedoms of natural persons, and the authorities that, in accordance with the law, receive personal data within the framework of the investigation of a specific case and process this data in accordance with the rules on the protection of personal data related to the purpose of processing;

**"Integrity and confidentiality"** - personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical, organizational and personnel measures;

**"Accountability"** - The controller shall be responsible for, and be able to demonstrate compliance with these principles.

**Personal Data which is being processed**

#### Član 4.

Rukovalac obrađuje sledeće podatke o ličnosti zaposlenih, radno angažovanih lica, spoljnih saradnika i drugih lica koja stupaju u ugovorne i druge pravne odnose sa Rukovaocem:

- Ime i prezime, ime roditelja, adresa prebivališta/boravišta, opština prebivališta/boravišta, datum i mesto rođenja, pol, jedinstveni matični broj građana, jedinstveni matični broj stranaca, broj lične karte, broj pasoša, državljanstvo, broj zdravstvenog osiguranja, akademske i profesionalne kvalifikacije, stepen obrazovanja, titule, podatke o veštinama, znanjima stranih jezika, obukama, istoriji zaposlenja, biografiji, radnom iskustvu, broju bankovnog računa, podatke o zaradama i dodatnim naknadama, poslovnoj e-mail adresi, IP (internet Protocol address), pristupnoj šifri i broju telefona, kao i druge neophodne podatke za izvršenje zakonom propisanih obaveza Rukovaoca i realizacije ugovora o radu odnosno drugog ugovornog odnosa.

Rukovalac može obrađivati i određene kategorije posebnih vrsta podataka o ličnosti, u skladu sa članom 17. Zakona (na primer, obrada posebne vrste podataka o ličnosti zaposlenih i članova njihovih porodica za svrhu izvršenja obaveza ili primene zakonom propisanih ovlašćenja u oblasti radnih odnosa, socijalnog osiguranja i socijalne zaštite). Rukovalac ne obrađuje veći broj ili drugu vrstu ličnih podataka od onih koji su potrebin da bi se ispunila navedena svrha.

Rukovalac ne može vršiti obradu podataka kojom se otkriva rasno ili etničko poreklo, političko mišljenje, versko ili filozofsko uverenje ili članstvo u sindikatu, kao i obrada genetskih podataka, biometrijskih podataka u cilju jedinstvene identifikacije lica, podataka o zdravstvenom stanju ili podataka o seksualnom životu ili seksualnoj orijentaciji fizičkog lica. Od ovog pravila dozvoljeni su izuzeci samo u slučajevima predviđenim članom 17. stav 2. Zakona.

Ukoliko se obrada posebnih vrsta podataka, shodno Zakonu, vrši na osnovu saglasnosti zaposlenih, ta saglasnost mora biti data u pisanoj formi koja obuhvata detaljne informacije o vrsti podataka koji se obrađuju, svrsi obrade i načinu korišćenja podataka.

#### Article 4.

The Controller processes the following personal data of employees, persons engaged to work, external associates and other persons entering contractual and other legal relations with the Controller:

- Name and surname, parent's name, address of residence/temporary residence, municipality of residence/temporary residence, date and place of birth, gender, unique personal identification number, unique foreigner's identification number, ID card number, passport number, citizenship, health insurance number, academic and professional qualifications, level of education, titles, data on skills, knowledge of foreign languages, training, employment history, biography, work experience, bank account number, data on salaries and additional fees, business email address, IP (Internet Protocol address), access password and telephone number, as well as other necessary data for the execution of the Controller's legal obligations and realization of the employment contract or other contractual relationship.

The Controller may also process certain categories of special types of personal data, in accordance with Article 17 of the Law (for example, processing a special type of personal data of employees and their family members for the purpose of fulfilling obligations or applying legally prescribed powers in the field of labor relations, social security and social protection). The Controller does not process a larger number or other type of personal data than those necessary to fulfill the stated purpose.

The Controller cannot process data that reveals racial or ethnic origin, political opinion, religious or philosophical belief or trade union membership, as well as process genetic data, biometric data for the purpose of unique identification of a person, data on health condition or data on sexual life or sexual orientation of an individual. Exceptions to this rule are only allowed in cases provided for in Article 17, paragraph 2 of the Law.

If the processing of special types of data, in accordance with the Law, is performed based on the consent of employees, that consent must be given in written form which includes detailed information on the type of data processed, the purpose of processing and the manner of using the data.

Rukovalac obrađuje sledeće podatke o ličnosti kandidata za posao:

- Ime i prezime, ime roditelja, adresa prebivališta/boravišta, opština prebivališta/boravišta, datum i mesto rođenja, pol, jedinstveni matični broj građana, jedinstveni matični broj stranaca, broj lične karte, broj pasoša, državljanstvo, akademske i profesionalne kvalifikacije, stepen obrazovanja, titule, podatke o veštinama, znanjima stranih jezika, obukama, istoriji zaposlenja, biografija, radno iskustvo, e-mail adresa, broj telefona.

Podaci o ličnosti dobijeni putem radnih biografija kandidata za zaposlenje, mogu biti u većem obimu od podataka navedenih u prethodnom stavu, ukoliko ih kandidati samoinicijativno dostavljaju.

Rukovalac može obrađivati sledeće podatke o ličnosti drugih lica (korisnici usluga/klijenti, poslovni partneri i sl.):

- Ime i prezime, naziv poslodavca/organa/organizacije koju lice predstavlja, datum rođenja, mesto rođenja, adresu prebivališta, pol, podatke o akademskim i profesionalnim/stručnim kvalifikacijama, kontakt adresa elektronske pošte, kontakt telefon. lični i kontakt podaci predstavnika, broj računa kompanije/organizacije i sl.);

Rukovalac u svrhu obučavanja AI algoritama u cilju poboljšanja medicinske dijagnostike i radioterapije korisnika usluga primarno prikuplja sledeću vrstu podataka o ličnosti:

- Anonimizovani zdravstveni podaci iz CT snimaka, kolonoskopije, magnetne rezonance, ultrazvuka itd.

U skladu sa članom 20. Zakona o zaštiti podataka o ličnosti, ako za ostvarivanje svrhe obrade nije potrebno da VINAVER MEDICAL DOO NOVI SAD identifikuje lice na koje se podaci odnose, Rukovalac nije dužan da zadrži, pribavi ili obradi dodatne informacije radi identifikacije tog lica samo u cilju primene Zakona.

The Controller processes the following personal data of job candidates:

- Name and surname, parent's name, address of residence/temporary residence, municipality of residence/temporary residence, date and place of birth, gender, unique personal identification number, unique foreigner's identification number, ID card number, passport number, citizenship, academic and professional qualifications, level of education, titles, data on skills, knowledge of foreign languages, training, employment history, biography, work experience, email address, phone number.

Personal data obtained through job candidates' resumes may be more extensive than the data listed in the previous paragraph if the candidates voluntarily provide them.

The Controller may process the following personal data of other persons (service users/clients, business partners, etc.):

- Name and surname, name of the employer/authority/organization represented by the person, date of birth, place of birth, address of residence, gender, data on academic and professional/expert qualifications, contact email address, contact phone number, personal and contact data of the representative, company/organization account number, etc.);

For the purpose of training AI algorithms to improve medical diagnostics and radiotherapy for service users, the Controller primarily collects the following type of personal data:

- Anonymized health data from CT scans, colonoscopies, magnetic resonance imaging, ultrasounds, etc.

In accordance with Article 20 of the Personal Data Protection Law, if it is not necessary for VINAVER MEDICAL DOO NOVI SAD to identify the person to whom the data relates in order to achieve the purpose of processing, the Controller is not obliged to retain, obtain or process additional information to identify that person solely for the purpose of applying the Law.

VINAVER MEDICAL DOO NOVI SAD prvenstveno obrađuje anonimizovane zdravstvene podatke iz CT snimaka, kolonoskopije, magnetne rezonance, ultrazvuka itd. u svrhu obučavanja AI algoritama za unapređenje dijagnostičkih i terapijskih metoda korisnika usluga.

