УДРУЖЕЊЕ ОСИГУРАВАЧА СРБИЈЕ
Бр. 24- 19670-05
Датум: 31 -12- 2021

Удружење осигуравача Србије
Association of Serbian Insurers

БЕОГРАД, Трешњиног цвета 1 г

На основу члана 8. Закона о информационој безбедности („Службени гласник РС", број 6/16), члана 2. Уредбе о ближем садржају Правилника о безбедности информационо-комуникационих система од посебног значаја, начину провере информационо-комуникационих система од посебног значаја и садржају извештаја о провери информационо-комуникационог система од посебног значаја („Сл. Гласник РС", бр. 94/2016) и члана 53. Статута Удружења осигуравача Србије (у даљем тексту: Удружење или Удружење осигуравача Србије) број 13/01-22/2/1 од 04.11.2013. године (Пречишћен текст), Генерални секретар Удружења, дана 31.12.2021. године доноси:

ПОЛИТИКА ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ УДРУЖЕЊА ОСИГУРАВАЧА СРБИЈЕ

Београд, децембар 2021.

I. Подаци о документу

Верзија документа:	0.2
Датум верзије:	30.12.2021
Израдио:	Гојко Грубор
Верификовао:	Александар Ђоковић, Бранко Дамјановић
Одобрио:	Душко Јовановић
Степен поверљивости:	Јавна информација
Чување:	У папирној форми у седишту УОС и свим резервним локацијама У електронској форми на серверима ИЦ УОС

Београд, децембар 2021.

II. Дефиниције термина

- **Анонимизација** (*Anonimization*)**:** Неповратна де-идентификација података о личности тако да лице чији се подаци обрађују не може бити идентификовано у разумном времену, трошковима и доступном технологијом било од стране руковаоца или другог лица. Принципи обраде података о личности не примењују се анонимизацију података о личности пошто они после анонимизације више нису подаци о личности.
- **Група повезаних друштава** (*Group of undertakings*): друштво које остварује контролу и друштва који су под његовом контролом.
- **Руковалац података** (*Controller*): физичко или правно лице, односно орган власти који самостално или заједно са другима одређује сврху и начин обраде. Законом којим се одређује сврха и начин обраде, може се одредити и руковалац или прописати услови за његово одређивање.
- **Подаци о личности** (*Personal data*): сви подаци који се односе на физичко лице чији је идентитет одређен или се може одредити (у даљем тексту: **лице на које се подаци односе**); физичко лице чији се идентитет може одредити је лице која се може идентификовати посредно или непосредно, посебно помоћу персоналних идентификационих информација - идентификатора као што су име, идентификациони број, подаци о локацији, мрежни идентификатор или помоћу једног или више фактора својствених за физички, физиолошки, генетски, ментални, економски, културни или друштвени идентитет тог физичког лица.
- **Повереник за информације од јавног значаја и заштиту података о личности** (*Supervisory authority*): независан и самостални орган власти установљен на основу закона, који је надлежан за надзор над спровођењем Закона о заштити података о личности и обављање других послова прописаних законом;
- **Обрада** (*Processing)*: свака радња или скуп радњи које се врше аутоматизовано или неаутоматизовано са подацима о личности или њиховим скуповима, као што су прикупљање, бележење, разврставање, груписање, односно структурисање, похрањивање, уподобљавање или мењање, откривање, увид, употреба, откривање преносом, односно достављањем, умножавање, ширење или на други начин чињење доступним, упоређивање, ограничавање, брисање или уништавање.
- **Обрађивач података о личности** (*Processor*): физичко или правно лице, односно орган власти који обрађује податке о личности у име руковаоца;
- **Прималац података о личности** (*Recipient*): физичко или правно лице, односно орган власти коме су подаци о личности откривени, без обзира да ли се ради о трећој страни или не, осим ако се ради о органима власти који у складу са законом примају податке о личности у оквиру истраживања одређеног случаја и обрађују ове податке у складу са правилима о заштити података о личности која се односе на сврху обраде;
- **Трећа страна** (*Third Party*): физичко или правно лице, односно орган власти, који није лице на које се подаци односе, руковалац или обрађивач, као ни лице које је овлашћено да обрађује податке о личности под непосредним надзором руковаоца или обрађивача;
- **Посебне категорије података о личности** (*Special categories of personal data*): подаци о личности који откривају расно или етничко порекло, политичко опредељење, верска или филозофска убеђења или припадност синдикату, као и обрада генетских података, биометријских података у сврху јединствене идентификације физичког лица, података о здравственом стању или података о сексуалном животу или сексуалној оријентацији физичког лица;

- **Податак** (*Data*): Појам, симбол, број, реч или било који други део информације који без контекста може имати више значења. Информација је податак у контексту који даје ново сазнање.
- **Пренос података о личности** (*Cross-border processing of personal data*): обрада података ван територије Републике Србије
- **Пристанак** (*Consent*)**:** свако добровољно, одређено, информисано и недвосмислено изражавање воље тог лица, којим то лице, изјавом или јасном потврдном радњом, даје пристанак за обраду података о личности који се на њега односе;
- **Повреда безбедности података о личности (***Data breach***)**: повреда безбедности података о личности која доводи до случајног или незаконитог уништења, губитка, измене, неовлашћеног откривања или приступа подацима о личности који су пренесени, похрањени или на други начин обрађивани.
- **Профилисање** (*Profiling*): сваки облик аутоматизоване обраде који се користи да би се оценило одређено својство личности, посебно у циљу анализе или предвиђања радног учинка физичког лица, његовог економског положаја, здравственог стања, личних склоности, интереса, поузданости, понашања, локације или кретања;
- **Псеудонимизација** (*Pseudonimization*): обрада на начин који онемогућава приписивање података о личности одређеном лицу без коришћења додатних података, под условом да се ови додатни подаци чувају посебно и да су предузете техничке, организационе и кадровске мере које обезбеђују да се податак о личности не може приписати одређеном или одредивом лицу. Псеудонимизација смањује али не елиминише потпуно могућност повезивања података о личности са лицем чији се подаци обрађују, зато што су ови подаци још увек подаци о личности, и обрада ових података треба да је усаглашена са принципима заштите података о личности.
- **Технологија** (*Technology*): Свако средство за прикупљање или обраду података, укључујући, без ограничења, и рачунаре и рачунарске мреже, телекомуникационе системе, видео и аудио уређаје за снимање, биометријске уређаје видео надзор итд.
- **Збирка података о личности** (*Data Filing System*)**:** сваки структурисани скуп података о личности који је доступан у складу са посебним критеријумима, без обзира да ли је збирка централизована, децентрализована или разврстана по функционалним или географским основама.