Obrada ovih podataka ne zahteva identifikaciju lica na koje se podaci odnose.

U slučajevima obrade bez identifikacije, određena prava lica na koje se podaci odnose predviđena Zakonom se ne primenjuju ( iz člana 26. st. 1. do 4, člana 29, člana 30. st. 1. do 5, člana 31. st. 1. do 3, člana 33. st. 1. i 2. i člana 36. st. 1. do 4. ovog Zakona), osim ako lice dostavi dodatne informacije koje omogućavaju njegovu identifikaciju.

Informacije od javnog značaja koje sadrže podatke o ličnosti mogu biti učinjene dostupnim tražiocu od Rukovaoca, u skladu sa zakonom.

Na obradu jedinstvenog matičnog broja građana, primenjuju se odredbe zakona kojim se uređuje jedinstveni matičnu broj građana, odnosno odredbe drugog zakona uz primenu odredbi Zakona koje se odnose na zaštitu prava i sloboda lica na koje se podaci odnose.

Na obradu u oblasti rada i zapošljavanja primenjuju se odredbe zakona kojima se uređuje rad i zapošljavanje i opšti akti. uz primenu odredbi zakona kojim se uređuje zaštita podataka o ličnosti.

#### **Svrha obrade podataka Član 5.**

Rukovalac obrađuje podatke o ličnosti u svrhe utvrđene u ovom članu, s tim da ne obrađuje više podataka, odnosno širi krug podataka od onih koji su neophodni za ostvarenje ovih svrha.

Svrhe u koje se obrađuju podaci o ličnosti su:

- 1) zapošljavanje i upravljanje ljudskim resursima - Rukovalac obrađuje podatke o ličnosti za potrebe zasnivanja i realizacije radnog odnosa i drugih oblika radnog angažovanja (na primer, obrada podataka o ličnosti za potrebe: utvrđivanja znanja i veština kandidata za određena radna mesta, upravljanja radnim vremenom i odsustvima sa rada, obračun

VINAVER MEDICAL DOO NOVI SAD primarily processes anonymized health data from CT scans, colonoscopies, magnetic resonance imaging, ultrasounds, etc. for the purpose of training AI algorithms to improve diagnostic and therapeutic methods for service users.

Processing this data does not require identification of the persons to whom the data relates.

In cases of processing without identification, certain rights of the person to whom the data relates, as provided for in Article 26, paragraphs 1 to 4, Article 29, Article 30, paragraphs 1 to 5, Article 31, paragraphs 1 to 3, Article 33, paragraphs 1 and 2, and Article 36, paragraphs 1 to 4 of this Law, do not apply, unless the person provides additional information that enables their identification.

Information of public importance containing personal data may be made available to the applicant by the Controller, in accordance with the law.

The processing of the unique personal identification number is subject to the provisions of the law governing the unique personal identification number, or the provisions of another law with the application of the provisions of the Law relating to the protection of the rights and freedoms of the person to whom the data relates.

The provisions of the laws governing labor and employment and general acts apply to processing in the field of labor and employment, with the application of the provisions of the law governing personal data protection.

#### **Purpose of data processing Article 5.**

The Controller processes personal data for the purposes set out in this Article, provided that it does not process more data or a wider range of data than is necessary to achieve these purposes.

The purposes for which personal data is processed are:

- 1) Employment and human resource management - The Controller processes personal data for the purposes of establishing and realizing an employment relationship and other forms of work engagement (e.g. processing personal data for the purposes of: determining the knowledge and skills of candidates for certain jobs, managing working hours and absences from work,



zarada, putnih troškova i dnevnica, utvrđivanja naknada po osnovu bolovanja i drugih vidova odsustva sa radnog mesta, procene napredovanja zaposlenih, obezbeđivanja dodatnih obuka i edukacija i disciplinske postupke);

- 2) obavljanje delatnosti i vršenje poslovnih aktivnosti - Rukovalac je registrovan pod šifrom 7219 - Istraživanje i razvoj u ostalim prirodnim i tehničko-tehnološkim naukama, te anonimizovane podatke o ličnosti isti primarno obrađuje radi obučavanja AI algoritma za unapređenje dijagnostičkih ili terapijskih metoda korisnika svojih usluga.

Rukovalac takođe obrađuje podatke o ličnosti za potrebe nabavke i plaćanja roba i usluga, poslovni razvoj, poslovnu saradnju, upravljanje projektima, organizaciju rada, kancelarijsko poslovanje i druge vidove obavljanja delatnosti i sprovođenja poslovnih aktivnosti, uključujući izveštavanje klijenata o sprovedenim poslovnim aktivnostima;

- 3) komunikacija, informacione tehnologije i informaciona bezbednost - Rukovalac obrađuje podatke o ličnosti u svrhu upravljanja i održavanja funkcionisanja komunikacijske i informacione mreže, održavanja informacione bezbednosti i prevencije ostvarenja informacionih rizika;
- 4) usklađivanje poslovanja sa zakonima i drugim propisima - Rukovalac obrađuje podatke o ličnosti radi ispunjenja propisanih obaveza i usklađivanja poslovanja sa zakonima i drugim propisima (trgovinsko, radno i poresko zakonodavstvo i dr).

#### **Pravni osnov za prikupljanje podataka o ličnosti Član 6.**

Rukovalac može obrađivati podatke o ličnosti ako je ispunjen jedan od sledećih uslova:

- 1) ako je lice na koje se podaci o ličnosti odnose pristalo na obradu svojih podataka o ličnosti za jednu ili više posebno određenih svrha;
- 2) ako je obrada neophodna za izvršenje ugovora zaključenog sa licem na koje se podaci odnose (radi isporuke proizvoda, pružanja usluga, obavljanja

calculating salaries, travel expenses and per diems, determining compensation for sick leave and other types of absence from the workplace, evaluating employee advancement, providing additional training and education, and disciplinary proceedings);

- 2) Carrying out activities and business operations - The Controller is registered under code 7219 - Research and development in other natural and technical-technological sciences, and primarily processes anonymized personal data for the purpose of training AI algorithms to improve diagnostic or therapeutic methods for users of its services.

The Controller also processes personal data for the purposes of procurement and payment of goods and services, business development, business cooperation, project management, work organization, office operations and other forms of carrying out activities and conducting business operations, including reporting to clients on business activities carried out;

- 3) Communication, information technology and information security - The Controller processes personal data for the purpose of managing and maintaining the functioning of the communication and information network, maintaining information security and preventing the realization of information risks;
- 4) Compliance of operations with laws and other regulations - The Controller processes personal data in order to fulfill prescribed obligations and align operations with laws and other regulations (commercial, labor and tax legislation, etc.).

#### **Legal Basis for Collecting Personal Data Article 6.**

The Controller may process personal data if one of the following conditions is met:

- 1) if the person to whom the personal data relates has consented to the processing of their personal data for one or more specific purposes;
- 2) if the processing is necessary for the performance of a contract concluded with the person to whom the data relates (for the delivery of products, provision of