III. РЕФЕРЕНТНА ДОКУМЕНТА

- Закон о заштити података о личности („Сл. гласник РС“ бр. 87/2018) („ЗЗПЛ“)
- Закон о информационој безбедности ("Сл. гласник РС", бр. 6/2016, 94/2017 и 77/2019)
- Политика заштите информација (ИСМС кровна политика и ИСМС модуларне политике и односне процедуре) УОС
- Стандард ИСМС, СРПС ИСО/ИЕЦ 27001:2014
- Стандарда ПИМС, СРПС ИСО/ИЕЦ 27701.: 2019
- Политика задржавања личних података УОС
- Одлука о именовању Лица за заштиту података (*Дата Протецтион Оффицер*)
- Смернице за инвентарисање података о личности и активности обраде (*Регистар активности обраде*)
- Процедура за добијање пристанак лица чији се подаци о личности обрађују;
- Смернице Радне Групе 29 за процену утицаја обраде на заштиту података о личности („Методологија ДПИА процене“ ;
- Процедура за пренос података;
- Процедура за обавештавање о повреди система заштите података о личности.

IV. СКРАЋЕНИЦЕ

DF (*Data Filing System*): Zbirka podataka o ličnosti;
DPO (*Data Protection Officer*): Lice za zaštitu podataka o ličnosti;
DPIA (*Data Privacy Impact Assesment*): Procena uticaja obrade na zaštitu podataka ličnosti;
CIO *(Chief Information Officer):* Menadžer (direktor) informacionog sistema;
CSIO (*Chief Information Security Officer*): Menadžer informacione bezbednosti;
ENISA (*Europian Network and Information Security Agency*): EU agencija za zaštitu mreža i informacija;
GDPR (*General Data Protection Regulation*): Opšta Uredba o zaštiti podataka o ličnosti;
ИКТ (*Information Communicattion Technologies*): Informaciono komunikacione tehnologije;
ISMS (*Information Security Management System*): Menadžment sistema informacione bezbednosti.
PIMS (*Personal Information Management System*): Menadžment sistema podataka o ličnosti

САДРЖАЈ

1. ЦИЉ ПОЛИТИКЕ

1.1 Главни безбедносни циљ ове политике је да дефинише безбедносне захтеве ИЦ УОС за осигурање усаглашености са стандардом ИСО/ИЕЦ 27701:2019 (ПИМС) и релевантним законима и регулативама Републике Србије које су примењиве на УОС.

1.2 Циљ политике је и да покаже експлицитну намеру главног менаџмента УОС да успостави, имплементира, одржава и побољшава систем заштите података о личности запослених, партнера, добављача и клијената које УОС прикупља, обрађује, преноси или складишти, а који је усаглашен са Законом о заштити података о личности, Законом о информационој безбедности Републике Србије, ИСМС стандардом (ИСО/ИЕЦ 27001:2013) и ПИМС стандардом.

2. НАМЕНА ПОЛИТИКЕ

1.2 Ова политика је намењена запосленима и спољним консултантима УОС, као и партнерима, клијентима и добављачима чији се подаци о личности могу наћи у ИКТ систему УОС.

3. ОБИМ ПОЛИТИКЕ

3.1 УОС се обавезује да усагласи безбедносне захтеве за примењиву заштиту података о личности, у складу са законима и стандардима Републике Србије и релевантним међународним стандардима за заштиту података (ЕНИСА – ГДПР препоруке, смернице Европског борда за заштиту података о личности, ИСО/ИЕЦ 27001, 27017, 27018, 27701). Ова политика се примењује на све запослене у УОС, спољне консултанте, запослене у партнерским организацијама и код добављача који користе податке о личности запослених у УОС, или имају приступ подацима о личности запослених које УОС прикупља или обрађује, као и на појединце који достављају информације и податке о личности УОС, без обзира на географску локацију.

4. БЕЗБЕДНОСНИ ЗАХТЕВИ ПОЛИТИКЕ

4.1 УОС ће, именовати Лице за заштиту података о личности (ДПО), одговорно за израду, праћење промена, имплементацију, контролу и праћење спровођења ове политике у пракси. Лице за заштиту података о личности ће свој рад координирати са Сарадником за информациону безбедности (СИБ, ЦИСО). Дужности Лица за заштиту података о личности су прописане овом Политиком и процедурама које се могу израдити, примењивим законима и регулативама Републике Србије. Те дужности треба да укључе најмање следеће:

4.1.1 информисање и давање мишљења руковаоцу или обрађивачу, као и запосленима који врше радње обраде, о њиховим законским обавезама у вези са заштитом података о личности;

4.1.2 праћење примене одредби ЗЗПЛ, других закона и интерних прописа руковаоца или обрађивача који се односе на заштиту података о личности, укључујући и питања поделе одговорности, подизања свести и обуке запослених који учествују у радњама обраде, као и контроле;

4.1.3 давање мишљења, када се то затражи, о процени утицаја обраде на заштиту података о личности и прати поступање по тој процени, у складу са чланом 54. ЗЗПЛ;

4.1.4. сарадња са Повереником и контакт тачку за сарадњу са Повереником и саветује се са њим у вези са питањима које се односе на обраду, укључујући и обавештавање и прибављање мишљења из члана 55. ЗЗПЛ.

4.2 Принципи за менаџмент прикупљања, коришћења и преноса података о личности

За усаглашавање са ПИМС стандардом, УОС ће усвојити и имплементирати следеће принципе:

4.2.1 Подаци о личности ће се обрађивати само у складу са законом и стандардима најбоље праксе.

4.2.2 Подаци о личности обрађиваће се само у специфичне, експлицитне, законске, уговорне и легитимне сврхе и неће бити даље обрађивани ни на један начин који није у складу са првобитним сврхама обраде.

4.2.3 Подаци о личности биће адекватни, релевантни у односу на сврху за коју су прикупљени и/или обрађивани.

4.2.4 Подаци о личности биће тачни и кад је то могуће, ажурни.

4.2.5 Податке о личности не треба чувати у форми која допушта идентификацију лица чији се подаци обрађују, и не дуже него што је потребно за спровођење сврха обраде.

4.2.6 Подаци о личности се неће прикупљати или обрађивати, осим ако:

a) лице чији се подаци обрађују није дало пристанак за обраду (где је примењиво, видети секцију 3.3);

b) обрада није неопходна за извршавање уговора у коме је уговорна страна лице чији се подаци о личности обрађују, или да би се предузели кораци на захтев лица чији се подаци обрађују, пре закључења уговора;

c) обрада није неопходна за усаглашавање са законским обавезама УОС;

d) обрада није неопходна да би се заштитили витални интереси лица чији се подаци обрађују;

e) обрада није неопходна за извршавање задатака од јавног интереса;

f) обрада није неопходна ради остварења оправданих интереса УОС, партнера или треће стране којој су подаци откривени, осим ако такви интереси нису у сукобу са основним правима и слободама лица чији се подаци о личности обрађују.

4.2.7 Подаци о личности обрађиваће се у складу са правима лица чији се подаци о личности обрађују (видети секцију 4.9).

4.2.8 Одговарајуће физичке, техничке и процедуралне мере (контроле) заштите ће бити предузете да се:

a) спрече и/или идентификује неовлашћено или незаконито прикупљање, обрађивање и пренос података о личности; и

b) спрече случајни губитак или деструкцију, или оштећење података о личности (видети секцију 4.19).

4.3 Принципи заштите података о личности

Ови принципи (начела) истичу основне одговорности за УОС као заједничког руковаоца и одређују сврху и начин обраде података о личности. Руковалац ће бити одговоран за заштиту података о личности и способан да демонстрира усаглашеност са овим принципима (члан 5 став 2)) када је то потребно:

*a) **Законитост, поштење и транспарентност**: Подаци о личности морају се обрађивати законито, поштено и транспарентно ;*

b) ***Ограничење сврхе обраде**: прикупљати и обрађивати податке о личности у сврхе које су конкретно одређене, изричите, оправдане и законите и даље се не могу обрађивати на начин који није у складу са тим сврхама („ограничење у односу на сврху обраде").*

c) ***Минимизација података о личности:** подаци о личности морају бити примерени, релевантни и ограничени на оно што је неопходно за сврхе у које се обрађују. За смањење ризика за податке о личности, УОС може спровести псеудонимизацију података о личности у потпроцесима обраде (на пример, у Базама података).*

d) ***Тачност:** Подаци о личности морају бити тачни и ажурни, где је неопходно, у односу на одређену сврху обраде; треба предузети разумне и благовремене кораке за брисање или исправку података о личности који нису тачни у односу на сврху за коју се обрађују.*

e) ***Ограничено време чувања:** Подаци о личности се морају складиштити не дуже од потребног времена за одређену(е) сврх(е) у коју(е) се подаци о личности обрађују.*

f) ***Интегритет, поверљивост, расположивост и отпорност на инциденте:** УОС ће осигурати одговарајућу заштиту података о личности (усаглашеност са ИСМС, Прилог 1). Узимајући у обзир стање технологија заштите и друге расположиве мере заштите, трошкове имплементације и вероватноћу и интензитет ризика за податке о личности, руковалац ће, пропорционално процењеном ризику, имплементирати одговарајуће процедуралне (административне и организационо-оперативне) и техничке (хардверско-софтверске) мере за заштиту (ИСМС) од случајног или незаконитог уништења, губитка, измене, неовлашћеног приступа или откривања података о личности, укључујући, између осталог следеће процесе: псеудонимизације, шифровања, ИСМС мере заштите поверљивости, интегритета и расположивости система за обраду, благовременог опоравка расположивости и приступа подацима о личности у случају физичког или техничког инцидента (ИСМС), и процену утицаја обраде на права и слободе лица чији се подаци обрађују (ДПИА), да би се мере имплементиране заштите ефективно спроводиле.*

g) ***Одговорност:** Руковалац је одговоран за спровођење принципа заштите података о личности и дужан је да демонстрира усаглашеност са овим принципима.*

4.4 Пристанак лица чији се подаци обрађују

У било којем случају обраде података о личности на основу пристанка лица чији се подаци обрађују, УОС ће спровести следеће мере:

4.4.1 Директор информационог центра (ДИЦ) ће успоставити системе за прикупљање и документовање пристанака лица чији се подаци о личности обрађују.

4.4.2 Да би био законит, пристанак мора бити у форми информације, јасно израђен и дат слободном вољом.

4.4.3 Ако је пристанак добијен кроз друге писане изјаве, захтев за пристанак се може сматрати сумњивим.

4.4.3 Пристанак који се односи на посебне категорије података о личности као и за опозив пристанка мора се прецизно изразити овим подацима:

систем за пријем пристанака укључиваће захтеве за одређивање које информације се морају пружити лицима чији се подаци о личности обрађују да би се добио валидан пристанак и документовали подаци, начин и садржај обавештења, као и валидност, обим и добровољност датог пристанка.

4.5 Пренос података о личности у државе које не обезбеђују адекватне мере заштите (треће државе)

4.5.1 Подаци о личности се неће преносити другом ентитету, држави или територији, све док нису предузети адекватне мере за одржавање захтеваног нивоа заштите података о личности.

4.5.2 Подаци о личности се могу пренети лицима у трећим земљама, само због разлога који су компатибилни са сврхом у коју се обрађују, или другим законским сврхама.

4.5.3 Посебне категорије података које УОС преноси лицима у трећим земљама, или кроз јавне комуникационе мреже, морају бити анонимизовани или криптолошки заштићени од неовлашћеног приступа.