<p>transakcija i sl.) ili za preduzimanje radnji, na zahtev lica na koje se podaci odnose, pre zaključenja ugovora (radi obrađivanja i dostavljanja ponuda, poručivanja proizvoda i usluga i sl.);</p> <p>3) ako je obrada neophodna u cilju poštovanja obaveza rukovaoca predviđenih zakonskim propisima;</p> <p>4) ako je obrada neophodna u cilju zaštite životno važnih interesa lica na koje se podaci odnose ili drugog fizičkog lica;</p> <p>5) ako je obrada neophodna u cilju obavljanja poslova u javnom interesu ili izvršenja zakonom propisanih ovlašćenja rukovaoca;</p> <p>6) ako je obrada neophodna u cilju ostvarivanja legitimnih interesa rukovaoca ili treće strane, osim ako su nad tim interesima pretežniji interesi ili osnovna prava i slobode lica na koje se podaci odnose koji zahtevaju zaštitu podataka o ličnosti, a posebno ako je lice na koje se podaci odnose maloletno lice.</p> <p>Ukoliko se obrada podataka o ličnosti vrši na osnovu pristanka on se daje u pisanoj formi i predstavlja dobrovoljno, određeno, informisano i nedvosmisleno izražavanje volje tog lica, kojim se ono saglašava sa obradom podataka o ličnosti koji se na njega odnose.</p> <p>Ako se pristanak lica na koje se podaci odnose daje u okviru pismene izjave koja se odnosi i na druga pitanja, zahtev za davanje pristanka mora biti predstavljen na način kojim se izdvaja od tih drugih pitanja, u razumljivom i lako dostupnom obliku, kao i uz upotrebu jasnih i jednostavnih reči.</p> <p>Lice pre davanja pristanka mora biti obavješteno o:</p> <ul style="list-style-type: none"> <li>– vrsti podataka koji se obrađuju,</li> <li>– svrsi obrade,</li> <li>– načinu korišćenja podataka i rokovima čuvanja, kao i</li> <li>– pravu lica na koje se podaci odnose da opozove pristanak u svakom trenutku.</li> </ul> <p>Opoziv pristanka ne utiče na dopuštenost obrade koja je vršena na osnovu pristanka pre opoziva. Opozivanje pristanka mora biti jednostavno, kao i davanje pristanka.</p>	<p>services, execution of transactions, etc.) or for taking actions, at the request of the person to whom the data relates, prior to the conclusion of the contract (for processing and submitting offers, ordering products and services, etc.);</p> <p>3) if the processing is necessary for the purpose of complying with the obligations of the Controller stipulated by legal regulations;</p> <p>4) if the processing is necessary for the purpose of protecting the vital interests of the person to whom the data relates or another natural person;</p> <p>5) if the processing is necessary for the purpose of performing tasks in the public interest or exercising statutory powers of the Controller;</p> <p>6) if the processing is necessary for the purpose of achieving the legitimate interests of the Controller or a third party, unless the interests or fundamental rights and freedoms of the person to whom the data relates, which require the protection of personal data, prevail over those interests, especially if the person to whom the data relates is a minor.</p> <p>If the processing of personal data is carried out on the basis of consent, it is given in written form and represents a voluntary, specific, informed and unambiguous expression of will of that person, by which they agree to the processing of personal data relating to them.</p> <p>If the consent of the person to whom the data relates is given within a written statement relating to other matters, the request for consent must be presented in a manner that separates it from those other matters, in an understandable and easily accessible form, and using clear and simple words.</p> <p>Before giving consent, the person must be informed about:</p> <ul style="list-style-type: none"> <li>– the type of data being processed,</li> <li>– the purpose of processing,</li> <li>– the manner of using the data and the retention periods, as well as</li> <li>– the right of the person to whom the data relates to withdraw consent at any time.</li> </ul> <p>The withdrawal of consent does not affect the lawfulness of processing carried out on the basis of consent before its withdrawal. The withdrawal of consent must be as simple as giving consent.</p>
---	--

Kada se podaci o ličnosti prikupljaju i obrađuju u cilju poštovanja obaveza rukovaoca ili izvršenja zakonom propisanih ovlašćenja rukovaoca, obrada se vrši uvek u meri u kojoj je to predviđeno zakonom uz primenu opštih načela obrade i adekvatnih mera zaštite.

Akt (Opšta Uredba) o veštačkoj inteligenciji (AI Act) pruža izuzeće od člana 9. Opšte uredbe o zaštiti podataka Evropske unije za obradu posebnih kategorija podataka (kao što su podaci o zdravlju) u svrhu praćenja pristrasnosti kod visokorizičnih AI sistema (vidi član 29. ovog Pravilnika).

#### **Izvor prikupljanja podataka o ličnosti Član 7.**

Rukovalac može prikupljati podatke o ličnosti neposredno od lica na koje se odnose u kom slučaju je dužan da tom licu u trenutku prikupljanja podataka dostavi obaveštenje koje sadrži informacije predviđene članom 23. Zakona.

Podaci o ličnosti se mogu prikupljati i od drugih lica, odnosno iz javno dostupnih izvora, u kom slučaju je Rukovalac dužan da licu na koje se podaci odnose pruži informacije predviđene članom 24. Zakona.

Primarni izvor podataka koje VINAVER MEDICAL DOO NOVI SAD obrađuje su korisnici usluga i to bolnice i klinike koje prikupljaju ove podatke u dijagnostičke svrhe.

VINAVER MEDICAL DOO NOVI SAD će kao obrađivač sa korisnicima usluga iz prethodnog stava zaključiti poseban ugovor kojim će se regulisati međusobna prava i obaveze povodom obrade podataka.

#### **Poveravanje obrade podataka drugom licu, prenošenje podataka, iznošenje podataka o ličnosti u drugu državu ili međunarodnu organizaciju. Član 8.**

Rukovalac može poveriti obradu podataka drugom licu (obrađivaču), ali samo pod uslovom da to drugo lice u potpunosti garantuje primenu odgovarajućih tehničkih, organizacionih i kadrovskih mera, na način koji obezbeđuje da se obrada vrši u skladu sa odredbama Zakona i da se obezbeđuje zaštita prava lica na koje se podaci odnose.

When personal data is collected and processed for the purpose of complying with the obligations of the Controller or exercising the statutory powers of the Controller, the processing is always carried out to the extent provided for by law, with the application of general processing principles and adequate protection measures.

The the Artificial Intelligence Act (AI Act), provides an exemption from Article 9 of the European Union's General Data Protection Regulation for the processing of special categories of data (such as health data) for the purpose of monitoring bias in high-risk AI systems (see Article 27 of this Rulebook).

#### **Source of Collecting Personal Data Article 7.**

The Controller may collect personal data directly from the person to whom it relates, in which case it is obliged to provide that person with a notification containing the information stipulated in Article 23 of the Law at the time of data collection.

Personal data may also be collected from other persons or from publicly available sources, in which case the Controller is obliged to provide the person to whom the data relates with the information stipulated in Article 24 of the Law.

The primary source of data that VINAVER MEDICAL DOO NOVI SAD processes are service users, namely hospitals and clinics that collect this data for diagnostic purposes.

VINAVER MEDICAL DOO NOVI SAD will conclude a separate contract with the service users from the previous paragraph as a processor, which will regulate their mutual rights and obligations regarding data processing.

#### **Entrusting Data Processing to Another Entity, Transferring Data, Transferring Personal Data to Another Country or International Organization Article 8.**

The Controller may entrust the processing of data to another entity (processor), but only if that other entity fully guarantees the application of appropriate technical, organizational and personnel measures in a manner that ensures that the processing is carried out in accordance with the provisions of the Law and that the protection of the rights of the person to whom the data relates is ensured.

U slučaju iz prethodnog stava ovog člana Rukovalac će sa obrađivačem zaključiti poseban ugovor kojim će se regulisati međusobna prava i obaveze povodom obrade podataka.

#### **Član 9.**

Rukovalac može ustupati podatke o ličnosti trećoj strani (npr. povezana lica, poslovni partneri i druga lica koja pružaju usluge u ime Rukovaoca) kada je to neophodno, pod uslovom da je obezbeđen adekvatan nivo zaštite utvrđen Zakonom i ovim Pravilnikom.

#### **Član 10.**

Prenos podataka o ličnosti u drugu državu, na deo njene teritorije, ili u jedan ili više sektora određenih delatnosti u toj državi ili u međunarodnu organizaciju, bez prethodnog odobrenja, može se izvršiti ako je utvrđeno da ta druga država, deo njene teritorije ili jedan ili više sektora određenih delatnosti u toj državi ili ta međunarodna organizacija obezbeđuje primereni nivo zaštite podataka o ličnosti.

Smatra se da je primereni nivo zaštite iz stava 1. ovog člana obezbeđen u državama i međunarodnim organizacijama koje su članice Konvencije Saveta Evrope o zaštiti lica u odnosu na automatsku obradu ličnih podataka, odnosno u državama, na delovima njihovih teritorija ili u jednom ili više sektora određenih delatnosti u tim državama ili međunarodnim organizacijama za koje je od strane Evropske unije utvrđeno da obezbeđuju primereni nivo zaštite, a čiji se spisak objavljuje u „Službenom glasniku Republike Srbije”.