4.5.4 Сви преноси података о личности у треће државе извршиће се на основу писаних уговора о преносу, у складу са ЗЗПЛ. Додатно, подаци о личности могу се преносити у треће земље ако:

1) лице на које се подаци односе је изричито пристало на предложени пренос, пошто је, због непостојања одлуке о примереном нивоу заштите и одговарајућих мера заштите, информисано о могућим ризицима везаним за тај пренос;

2) пренос је неопходан за извршење уговора између лица на које се подаци односе и руковаоца или за примену предуговорних мера предузетих на захтев лица на које се подаци односе;

3) пренос је неопходан за закључење или извршење уговора закљученог у интересу лица на које се подаци односе између руковаоца и другог физичког или правног лица;

4) пренос је неопходан за остваривање важног јавног интереса прописаног законом Републике Србије, под условом да пренос појединих врста података о личности овим законом није ограничен;

5) пренос је неопходан за подношење, остваривање или одбрану правног захтева;

6) пренос је неопходан за заштиту животно важних интереса лица на које се подаци односе или другог физичког лица, ако лице на које се подаци односе физички или правно није у могућности да даје пристанак;

7) врши се пренос појединих података о личности садржаних у јавном регистру, који су доступни јавности или било ком лицу које може да докаже да има оправдани интерес, али само у мери у којој су испуњени законом прописани услови за увид у том посебном случају.

4.6 Спречавање нових или проширених неусаглашених активности

4.6.1 Не могу се предузимати нове активности прикупљања или обраде посебних категорија података о личности, без претходног одобрења ДИЦ и ДПО.

4.6.2 За добијање одобрења, организационе јединице УОС ће доставити ДИЦ-у и ДПО-у потребне информације.

4.6.3 ДПО, у сарадњи са ДИЦ, успоставиће процедуре за процену утицаја нових технологија за заштиту приватности и поверљивости података о личности, вршити процену утицаја нових технологија на процесе сваке примене који укључују податке о личности.

4.6.4 Сви запослени у УОС примењиваће следеће смернице кад у обраду података уносе (пројектују) нове системе, користе или обрађују податке о личности, и/или ревидирају или проширују постојеће активности које укључују обраду података о личности:

a) *обрада података о личности биће прекинута, или ограничена када је разумно и могуће;*
b) *подаци о личности биће анонимизовани када се сврха обраде може да оствари по разумној цени без одржавања идентификације лица чији се подаци обрађују;*
c) *сврхе обраде података о личности биће хитно идентификоване у организационим саставима УОС, који обављају било коју активност или функцију за проширење сврхе обраде података о личности;*
d) *подаци о личности могу се обрађивати само у сврхе у које су прикупљени, плус у историјске, статистичке, научне сврхе, ради спровођења закона и по другим основима из 4.2.6.*

4.7 Информисање лица чији се подаци обрађују

4.7.1 Лицима чији се подаци обрађују или намеравају да се обрађују, УОС ће пре прикупљања/обраде података о личности доставити обавештење. Садржина обавештења је прописана чланом 23, ЗЗПЛ.

4.7.2 Обавештење се неће достављати уколико лице чији се подаци обрађују већ располаже потребним информацијама. Организациони састав УОС који прикупља податке ће, у сарадњи са Лицем за заштиту података о личности, успоставити техничке и административне мере за и како документовати чињеницу да лице чији се подаци обрађују већ има потребне информације.

4.7.3 Ако се ниједан изузетак не може применити, обавештење мора да садржи следеће информације:

1) о идентитету и контакт подацима руковаоца, као и његовог представника, ако је он одређен;
2) контактне податке лица за заштиту података о личности, ако је оно одређено;
3) о сврси намераване обраде и правном основу за обраду;
4) о постојању легитимног интереса руковаоца или треће стране, ако се обрада врши на основу члана 12. став 1. тачка 6) ЗЗПЛ;
5) о примаоцу, односно групи прималаца података о личности, ако они постоје;
6) о чињеници да руковалац намерава да изнесе или износи податке о личности у другу државу или међународну организацију, као и о томе да ли се та држава или међународна организација налази на листи из члана 64. став 7. ЗЗПЛ, а у случају преноса из чл. 65. и 67. или члана 69. става 2. овог ЗЗПЛ, о упућивању на одговарајуће мере заштите, као и о начину на који се лице на које се подаци односе може упознати са тим мерама.

Уз наведене информације, руковалац је дужан да у тренутку прикупљања података о личности лицу на које се подаци односе пружи и следеће додатне информације које могу да буду неопходне да би се обезбедила поштена и транспарентна обрада у односу на то лице:

1) о року чувања података о личности или, ако то није могуће, о критеријумима за његово одређивање;
2) о постојању права да се од руковаоца захтева приступ, исправка или брисање његових података о личности, односно постојању права на ограничење обраде, права на приговор, као и права на преносивост података;
3) о постојању права на опозив пристанка (где је примењиво) у било које време, као и о томе да опозив пристанка не утиче на допуштеност обраде на основу пристанка пре опозива, ако се обрада врши на основу члана 12. став 1. тачка 1) или члана 17. став 2. тачка 1) ЗЗПЛ;
4) о праву да се поднесе притужба Поверенику;
5) о томе да ли је давање података о личности законска или уговорна обавеза или је давање података неопходан услов за закључење уговора, као и о томе да ли лице на које се подаци односе има обавезу да достави податке о својој личности и о могућим последицама ако се подаци не дају;
6) о постојању аутоматизованог доношења одлуке, укључујући профилисање (ако је примењиво) из члана 38. ст. 1. и 4. овог закона, и, најмање у тим случајевима, сврсисходне информације о логици која се при томе користи, као и о значају и очекиваним последицама те обраде по лице на које се подаци односе.

4.7.4 Ако Руковалац намерава даље да обрађује податке о личности у сврху која се разликује од сврхе за коју су подаци о личности прикупљени, Руковалац пре те даље обраде пружа лицу чији се подаци обрађују информације о тој другој сврси и све додатне релевантне информације из члана 4.7.3.

4.7.5 Обавештење треба да буде достављено што је могуће раније, а пожељно је да то буде у првом контакту са лицем чији се подаци обрађују. У случају података о запосленима, ова обавештења треба да се доставе у уговорима са запосленима. Обавештење је потребно да се достави и у огласу за посао.