#### **Član 11.**

U države, delove njenih teritorija ili u jedan ili više sektora određenih delatnosti u tim državama ili u međunarodnim organizacijama za koje listom koju Vlada Republike Srbije objavljuje u „Službenom glasniku Republike Srbije” nije utvrđeno postojanje primerenog nivoa zaštite, Rukovalac može prenositi podatke samo ako je Rukovalac, odnosno obrađivač obezbedio odgovarajuće mere zaštite ovih podataka i ako je licu na koje se podaci odnose obezbeđena ostvarivost njegovih prava i delotvorna pravna zaštita.

#### **Obezbeđenje i zaštita podataka o ličnosti Član 12.**

In the case referred to in the previous paragraph of this Article, the Controller will conclude a separate contract with the processor to regulate their mutual rights and obligations regarding data processing.

#### **Article 9.**

The Controller may disclose personal data to a third party (e.g. affiliated entities, business partners and other entities providing services on behalf of the Controller) when necessary, provided that an adequate level of protection established by the Law and these Regulations is ensured.

#### **Article 10.**

The transfer of personal data to another country, part of its territory, or one or more sectors of certain activities in that country or to an international organization, without prior approval, may be carried out if it is established that that other country, part of its territory or one or more sectors of certain activities in that country or that international organization ensures an adequate level of personal data protection.

It is considered that an adequate level of protection referred to in paragraph 1 of this Article is ensured in the countries and international organizations that are members of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, or in countries, parts of their territories or in one or more sectors of certain activities in those countries or international organizations for which the European Union has determined that they ensure an adequate level of protection, and whose list is published in the "Official Gazette of the Republic of Serbia".

#### **Article 11.**

To countries, parts of their territories or one or more sectors of certain activities in those countries or international organizations for which the list published by the Government of the Republic of Serbia in the "Official Gazette of the Republic of Serbia" has not established the existence of an adequate level of protection, the Controller may transfer data only if the Controller or the processor has provided appropriate safeguards for the protection of this data and if the person to whom the data relates is ensured the exercise of their rights and effective legal protection.

#### **Ensuring and Protecting Personal Data Article 12.**

Prilikom prikupljanja i obrade podataka o ličnosti Rukovalac primenjuje tehničke, organizacione i kadrovske mere, koje imaju za cilj obezbeđivanje delotvorne primene načela zaštite podataka o ličnosti i obezbeđuje primenu neophodnih mehanizama zaštite u toku obrade.

Stalnom primenom odgovarajućih tehničkih, organizacionih i kadrovskih mera Rukovalac obezbeđuje da se uvek obrađuju samo oni podaci o ličnosti koji su neophodni za ostvarivanje svake pojedinačne svrhe obrade.

Ta se obaveza primenjuje u odnosu na broj prikupljenih podataka, obim njihove obrade, rok njihovog pohranjivanja i njihovu dostupnost.

### **Član 13.**

Prema potrebi, tehničke, organizacione i kadrovske mere naročito obuhvataju:

- 1) pseudonimizaciju kao obradu na način koji onemogućava pripisivanje podataka o ličnosti određenom licu bez korišćenja dodatnih podataka, pod uslovom da se ovi dodatni podaci čuvaju posebno i da su preduzete tehničke, organizacione i kadrovske mere koje obezbeđuju da se podatak o ličnosti ne može pripisati određenom ili odredivom licu;
- 2) kriptozastitu podataka uključujući i šifrovanje, obradu putem sistema lozinki i sl.;
- 3) sposobnost obezbeđivanja trajne poverljivosti, integriteta, raspoloživosti i otpornosti sistema i usluga obrade;
- 4) obezbeđivanje uspostavljanja ponovne raspoloživosti i pristupa podacima o ličnosti u slučaju fizičkih ili tehničkih incidenata u najkraćem roku;
- 5) postupak redovnog testiranja, ocenjivanja i ažuriranja delotvornosti tehničkih, organizacionih i kadrovskih mera bezbednosti obrade.

Mere zaštite koje Rukovalac primenjuje moraju biti takve da se obezbedi da se bez učešća fizičkog lica podaci o ličnosti ne mogu učiniti dostupnim neograničenom broju fizičkih lica.

### **Član 14.**

When collecting and processing personal data, the Controller applies technical, organizational and personnel measures aimed at ensuring the effective application of the principles of personal data protection and ensures the application of necessary protection mechanisms during processing.

Through the continuous application of appropriate technical, organizational and personnel measures, the Controller ensures that only the personal data necessary for achieving each individual purpose of processing is processed.

This obligation applies in relation to the number of data collected, the scope of their processing, the period of their storage and their availability.

### **Article 13.**

As needed, the technical, organizational and personnel measures shall in particular include:

- 1) pseudonymization as processing in a manner that prevents the attribution of personal data to a specific person without the use of additional data, provided that this additional data is kept separately and that technical, organizational and personnel measures have been taken to ensure that the personal data cannot be attributed to an identified or identifiable person;
- 2) cryptographic protection of data, including encryption, processing through password systems, etc.;
- 3) the ability to ensure the permanent confidentiality, integrity, availability and resilience of processing systems and services;
- 4) ensuring the establishment of data recovery and access to personal data in the shortest possible time in the event of physical or technical incidents;
- 5) a procedure for regularly testing, evaluating and updating the effectiveness of technical, organizational and personnel security measures for processing.

The protection measures applied by the Controller must be such as to ensure that personal data cannot be made available to an unlimited number of individuals without the participation of an individual.

### **Article 14.**

U cilju obezbeđenja i zaštite podataka o ličnosti Rukovalac će u zavisnosti od potrebnog nivoa obezbeđenja u odnosu na vrstu podataka, prirodu, obim, okolnosti i svrhu obrade, kao i verovatnoću nastupanja rizika i nivoa rizika za prava i slobode fizičkih lica sprovoditi odgovarajuće postupke i mere za zaštitu podataka o ličnosti.

Posebne procedure i postupanja zaposlenih i drugih radno angažovanih lica u vezi sa zaštitom podataka o ličnosti Rukovalac će u zavisnosti od potrebe i konkretne situacije detaljnije predvideti svojim internim aktima i/ili u ugovorima o radu i/ili ovlašćenjima i sl.

Rukovalac je dužan da sve zaposlene upozna sa obavezom zaštite podataka o ličnosti kao i njihovom odgovornošću u smislu važećih propisa i ovog Pravilnika.

#### **Član 15.**

Postupci i mere koje Rukovalac primenjuje radi obezbeđenja i zaštite podataka o ličnosti podrazumevaju:

- pravo na pristup podacima o ličnosti dozvoljeno je samo ovlašćenim licima kojima je to u opisu poslova koje obavljaju, ili koja su za to posebno ovlašćena;
- u slučaju ugovorne obrade podataka zaključuje se pismeni ugovor o obradi podataka o ličnosti kojim se obezbeđuje adekvatan nivo zaštite podataka o ličnosti;
- pravo zaposlenih i drugih angažovanih lica na pristup podacima o ličnosti mora biti primereno njihovim radnim, odnosno ugovorenim zadacima;
- čuvanje podataka, bez obzira u kom obliku se čuvaju (registratori, fascikle, dokumenta, diskovi, memorije itd.) moraju se čuvati na način da budu nedostupni neovlašćenim licima (zaključani u ormarima, radnim stolovima, pod lozinkom i sl.);
- za rad na računarima na kojima su smešteni podaci o ličnosti predviđa se obaveza korišćenja lozinki i to sa propisanom dužinom i strukturom lozinki;
- podrazumeva se redovna izmena lozinki;
- praćenje pristupa i promena unosa podataka o ličnosti;
- upoznavanje zaposlenih i drugih angažovanih lica koja imaju pristup podacima sa postupcima i merama za zaštitu podataka o ličnosti;

In order to ensure and protect personal data, the Controller will, depending on the required level of security in relation to the type of data, the nature, scope, circumstances and purpose of processing, as well as the probability of risk and the level of risk to the rights and freedoms of individuals, implement appropriate procedures and measures for the protection of personal data.

The Controller will, depending on the need and specific situation, provide more detailed procedures and actions of employees and other engaged persons in connection with the protection of personal data through its internal acts and/or employment contracts and/or authorizations, etc.

The Controller is obliged to inform all employees about the obligation to protect personal data, as well as their responsibility in terms of applicable regulations and these Regulations.

#### **Article 15.**

The procedures and measures applied by the Controller to ensure and protect personal data include:

- The right to access personal data is only allowed to authorized persons whose job description includes this, or who are specifically authorized for it;
- In case of contracted data processing, a written contract on personal data processing is concluded to ensure an adequate level of personal data protection;
- The right of employees and other engaged persons to access personal data must be commensurate with their work or contracted tasks;
- Storing data, regardless of the form in which it is stored (registers, files, documents, disks, memories, etc.), must be done in a way that makes it inaccessible to unauthorized persons (locked in cabinets, desks, password protected, etc.);
- For working on computers where personal data is stored, the use of passwords is required, with prescribed password length and structure;
- Regular password changes are required;
- Monitoring access and changes to personal data entries;
- Informing employees and other engaged persons who have access to data about the procedures and measures for personal data protection;

- uništavanje podataka o ličnosti po isteku roka čuvanja na način kojim se obezbeđuje da podatak postane neprepoznatljiv i neobnovljiv;
- preduzimanje informaciono-tehničkih mera (ograničen pristup mreži, redovno ažuriranje protivvirusne zaštite, kriptovanje podataka, čuvanje sigurnosnih kopija i sl.).

Pored gore navedenih mera u ovom članu, Rukovalac može koristiti i druge raspoložive mere i postupke u cilju zaštite podataka o ličnosti, a naročito će posvetiti oprez ukoliko se radi o posebnoj vrsti podataka o ličnosti iz čl. 4, stav 2. ovog Pravilnika, kao i anonimizovanim zdravstveni podaci iz CT snimaka, kolonoskopije, magnetne rezonance, ultrazvuka itd i to na sledeći način:

- korišćenjem dvofaktorske autentifikacije (2FA) za pristup osetljivim podacima.
- enkripcijom najsenzitivnijih podataka korišćenjem 256-bitne AES enkripcije.
- bezbednim skladištenjem podataka na NAS uređajima i AWS serverima, oba opremljena 2FA i dodatnim merama bezbednosti.

Zaposleni su dužni da se u potpunosti pridržavaju pravila postupanja prilikom prikupljanja i obrade podataka, kao i da bez izuzetka primenjuju sve mere koje je Rukovalac predvideo u vezi sa zaštitom podataka o ličnosti.

### **Skladištenje podataka o ličnosti Član 16.**

VINAVER MEDICAL DOO NOVI SAD primenjuje hibridnu strategiju skladištenja podataka koja kombinuje lokalno skladištenje i skladištenje u oblaku.

### **Član 17.**

Lokalno skladištenje – Koristi se za skladištenje najsenzitivnijih podataka uz primenu jakih kontrola pristupa, enkripcije i mera mrežne bezbednosti. Omogućava direktnu kontrolu nad upravljanjem podacima radi usklađenosti sa propisima.

Obezbeđuje brz pristup podacima za treniranje AI modela.

### **Član 18.**

- Destroying personal data after the retention period expires in a manner that ensures the data becomes unrecognizable and unrecoverable;
- Implementing information technology measures (restricted network access, regular anti-virus updates, data encryption, backup storage, etc.).

In addition to the measures listed in this article, the Controller may use other available measures and procedures to protect personal data, and will exercise particular caution when dealing with special categories of personal data from Art. 4, paragraph 2 of these Regulations, as well as anonymized health data from CT scans, colonoscopies, MRIs, ultrasounds, etc., in the following manner:

- Using two-factor authentication (2FA) to access sensitive data.
- Encrypting the most sensitive data using 256-bit AES encryption.
- Securely storing data on NAS devices and AWS servers, both equipped with 2FA and additional security measures.

Employees are obliged to fully adhere to the rules of conduct when collecting and processing data, and to apply without exception all measures envisaged by the Controller in relation to the protection of personal data.

### **Storage of Personal Data Article 16.**

VINAVER MEDICAL DOO NOVI SAD applies a hybrid data storage strategy that combines local storage and cloud storage:

### **Article 17.**

Local Storage - Used for storing the most sensitive data with strong access controls, encryption and network security measures applied. Enables direct control over data management for regulatory compliance.

Provides fast access to data for training AI models.

### **Article 18.**

<p>Skladištenje u oblaku - Pruža skalabilnost za upravljanje velikim skupovima podataka i pikovima u prikupljanju podataka.</p> <p>Koristi se za skladištenje manje osetljivih, anonimizovanih ili enkriptovanih podataka.</p> <p>Snažnije i izdržljivije mogućnosti za rezervno kopiranje podataka, oporavak u slučaju incidenta i otpornost na bezbednosne rizike.</p>	<p>Cloud Storage - Provides scalability for managing large data sets and spikes in data collection.</p> <p>Used for storing less sensitive, anonymized or encrypted data.</p> <p>Robust options for data backup, incident recovery and resilience to security risks.</p>
<p style="text-align: center;"><b>Član 19.</b></p> <p>Primenom odgovarajućih mera zaštite se obezbeđuje da se:</p> <ol style="list-style-type: none"> <li>1) onemogući neovlašćenom licu pristup opremi koja se koristi za obradu („kontrola pristupa opremi“);</li> <li>2) spreči neovlašćeno čitanje, umnožavanje, izmena ili uklanjanje nosača podataka („kontrola nosača podataka“);</li> <li>3) spreči neovlašćeno unošenje podataka o ličnosti, kao i neovlašćena izmena, brisanje i kontrola pohranjenih podataka o ličnosti („kontrola pohranjivanja“);</li> <li>4) spreči korišćenje sistema za automatsku obradu od strane neovlašćenog lica, upotrebom opreme za prenos podataka („kontrola upotrebe“);</li> <li>5) osigura da lice koje je ovlašćeno za korišćenje sistema za automatsku obradu ima pristup samo onim podacima o ličnosti na koje se odnosi njegovo ovlašćenje za pristup podacima („kontrola pristupa podacima“);</li> <li>6) može proveriti, odnosno ustanoviti kome su podaci o ličnosti preneti, mogu biti preneti ili učinjeni dostupnim, upotrebom opreme za prenos podataka („kontrola prenosa“);</li> <li>7) može naknadno proveriti, odnosno utvrditi koji su podaci o ličnosti uneti u sistem automatske obrade, od strane kog lica i kada su uneti („kontrola unosa“);</li> <li>8) spreči neovlašćeno čitanje, umnožavanje, izmena ili brisanje podataka o ličnosti u toku njihovog prenosa ili u toku prevoza nosača podataka („kontrola prevoza“);</li> <li>9) ponovo uspostavi instalirani sistem u slučaju prekida njegovog rada („obnavljanje sistema“);</li> </ol>	<p style="text-align: center;"><b>Article 19.</b></p> <p>By applying appropriate safeguards, it is ensured that:</p> <ol style="list-style-type: none"> <li>1) Unauthorized persons are prevented from accessing equipment used for processing ("equipment access control");</li> <li>2) Unauthorized reading, copying, modification or removal of data media is prevented ("data media control");</li> <li>3) Unauthorized entry, modification, deletion and control of stored personal data is prevented ("storage control");</li> <li>4) Use of automated processing systems by unauthorized persons is prevented by using data transmission equipment ("user control");</li> <li>5) Persons authorized to use an automated processing system only have access to the personal data covered by their access authorization ("data access control");</li> <li>6) It can be verified to which bodies personal data have been or may be transmitted or made available using data transmission equipment ("transmission control");</li> <li>7) It can be subsequently verified which personal data have been entered into automated processing systems, when and by whom ("input control");</li> <li>8) Unauthorized reading, copying, modification or deletion of personal data is prevented during transmission or transport ("transport control");</li> <li>9) The installed system can be re-established in case of interruption ("recovery");</li> </ol>



10) osigura da sistem ispravno radi i da se greške u radu sistema uredno prijavljuju („pouzdanost“), kao i da se pohranjeni podaci o ličnosti ne mogu ugroziti zbog nedostataka u radu sistema („integritet“).