4.7.6 Обавештење се мора учинити у сажетом, транспарентном, разумљивом и лако доступном облику, уз употребу јасног и једноставног језика. Информације се пружају у писаном облику или на друге начине, укључујући и електронски облик када је примерено. Ако лице чији се подаци обрађују то затражи, информације се могу пружити усмено, под условом да је идентитет лица чији се подаци обрађују одређен на друге начине.

4.8 Извори података о личности

4.8.1 Подаци о личности прикупљаће се само од других партнерских организација и/или ентитета, осим ако сврха обраде захтева прикупљање података од лица чији се подаци обрађују.

4.8.2 Ако се подаци прикупљају од других лица, лице чији се подаци обрађују мора бити информисано о чињеницама из члана 4.7.3, осим ако је лице чији се подаци обрађују примило информације преко других средстава, или би обавештавање захтевало непропорционалан напор, или подаци о личности морају да остану поверљиви у складу с обавезом чувања професионалне тајне коју уређује право ЕУ или национално право, укључујући и законску обавезу чувања тајне.

4.8.3 Организациони састави у УОС, у сарадњи са ДИЦ, СИБ и Лицем за заштиту података о личности (ДПО), израдиће формулар или систем за документовање и што је могуће већу аутоматизацију овог процеса.

4.9 Права лица чији се подаци обрађују

4.9.1 Лице за заштиту података о личности (ДПО) успоставиће систем који омогућава и олакшава остваривање права лица чији се подаци обрађују на информације, приступ, брисање, право на ограничавање обраде, опозив, исправку, преносивост података и, где одговара, или се захтева по примењивом закону, као и систем за обавештавање лица чији се подаци обрађују о продору у безбедност података о личности.

4.9.2 Лицима чији се подаци обрађују биће омогућено да добију следеће информације о њиховим персоналним подацима на основу писаног захтева, усаглашеног са рационалном политиком и успостављеним процедурама ИСМС/ПИМС УОС:

(а) сврси обраде;
(б) категоријама података о личности који су у питању;
(ц) корисницима или категоријама корисника којима су подаци о личности откривени или ће им бити откривени, а посебно корисницима у трећим земљама или међународним организацијама;
(д) уколико је могуће, предвиђеном року у којем ће се подаци о личности чувати или, ако то није могуће, критеријумима који су коришћени за одређивање тог рока;
(е) постојању права да се од руковаоца затражи приступ подацима о личности и исправка или брисање података о личности (ако нема законских ограничења) или ограничавање обраде у вези са лицем чији се подаци о личности обрађују и права на приговор на обраду;
(ф) праву на подношење притужбе надзорном органу (Поверенику);
(г) ако се подаци о личности не прикупљају од лица чији се подаци обрађују, свакој доступној информацији о њиховом извору;
х) постојању аутоматизованог доношења одлука, укључујући и профилисање из члана 38. ЗЗПЛ и, барем у тим случајевима, садржајне информације о логици која се користи, као и значај и предвиђене последице такве обраде за лице чији се подаци обрађују;
и) ако се подаци о личности преносе у трећу земљу или међународну организацију, лице чији се подаци обрађују има право да буде информисано о одговарајућим мерама заштите.

4.9.3 УОС ће обезбедити одговор на захтев из секције 4.9.2 у року од месец дана од пријема писаног захтева лица чији се подаци обрађују и одговарајуће верификације да је подносилац захтева лице чији подаци обрађују или његов пуномоћник.

4.9.4 Захтеви за приступ или исправљање података о личности морају се поднети Лицу за заштиту података о личности (ДПО) у УОС.

4.9.5 Лице за заштиту података о личности (ДПО) ће успоставити систем за евиенцију сваког захтева из ове секције са подацима како су примљени и који је датум одговора.

4.9.8 Ако руковалац не поступи по захтеву лица чији се подаци обрађују, Руковалац обавештава лице чији се подаци обрађују одмах или најкасније месец дана од пријема захтева, о разлозима због којих није поступио по захтеву и о могућности подношења притужбе надзорном органу (Поверенику) и тражења правног лека.

4.9.9 Уколико би обезбеђивање информација по захтевима могло да открије податке о личности другог лица, УОС је дужна да заштити права тог лица.

4.9.10 УОС може захтева разумну надокнаду да покрије трошкове одговора на захтеве лица које није запослено у УОС, ако су захтеви чести прекомерни.

4.9.11 Лице за заштиту *података о личности* (ДПО) може да успостави процедуре за спречавање и одбијање увредљивих, злонамерних и учесталих захтева.

4.10 Аутоматизовано доношење појединачних одлука и профилисање

4.10.1 Осим у случајевима прописаним ЗЗПЛ, лице чији се подаци обрађују има право да се на њега не примењује одлука заснована искључиво на аутоматској обради, укључујући и профилисање, која производи правна дејства који се на њу/њега односе или на сличан начин значајно утичу на њу/њега.

4.11 Посебне категорије података о личности

4.11.1 Забрањена је обрада података о личности који откривају расно или етничко порекло, политичко опредељење, верска или филозофска убеђења или припадност синдикату, као и обрада генетских података, биометријских података у сврху јединствене идентификације физичког лица (отисак прста, препознавање лица...), података о здравственом стању или података о сексуалном животу или сексуалној оријентацији физичког лица, осим у случајевима прописаним примењивим законом.

4.11.2 УОС може да обрађује посебне категорије података о личности на основу неког од изузетака за обраду посебних категорија података.

4.12 Директни маркетинг и профилисање

4.12.1 Када се подаци о личности обрађују у сврху директног маркетинга и профилисања, Руковалац треба да буде у могућности да прибави пристанак лица чији се подаци обрађују за обраду података о личности у ове сврхе.

4.13 Осигурање квалитета података

4.13.1 УОС ће предузети кораке да осигура да прво прикупљање или обрађивање података о личности буде комплетирано и тачно. Подаци морају бити тачни и ажурирани на такав начин да дају праву слику текуће ситуације података о личности лица чији се подаци обрађују.

4.13.2 УОС ће исправити податке за које сазна да су нетачни и неажурни, чак и када лице чији се подаци обрађују не захтева исправку. Нетачни подаци се морају избрисати и заменити са коригованим додатним подацима.