### **Procena uticaja na zaštitu podataka o ličnosti Član 20.**

Rukovalac je dužan da pre nego što započne sa obradom, izvrši procenu uticaja predviđenih radnji obrade na zaštitu podataka o ličnosti u skladu sa zakonom i podzakonskim aktom, ako je verovatno da će neka vrsta obrade, posebno upotrebom novih tehnologija i uzimajući u obzir prirodu, obim, okolnosti i svrhu obrade prouzrokovati visok rizik za prava i slobode fizičkih lica.

U slučaju da Rukovalac proceni da neka obrada ima visok stepen rizika po obradu ličnih podataka, doneće odluku o sprovođenju Procene uticaja na zaštitu podataka o ličnosti u odnosu na konkretnu obradu podataka.

Procena uticaja na zaštitu podataka o ličnosti sadrži najmanje sledeće elemente:

- 1) opis radnji obrade;
- 2) objašnjenje zašto je obrada neophodna i da li je srazmerna;
- 3) rizike i način odgovora na te rizike.

Ako Procena uticaja iz stava 1. ovog člana, ukaže da će nameravane radnje obrade proizvesti visok rizik ako se ne preduzmu mere za umanjene rizika, Rukovaoc će bez odlaganja zatražiti mišljenje Poverenika.

### **Član 21.**

Rukovalac će u skladu sa Odlukom o listi vrsta radnji obrade podataka o ličnosti za koje se mora izvršiti procena uticaja na zaštitu podataka o ličnosti i tražiti mišljenje Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti („Službeni glasnik RS“, br. 45/19 i 112/20“) listu radnji obrade podataka o ličnosti za koje rukovalac, pre nego što započne sa obradom, mora izvršiti procenu uticaja na zaštitu podataka o ličnosti i tražiti mišljenje Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti.

10) The system functions properly, that faults are reported ("reliability") and that stored personal data cannot be corrupted by system malfunctions ("integrity").

### **Impact Assessment on Personal Data Protection Article 20.**

The Controller is obliged to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data in accordance with the law and bylaws, before commencing the processing, if it is likely that a particular type of processing, especially when using new technologies and taking into account the nature, scope, circumstances and purposes of the processing, will result in a high risk to the rights and freedoms of individuals.

If the Controller assesses that certain processing poses a high degree of risk to personal data processing, it will decide to conduct a Personal Data Protection Impact Assessment in relation to that specific data processing.

The Personal Data Protection Impact Assessment shall contain at least the following elements:

- 1) A description of the processing operations;
- 2) An explanation of why the processing is necessary and proportionate;
- 3) The risks and how to respond to those risks.

If the Impact Assessment referred to in paragraph 1 of this Article indicates that the intended processing operations will result in a high risk if measures to mitigate the risk are not taken, the Controller shall, without delay, seek the opinion of the Commissioner.

### **Article 21.**

In accordance with the Decision on the list of types of personal data processing operations for which a personal data protection impact assessment must be carried out and the opinion of the Commissioner for Information of Public Importance and Personal Data Protection must be sought ("Official Gazette of RS", No. 45/19 and 112/20"), the Controller shall, before commencing processing, carry out a personal data protection impact assessment and seek the opinion of the Commissioner for Information of Public Importance and Personal Data Protection for the list of personal data processing operations.

**Bezbednosni incident  
Član 22.**

Rukovalac će u slučaju bezbednosnog incidenta koji ugrožava podatke o ličnosti:

1. blagovremeno primeniti sve mere u cilju saniranja posledica ovog incidenta;
2. obavestiti o incidentu Poverenika, ako se radi o incidentu iz člana. 52. stav 1. Zakona i ispuniti ostale obaveze koje se tiču prijavljivanja incidenta, a sve u skladu sa relevantnim odredbama Zakona;
3. bez odlaganja obavesti lice na koje se podaci odnose. ako povreda podataka o ličnosti može da proizvede visok rizik po prava i slobode fizičkih lica.

**Prava lica na koje se podaci odnose  
Član 23.**

**Pravo na pristup podacima** - Lice na koje se podaci odnose ima pravo da od Rukovaoca zahteva informaciju o tome da li obrađuje njegove podatke o ličnosti, kao i da zahteva pristup tim podacima.

**Pravo na ispravku podataka** - Lice na koje se podaci odnose ima pravo da se njegovi netačni podaci o ličnosti bez nepotrebnog odlaganja isprave.

**Pravo na brisanje podataka** - Lice na koje se podaci odnose ima pravo da se njegovi podaci o ličnosti izbrišu u sledećim slučajevima:

- ako podaci o ličnosti više nisu neophodni za ostvarivanje svrhe zbog koje su prikupljeni ili na drugi način obrađivani;
- ako je lice na koje se podaci odnose opozvalo pristanak na osnovu kojeg se obrada vršila;
- lice na koje se podaci odnose je podnelo prigovor na obradu;
- podaci o ličnosti su nezakonito obrađivani;
- ako podaci o ličnosti moraju biti izbrisani u cilju izvršenja zakonskih obaveza rukovaoca.

**Pravo na ograničenje obrade podataka** - Lice na koje se podaci odnose ima pravo da se obrada njegovih podataka o ličnosti ograniči od strane Rukovaoca u slučaju da to lice osporava tačnost podataka o ličnosti; ili ako je obrada

**Security Incident  
Article 22.**

In the event of a security incident that jeopardizes personal data, the Controller will:

1. Timely implement all measures to remedy the consequences of this incident;
2. Notify the Commissioner of the incident, if it is an incident referred to in Article 52, paragraph 1 of the Law, and fulfill other obligations related to reporting the incident, all in accordance with the relevant provisions of the Law;
3. Without delay, notify the person to whom the data relates, if the personal data breach is likely to result in a high risk to the rights and freedoms of individuals.

**Rights of the Data Subject  
Article 23.**

**Right of access** - The data subject has the right to request from the Controller information on whether their personal data is being processed, as well as to request access to that data.

**Right to rectification** - The data subject has the right to have their inaccurate personal data rectified without undue delay.

**Right to erasure** - The data subject has the right to have their personal data erased in the following cases:

- if the personal data is no longer necessary for the purpose for which it was collected or otherwise processed;
- if the data subject has withdrawn the consent on which the processing was based;
- the data subject has objected to the processing;
- the personal data was unlawfully processed;
- the personal data has to be erased for compliance with a legal obligation of the Controller.

**Right to restriction of processing** - The data subject has the right to obtain restriction of processing of their personal data from the Controller in case the data subject contests the accuracy of the personal data; or if the processing is

nezakonita; ili Rukovaocu više nisu potrebni podaci o ličnosti za ostvarivanje svrhe obrade; ili je lice na koje se podaci odnose je podnelo prigovor na obradu.

**Pravo na prigovor** - Ako smatra da je to opravdano u odnosu na posebnu situaciju u kojoj se nalazi, lice na koje se podaci odnose ima pravo da u svakom trenutku podnese rukovaocu prigovor na obradu njegovih podataka o ličnosti, koja se vrši u cilju obavljanja poslova u javnom interesu ili izvršenja zakonom propisanih ovlašćenja rukovaoca, kao i koja se vrši u cilju ostvarenja legitimnih interesa rukovaoca ili treće strane, uključujući i profilisanje koje se zasniva na tim odredbama.

**Pravo na prenosivost** - Lice na koje se podaci odnose ima pravo da podatke prenese drugom rukovaocu ako je obrada zasnovana na pristanku, ili se obrada vrši automatizovano.

**Pravo protiv odlučivanja isključivo na osnovu automatizovane obrade** - Lice na koje se podaci odnose ima pravo da se na njega ne primenjuje odluka doneta isključivo na osnovu automatizovane obrade, uključujući i profilisanje, ako se tom odlukom proizvode pravne posledice po to lice ili ta odluka značajno utiče na njegov položaj.