4.13.3 Подаци о личности се морају чувати само у периоду који је неопходан за испуњење сврхе обраде. Када дефинише дозвољену обраду података, организациони састав УОС ће успоставити датум завршетка или ревизије наведене сврхе обраде.

4.13.4 Подаци о личности треба да буду избрисани ако је повређено било које правило заштите података, у складу са примењивим законом, или ако УОС-у односни подаци о личности нису више потребни.

4.14 Обавештавање о корекцијама података

4.14.1 Ако су подаци измењени, Руковалац мора обавестити сваког коме преноси измењене податке.

4.15 Пропорционалност обраде

4.15.1 Ова политика ће се применити на рационалан начин са трошковима и напорима пропорционалним значају предложене обраде и осетљивости односних података.

4.16 Коришћење треће стране за обраду података

4.16.1 У случају да УОС ангажује спољне обрађиваче, УОС ће пре преноса података, утврдити да ли обрађивач у довољној мери гарантује примену одговарајућих техничких, организационих и кадровских мера тако да обрада буде у складу са захтевима из примењивог закона и да обезбеђује заштиту права лица на која се подаци односе.

4.16.2 УОС ће закључити уговор у писаној форми са обрађивачем, у складу са Стандардним уговорним клаузулама Повереника.

4.16.3 У складу са интерним процесима провере (ревизије) у УОС, УОС ће редовно вршити проверу обраде код обрађивача, посебно у односу на мере заштите.

4.17 Обавештавање менаџмента о потенцијалним санкцијама за неусаглашеност

4.17.1 Лице за заштиту података о личности (ДПО) ће обавестити менаџмент и друге одговорне запослене, да:

а) неусаглашеност са примењивим прописима за заштиту података може имати кривичне и друге последице, укључујући дисциплинске, новчане и затворске казне; и

б) они могу бити лично одговорни за грешку коју учине уз пристанак УОС.

4.19 Безбедност података о личности

4.19.1 УОС ће применити процедуралне (административно-управљачке и организационо-оперативне), техничке и физичке мере (контроле) заштите, како би обезбедила заштиту података, укључујући спречавање њихове измене, губитка, оштећења и неовлашћене обраде или приступа, имајући у виду природу података, савремене технологије заштите и ризике којима су подаци изложени услед људске акције, процеса и процедура обраде, или физичког и природног окружења.

4.19.2 Адекватне безбедносне мере (контроле) треба да укључе све следеће компоненте:

*а) **Контрола физичког приступа:** Спречавање неовлашћеним лицима да добију приступ системима за обраду података у којима се обрађују подаци о личности.*

*b) **Контрола логичког приступа**: Осигурати да се у логовима система за обраду података о личности редовно проверава ко је унео, модификовао или уклонио податке о личности из система за обраду.*

*c) **Контрола овлашћења**: Спречавање неовлашћених лица да користе системе за обраду.*

d) ***Контрола ауторизације приступа**: Спречавање лица овлашћених да користе системе за обраду података да приступе подацима изван својих овлашћења и потреба, укључујући неовлашћено читање, копирање, модификацију или брисање за време и након обраде података.*

e) ***Контрола откривања поверљивости података**: Осигурати да подаци о личности у току електронске трансмисије за време преноса или складиштења на носаче података, не могу бити прочитани, копирани, модификовани или уклоњени без овлашћења, и који обезбеђују механизам за проверу ко је овлашћен да прими, а ко је примио информацију.*

f) ***Контрола процеса обраде**: Осигурати да у процесима (активностима) обраде података о личности, подаци буду обрађивани само у складу са инструкцијама Руковаоца.*

g) ***Контрола расположивости**: Осигурава да су подаци о личности заштићени од нежељеног уништења или губитка и да су на располагању кад год су потребни.*

h) ***Контрола коришћења и сепарације сврхе обраде**: Осигурати да се подаци о личности прикупљени за различите намене, могу и хоће обрађивати одвојено за различите сврхе обраде.*

i) ***Контрола времена чувања**: Осигурати да се подаци о личности не чувају дуже него што је потребно, укључујући захтев да се подаци пренесени трећој страни морају вратити или уништити.*

j) ***Споразум о поверљивости са запосленима**: Сва лица укључена у било коју фазу обраде података морају експлицитно потписати уговор/изјаву о поверљивости података, који може трајати и након престанка радног односа.*

4.20 Решавање спорова

4.20.1 Запослени који имају приговоре на обраду података о личности, прво треба да обаве разговор са непосредним руководиоцем. Ако лице чији се подаци обрађују не жели да поднесе притужбу непосредном руководиоцу, или ако лице чије се подаци обрађују и његов непосредни руководилац не постигну задовољавајуће решење, запослени треба да упути писани захтев Лицу за заштиту података о личности (ДПО).

4.20.2 Ако спор не може да се реши мирним путем кроз консултације са Лицем за заштиту података о личности (ДПО), спор треба решавати на следећи начин:

a) кроз вансудско решавање спорова, где је примењиво.
b) Подношењем притужбе Поверенику.

4.20.3 Ако спор није решен у консултацијама између лица чији се подаци обрађују и Лица за заштиту података о личности (ДПО), или кроз друге механизме прописаним уговорима о раду или интерним документима УОС, спор ће бити решен пред надлежним судом у Београду.

4.21 Специфична правила

4.21.1 Лице за заштиту података о личности (ДПО) може израдити смернице за примену ове Политике у одређеним државама, ако је примењиво.

4.21.2 Ако је УОС издала политику примењиву у одређеним државама ЕУ, та политика има предност над овом Политиком.

5. ЗАХТЕВИ ЗА ОДГОВОРНОСТ

5.1 Генерални секретар (ГС) УОС одговоран је за валидацију, одобравање, усвајање и потписивање предложене и образложене Политике. Одговоран је да обезбеди све неопходне ресурсе за успостављање адекватних мера заштите (ЗЗПЛ, ИСМС и ПИМС) за процесе заштите прикупљања, обраде, складиштења и преноса података о личности. Директор је одговоран за стриктну примену ове политике у пракси, менаџерску контролу, и примену репресивних мера за неспровођење ове политике.

5.2 Директор ИЦ УОС (ДИЦ) одговоран је за пријем захтева лица чији се подаци обрађују и обезбеђивање приступа подацима за остваривање права, у складу са овом политиком.

5.3 Лице за заштиту података о личности (ДПО), у сарадњи са ЦИСО и ЦИО, као и менаџером за људске ресурсе и главним правником УОС (ако није ДПО), одговорно је за израду, успостављање, имплементацију, праћење спровођења, провере и ревизију политике. Лице за заштиту података о личности (ДПО) је одговорно да прима и региструје све извештаје запослених о стању заштите података о личности и да обавештава Надзорни орган (Повереника) о повреди безбедности система заштите података о личности. Одговорности Лица за заштиту података о личности (ДПО) су:

1. *Надгледање система заштите приватности и побољшање технологија заштите;*
2. *Сарадња са ДИЦ и ЦИСО у УОС око усаглашавања процеса, метода и технологија заштите информационе имовине (ИСМС) и заштите података о личности;*
3. *Праћење промена и усаглашавање са новим променама у законима за заштиту приватности у свим земљама са којима УОС послује;*
4. *Израда и менаџмент политике и процедура заштите приватности;*
5. *Надгледање и контрола менаџмента односа са купцима/клијентима/партнерима/ спољним сарадницима и контрола свих односних питања заштите приватности;*
6. *Осигуравање и надгледање активности за израду инвентара података о личности у УОС, као дела Регистра информационе имовине са безбедносном класификацијом;*
7. *Праћење тока података о личности изван граница Републике Србије;*
8. *Осигурање и спровођење обуке запослених и других односних учесника о заштити приватности;*
9. *Осигурање, у сарадњи са ДИЦ и ЦИСО, метода и алата за имплементацију Политике за заштиту података о личности.*

5.4 Сарадник за информациону безбедност (ЦИСО) одговоран је за успостављање, имплементацију, контролу и проверу ИСМС/ПИМС система заштите и блиску сарадњу са Лицем за заштиту података о личности (ДПО) у вези са специфичностима захтева ЗЗПЛ.

5.5 Сви запослени у УОС дужни су да се упознају са свим захтевима ове политике и да спроводе све процедуре и активности које се односе на обраду података о личности у оквиру описа посла и радног места у УОС.

6. ОБАВЕЗА ПРИМЕНЕ, РЕПРЕСИВНЕ МЕРЕ И УСАГЛАШЕНОСТ

6.1 Сви корисници за које је ова политика намењена обавезни су да усагласе праксу обраде и заштите података о личности са захтевима политике и референтним законима, регулативама, стандардима, упутствима и процедурама заштите који је подржавају. Уколико дође до неусаглашености са овом политиком заштите и односним стандардима, упутствима и процедурама заштите, Лице за заштиту података о личности (ДПО), ЦИСО и ДИЦ морају о томе да обавесте Повереника.

6.2 За неспровођење, намерно игнорисање, немар или грешке у спровођењу ове политике и односних процедура примењиваће се репресивне мере, зависно од природе и озбиљности повреде ове политике и нанете штете УОС-у, и то дисциплинске мере према Дисциплинском правилнику УОС (ако је примењиво), које могу укључивати опомене, финансијске мере и отказ уговора о раду и отказ уговора са лицима ван УОС, као и прекршајне и кривичне санкције према ГДПР/ЗЗПЛ и примењивом закону и другим подзаконским актима и прописима Републике Србије.

6.3 Ова политика се ослања на одредбе ЗЗПЛ, ИСМС стандарда ИСО/ИЕЦ 27001:2013 Анекс А и ПИМС стандарда ИСО/ИЕЦ 27701:2019 Анекс А, и подложна је ревизији у складу са развојем стандарда, развојем и одржавањем пословног и ИКТ система УОС.

7. СМЕРНИЦЕ ЗА ИМПЛЕМЕНТАЦИЈУ ПОЛИТИКЕ

7.1 Ограничени ефекат политике

7.1.1 Ова политика не може дати лицу чији се подаци о личности обрађују већа права него што би то лице имало према примењивом закону (ЗЗПЛ).

7.2 Процена текуће усаглашености

7.2.1 Лице за заштиту података о личности (ДПО) израдиће план за имплементацију и имплементирати ревизију усаглашености са овом Политиком за све организационе саставе УОС. Лице за заштиту података о личности (ДПО), у сарадњи са ЦИСО, ДИЦ и ИМ организационих састава УОС, развиће акционе и динамичке планове за корекцију свих неусаглашености у разумном року.

7.3 Обука запослених

7.3.1 ИМ организационих састава УОС обезбедиће обуку запослених о процедурама за заштиту приватности података о личности и тајности (поверљивости) пословних података. Ове процедуре треба успоставити и треба да укључују најмање следеће:

a) дужност сваког запосленог је да користи и допушта обраду података о личности само овлашћеним лицима и у овлашћене сврхе;
b) принципе заштите података прописаних у секцији 4.3;
c) садржај (захтеви) политике;
d) односне ИСМС политике УОС и ова политика;
e) потребу за формулисањем и правилном применом усвојених процедура за имплементацију политике;
f) коректну употреба лозинки, безбедносних токена, смарт картица и других приступних механизама;

g) *ограничени приступ подацима о личности, као што је употреба лозинком заштићеног screen saver-а, излоговање када се информације не користе и када није присутно овлашћено лице;*
h) *безбедно складиштење фајлова, штампаних материјала и електронских медија за складиштење;*
i) *општа забрана преноса података изван интерног радног еста и физичких просторија УОС;*
j) *прописно одлагање поверљивих папирних података сецкањем, а е-podataka брисањем вишекратним преписивањем случајним карактерима (wipingг) итд.*