**Pravo na podnošenje Pritužbe Povereniku** - Lice na koje se podaci odnose ima pravo da podnese pritužbu Povereniku ako smatra da je obrada podataka o njegovoj ličnosti izvršena suprotno odredbama Zakona.

**Pravo na sudsku zaštitu** - Lice čiji se podaci o ličnosti obrađuju od strane Rukovaoca, ima pravo na sudsku zaštitu podnošenjem tužbe, ako smatra da su povređena njegova prava propisana Zakonom i ovim Pravilnikom.

#### **Rok čuvanja podataka o ličnosti Član 24.**

Podaci o ličnosti neće biti zadržani duže nego što je to neophodno za ostvarenje svrhe za koju su prikupljeni.

Ako je rok čuvanja podataka o ličnosti propisan zakonom, Rukovalac zadržaće podatke u datom zakonskom roku.

unlawful; or the Controller no longer needs the personal data for the purposes of processing; or the data subject has objected to the processing.

**Right to object** - If justified by their particular situation, the data subject has the right to object at any time to the processing of their personal data carried out for the performance of a task in the public interest or in the exercise of official authority vested in the Controller, as well as processing for the purposes of the legitimate interests of the Controller or a third party, including profiling based on those provisions.

**Right to data portability** - The data subject has the right to receive their personal data in a structured, commonly used and machine-readable format and to transmit that data to another controller if the processing is based on consent or automated.

**Right not to be subject to automated decision-making** - The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

**Right to lodge a complaint with the Commissioner** - The data subject has the right to lodge a complaint with the Commissioner if they consider that the processing of their personal data infringes the Law.

**Right to judicial protection** - The data subject whose personal data is processed by the Controller has the right to judicial protection by filing a lawsuit if they consider their rights under the Law and these Regulations have been violated.

#### **Retention Period for Personal Data Article 24.**

Personal data will not be retained longer than is necessary to fulfill the purpose for which it was collected.

If the retention period for personal data is prescribed by law, the Controller will retain the data for the given legal period.

Nakon ispunjenja svrhe, odnosno isteka zakonom propisanog roka za čuvanje podataka, podaci će biti trajno obrisani.

U određenim slučajevima, podaci o ličnosti mogu se čuvati duži period, za potrebe ispunjenja zakonskih obaveza ili za uspostavljanje, vršenje ili odbranu pravnog zahteva, u skladu sa važećim zakonima.

U slučaju da se podaci o ličnosti obrađuju isključivo na osnovu saglasnosti lica na koje se odnose, podaci će biti sačuvani do povlačenja iste saglasnosti.

Nakon isteka roka čuvanja podaci se uništavaju na način kojim se obezbeđuje da podatak postane neprepoznatljiv i neobnovljiv.

### **Evidencije o radnjama obrade Član 25.**

Rukovalac vodi evidencije o prikupljenim podacima o ličnosti, kao i o radnjama obrade za koje je odgovoran, a u svemu u skladu sa Zakonom.

Rukovalac podataka, dužan je pa vodi evidencije o radnjama obrade podataka o ličnosti, za koje je odgovoran, a koja sadrži informacije o:

1. Nazivu evidencije podataka o ličnosti;
2. Vrsti podataka o ličnosti koji se obrađuju;
3. Vrsti radnji obrade;
4. Nazivu, sedištu, adresi Rukovaoca podacima, e-mail adresi (registrovanim u APP-u), telefonu;
5. Imenu i kontakt podacima lica za zaštitu podataka o ličnosti;
6. Svrsi obrade;
7. Datumu započinjanja obrade, odnosno uspostavljanja evidencije;
8. Pravnom osnovu obrade;
9. Kategoriji lica na koje se podaci o ličnosti odnose;
10. Načinu prikupljanja podataka o ličnosti;
11. Roku posle čijeg isteka se brišu određene vrste podataka o ličnosti, ako je takav rok određen;
12. Vrsti primalaca kojima su podaci o ličnosti otkriveni ili će biti otkriveni, uključujući i primaoca u drugim državama ili međunarodnim organizacijama;

After the purpose has been fulfilled or the legally prescribed retention period has expired, the data will be permanently deleted.

In certain cases, personal data may be kept for a longer period, for the purpose of fulfilling legal obligations or for the establishment, exercise or defense of a legal claim, in accordance with applicable laws.

If personal data is processed solely on the basis of consent from the person to whom it relates, the data will be kept until such consent is withdrawn.

After the retention period expires, the data is destroyed in a manner that ensures the data becomes unrecognizable and unrecoverable.

### **Records of Processing Activities Article 25.**

The Controller maintains records of the personal data collected, as well as the processing activities for which it is responsible, all in accordance with the Law.

The Data Controller is obliged to keep records of personal data processing activities for which it is responsible, containing information on:

1. The name of the personal data record;
2. The type of personal data being processed;
3. The type of processing activities;
4. The name, registered office, address of the Data Controller, email address (registered in the Business Registers Agency), telephone number;
5. The name and contact details of the personal data protection officer;
6. The purpose of processing;
7. The date of commencement of processing or establishment of the record;
8. The legal basis for processing;
9. The category of individuals to whom the personal data relates;
10. The manner of collecting personal data;
11. The period after which certain types of personal data are deleted, if such a period is determined;
12. The type of recipients to whom the personal data has been or will be disclosed, including recipients in other countries or international organizations;

13. Prenosu podataka o ličnosti u druge države ili međunarodne organizacije, uključujući i naziv druge države ili međunarodne organizacije;
14. Opštem opisu mera zaštite utvrđene Zakonom (organizacione, kadrovske i tehničke mere);
15. Datumu ažuriranja evidencije.

Rukovalac podataka je dužan da ažurira evidencije, kada dođe do promene u vezi sa osnovnim podacima iz stava 1. ovog člana.

### **Obaveze zaposlenih Član 26.**

Svi zaposleni i druga radno angažovana lica, kao i ovlašćena lica od strane Rukovaoca koji prikupljaju i obrađuju podatke o ličnosti u ime ili za potrebe Rukovaoca, dužni su da se prilikom obrade podataka o ličnosti pridržavaju odredaba ovog Pravilnika i da sprovedu propisane mere za zaštitu podataka o ličnosti.

Zaposleni i radio angažovani su obavezni da ustupe svoje lične podatke koji su potrebni Rukovaocu za ispunjavanje zakonskih obaveza i redovno poslovanje, kao i da u roku od pet dana obaveste Rukovaoca o bitnim promenama ličnih podataka.

Svaki neovlašćeni pristup, zloupotrebu, uništenje ili oštećenje, kao i svaku drugu radnju kojom se narušava bezbednost podataka o ličnosti, zaposleni i druga radno angažovana lica su dužni da odmah prijave direktoru ili ovlašćenom licu.

Obaveza zaštite podataka o ličnosti ne prestaje prestankom radnog odnosa.

Za zaposlene kod Rukovaoca nepoštovanje odredaba ovog Pravilnika, znači povredu radnih obaveza, odnosno povlači za sobom odgovornost za eventualnu štetu pričinjenu licu na koje se podaci odnose.

### **Obuka i podizanje svesti Član 27.**

Svi zaposleni VINAVER MEDICAL DOO NOVI SAD redovno prolaze obuku o zaštiti podataka, usklađenosti sa Zakonom o zaštiti podataka o ličnosti, Opštom uredbom o zaštiti podataka Evropske unije, Akta (Opšte Uredbe) o veštačkoj

13. The transfer of personal data to other countries or international organizations, including the name of the other country or international organization;
14. A general description of the protection measures established by the Law (organizational, personnel and technical measures);
15. The date the record was updated.

The Data Controller is obliged to update the records when there is a change regarding the basic data from paragraph 1 of this Article.

### **Obligations of Employees Article 26.**

All employees and other engaged personnel, as well as persons authorized by the Controller who collect and process personal data on behalf of or for the needs of the Controller, are obliged to adhere to the provisions of these Regulations when processing personal data and to implement the prescribed measures for the protection of personal data.

Employees and engaged personnel are obliged to provide their personal data necessary for the Controller to fulfill legal obligations and regular operations, as well as to notify the Controller of significant changes to their personal data within five days.

Any unauthorized access, misuse, destruction or damage, as well as any other action that compromises the security of personal data, must be immediately reported by employees and other engaged personnel to the director or authorized person.

The obligation to protect personal data does not cease upon termination of employment.

For employees of the Controller, non-compliance with the provisions of these Regulations constitutes a breach of work duties and entails responsibility for any damage caused to the data subject.

### **Training and Awareness Raising Article 27.**

All employees of VINAVER MEDICAL DOO NOVI SAD regularly undergo training on data protection, compliance with the Personal Data Protection Law, the European Union's General Data Protection Regulation, the Artificial

inteligenciji (AI Act), kao i ostalih relevantnih propisa iz predmetne oblasti, kako bi se osigurala svest i pridržavanje politika zaštite podataka.

### **Lice za zaštitu podataka o ličnosti Član 28.**

Rukovalac odlukom može da imenuje lice za zaštitu podataka o ličnosti, i u tom slučaju će biti dužno da kontakt podatke imenovanog lica dostavi Povereniku.

Za izvršavanje obaveza u vezi sa zaštitom podataka o ličnosti, lice za zaštitu podataka o ličnosti, ukoliko je određeno, je dužno da se pridržava ovog Pravilnika i Zakona.

Sva lica čiji se podaci obrađuju od strane Rukovaoca, mogu da se obrate licu za zaštitu podataka o ličnosti, ukoliko je ono određeno, radi dobijanja svih informacija u vezi sa obradom njihovih podataka, kao i u vezi sa ostvarivanjem prava koja im pripadaju.

Lice za zaštitu je dužno da čuva tajnost svih podataka do kojih dođe u izvršavanju svojih poslova u vezi sa obradom i zaštitom podataka o ličnosti.

### **Usklađenost sa Aktom o veštačkoj inteligenciji Član 29.**

VINAVER MEDICAL DOO NOVI SAD obrađuje podatke o zdravlju u skladu sa odredbama Opštom uredbom o zaštiti podataka Evropske unije za obradu posebnih kategorija ličnih podataka, prvenstveno u svrhe naučnog istraživanja i unapređenja zdravstvene zaštite.

Član 9. Opšte uredbe o zaštiti podataka Evropske unije u principu zabranjuje obradu posebnih kategorija ličnih podataka, uključujući podatke o zdravlju, osim u određenim izuzecima navedenim u članu 9(2). Jedan od tih izuzetaka je kada je " obrada je neophodna u svrhe arhiviranja od javnog interesa, u svrhe naučnog ili istorijskog istraživanja .....". "obrada neophodna iz razloga javnog interesa u oblasti javnog zdravlja, kao što je zaštita od ozbiljnih prekograničnih pretnji po zdravlje ili osiguranje visokih standarda kvaliteta i bezbednosti zdravstvene zaštite i lekova ili medicinskih sredstava".

Međutim, Akt o veštačkoj inteligenciji (AI Act) uvodi dodatno izuzeće koje dozvoljava obradu posebnih kategorija podataka, poput podataka o zdravlju, u svrhu

Intelligence Act (AI Act), as well as other relevant regulations in the subject area, in order to ensure awareness and adherence to data protection policies.

### **Personal Data Protection Officer Article 28.**

The Controller may appoint a personal data protection officer by decision, and in that case, it will be obliged to provide the Commissioner with the contact details of the appointed person.

In performing duties related to the protection of personal data, the personal data protection officer, if appointed, must comply with these Regulations and the Law.

All persons whose data is processed by the Controller may contact the personal data protection officer, if appointed, in order to obtain all information regarding the processing of their data, as well as regarding the exercise of their rights.

The data protection officer is obliged to keep confidential all data obtained in the performance of their duties related to the processing and protection of personal data.

### **Compliance with the Artificial Intelligence Act Article 29.**

VINAVER MEDICAL DOO NOVI SAD processes health data in accordance with the provisions of the European Union's General Data Protection Regulation for the processing of special categories of personal data, primarily for the purposes of scientific research and improving healthcare.

Article 9 of the European Union's General Data Protection Regulation generally prohibits the processing of special categories of personal data, including health data, except in certain exceptions listed in Article 9(2). One of these exceptions is when "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices...".

However, the Artificial Intelligence Act (AI Act) introduces an additional exemption that allows the processing of special categories of data, such as health data, for the purpose of

praćenja pristrasnosti kod visokorizičnih AI sistema koje razvija VINAVER MEDICAL DOO NOVI SAD.

Relevantna odredba AI Akta glasi: "Akt o veštačkoj inteligenciji pruža izuzeće od člana 9. Opšte uredbe o zaštiti podataka Evropske unije za obradu posebnih kategorija podataka (kao što su podaci o zdravlju) u svrhu praćenja pristrasnosti kod visokorizičnih AI sistema."

Ovo znači da, pored svrha naučnog istraživanja i unapređenja zdravstvene zaštite dozvoljenih Opšte uredbe o zaštiti podataka Evropske unije, VINAVER MEDICAL DOO NOVI SAD može obrađivati podatke o zdravlju kada je to strogo neophodno za otkrivanje i ispravljanje pristrasnosti u visokorizičnim AI sistemima koje razvija, pod uslovom da se primene odgovarajuće mere zaštite predviđene Opštom uredbom o zaštiti podataka Evropske unije i AI Aktom.

### **Izmene i dopune Pravilnika Član 30.**

Ovaj Pravilnik o zaštiti podataka o ličnosti i povezane politike i procedure biće pregledani i revidirani na godišnjem nivou kako bi se osigurala kontinuirana usklađenost sa ZZPL, Opštom uredbom o zaštiti podataka Evropske unije za obradu posebnih kategorija ličnih podataka, Aktom o veštačkoj inteligenciji i svim promenama u zakonima o zaštiti podataka ili našim aktivnostima obrade.

Rukovalac zadržava pravo da vrši izmene i dopune Pravilnika u skladu sa važećim propisima iz predmetne oblasti.

### **Završne odredbe Član 31.**

Za sva pitanja koja nisu regulisana ovim Pravilnikom, primenjuje se Zakon, kao i ostali pravno relevantni propisi koji sadrže odredbe o zaštiti podataka o ličnosti.

Pravilnik se objavljuje na oglasnoj tabli Rukovaoca, a stupa na snagu i počinje da se primenjuje osmog dana od dana objavljivanja.

za RUKOVAOCA:



direktor Stevan Vrbaški

monitoring bias in high-risk AI systems developed by VINAVER MEDICAL DOO NOVI SAD.

The relevant provision of the AI Act states: "The Artificial Intelligence Act provides an exemption from Article 9 of the European Union's General Data Protection Regulation for the processing of special categories of data (such as health data) for the purpose of monitoring bias in high-risk AI systems."

This means that, in addition to the purposes of scientific research and improving healthcare allowed by the European Union's General Data Protection Regulation, VINAVER MEDICAL DOO NOVI SAD may process health data when strictly necessary for detecting and correcting bias in the high-risk AI systems it develops, provided that appropriate safeguards prescribed by the General Data Protection Regulation and the AI Act are applied.

### **Amendments to the Regulations Article 30.**

These Personal Data Protection Regulations and related policies and procedures will be reviewed and revised annually to ensure continued compliance with the LPDP, GDPR, the Artificial Intelligence Act, and any changes in data protection laws or our processing activities.

The Controller reserves the right to make amendments and additions to the Regulations in accordance with applicable regulations in the subject area.

### **Final Provisions Article 31.**

For all matters not regulated by these Regulations, the Law and other legally relevant regulations containing provisions on the protection of personal data shall apply.

The Regulations shall be published on the Controller's noticeboard and shall enter into force and become applicable on the eighth day after publication.

For the CONTROLLER



Stevan Vrbaški, CEO