7.4 Годишња ревизија (провера) система заштите личних података

7.4.1 Сваки организациони састав УОС извршиће годишњу ревизију система за обраду података и праксе заштите. Ова ревизија ће укључити најмање следеће:

a) *организациони састави одредиће које податке о личности исти прикупљају, или намеравају да прикупљају, сврху прикупљања и обраде података, сваку додатну допуштену сврху, стварну употребу података, да ли је обавештење из члана 4.7.3 достављено лицима чији се подаци о обрађују, постојање и обим пристанка лица чији се подаци обрађују, законске обавезе које се односе на прикупљање и обраду таквих података и обим, ефикасност и стање имплементације мера заштите.*
b) *организациони састави одредиће које податке о личности је потребно да држе у мануелним и полуаутоматизованим збиркама података о личности.*
c) *организациони састави треба да идентификују све преносе података о личности у њиховом поседу или контроли; односно где су подаци о личности пренети, сврху преноса, који су физички, технички и процедурални системи имплементирани да одржавају барем постојећи ниво заштите података и да спрече или контролишу накнадне преносе.*
d) *информације о резултатима годишње ревизије треба доставити Лицу за заштиту података о личности (ДПО) и другим релевантним организационим саставима ради одобравања одговарајућих акција, укључујући, без ограничења, следеће информације:*
   1. *Давање препорука за побољшање политика и процедура да би се побољшала усаглашеност са овом политиком и примењивим законом.*
   2. *Усаглашеност са прописима за трансфер персоналних података из ЕУ у треће земље.*

7.5 Објављивање

7.5.1 Ова политика биће на располагању запосленима УОС на интерном порталу/дељеном серверу, кроз правну службу УОС, а клијентима, партнерима и добављачима на интернет страници УОС, линком са Обавештења о заштити приватности клијената, или постављањем на неки алтернативни интернет сајт за приступ регистрованих корисника или путем других начина објављивања које одреди Лице за заштиту података о личности (ДПО).

7.6 Ступање на снагу

7.6.1 Ова политика ступа на снагу датумом одобравања и потписивања. Лице за заштиту података о личности (ДПО), у сарадњи са организационим саставима УОС, развиће динамички план за имплементацију ове политике и решавање сукоба ове политике са другим постојећим политикама УОС.

7.7 Ревизија политике

7.7.1 Ова политика може бити ревидирана у свако време. Забелешка о значајној ревизији треба да се обезбеди запосленима преко интерног портала или других механизама одобрених од стране Лица за заштиту података о личности (ДПО).

7.8 Спонзор политике

7.8.1 Спонзори ове политике су Лице за заштиту података (ДПО) и/или ДИЦ и/или ЦИСО. Било које питање које се односи на ову политику треба упутити Лицу за заштиту података о личности (ДПО).

7.9 Власник (стараоц) политике

7.9.1 Стараоц ове политике је Лице за заштиту података о личности (ДПО). ИМ организационих састава УОС одговорни су за имплементацију политике. Свако питање везано за имплементацију политике треба упутити Лице за заштиту података о личности (ДПО).

7.10 Степен поверљивости политике

7.10.1 Уколико је могуће, свака секција ове Политике биће интерпретирана у складу са релевантним законима Републике Србије, а сваку секцију за коју се утврди да није у складу са релевантним законима, треба ставити ван снаге, без утицаја на остале секције Политике.

7.11 Друге односне политике УОС

7.11.1 Политика менаџмента информационе безбедности (ИСМС политика)
7.11.2 Политика контроле приступа
7.11.3 Политика мобилног приступа и рада на даљину
7.11.4 Политика безбедносне класификације информација
7.11.5 Политика менаџмента инцидента
7.11.6 Политика менаџмента ризика и анализе утицаја на права и слободе лица (ДПИА)

7.12 Менаџмент записа који се одржавају на основу ове политике

Име записа	Локација складиштења	Лице одговорно за складиштење	Контроле за заштиту записа	Време чувања
Евиденције приступа и опозива	(спецификовати фолдер у Интераном пратлу УОС)	ДПО	Само овлашћено лице може приступити формулару	Трајно
Евиденција инцидената	(спецификовати фолдер у Интераном пратлу УОС)	ДПО	Само овлашћено лице може приступити формулару	Трајно
Евиденција односа са Повереником	(спецификовати фолдер у Интераном пратлу УОС)	ДПО	Само овлашћено лице може приступити формулару	Трајно
Уговори о преносу података о личности	(спецификовати фолдер у Интераном пратлу УОС)	ДПО	Само овлашћено лице може приступити формулару	5 година од престанка важења уговора
Регистар активности обраде	(спецификовати фолдер у Интераном пратлу УОС)	ДПО	Само овлашћено лице може приступити формулару	Трајно

7.13 Валидација и менаџмент документа

7.13.1 Валидацију ове политике врше власник (старатељ) ове политике, Лице за заштиту података о личности (ДПО), и директор који мора контролисати и проверавати примену политике а Лице за заштиту података о личности (ДПО), по потреби и ажурирати документ најмање једанпут годишње.

7.13.2 Ова политика ступа на снагу на дан потписивања.

7.14 Ауторизација

7.14.1 На документ ове политике примењује се ауторизација наведена у каталогу докумената за класу „Политике“ УОС.

Рб	Корисник или група корисника	Права
1	ГС	☒Читање ☒Мењање ☒Усвајање ☒Забрана ☒Валидација
2	Лице за заштиту података о личности (ДПО)	☒Читање ☒Мењање ☒Усвајање ☐Забрана ☒Валидација
4	Сви запослени у УОС	☒Читање ☐Мењање ☐Усвајање ☐Забрана ☐ Валидација
5	Обрађивачи	☒Читање ☒Мењање ☒Усвајање ☐Забрана ☒Валидација

Београд: 31.12. 2021.

Генерални секретар

УДРУЖЕЊЕ ОСИГУРАВАЧА СРБИЈЕ • БЕОГРАД •

Душко Јовановић

Бр	Документ	ГДПР чл./ИСМС	Обавезан по ГДПР	Обавезан по ИСМС
13	Прилог-План задржавања података	ГДПР чл.30	+	
14	Опис посла ДПО	ГДПР чл. 37,38,39	+**	
	5. Мапирање активности обраде			
15	Смернице за инвентар података и активности обраде	ГДПР чл.30		
16	Прилог-Инвентар активности одбране	ГДПР чл.30	+	
	6. Мапирање права власника ПОДАЦИ О ЛИЧНОСТИ			
17	Формулар пристанка власника података о личности	ГДПР чл. 6(1)(а),7(1),9(2)	+	
18	Формулар повлачења пристанка власника	ГДПР 7(3)		
19	Формулар родитељског пристанка	ГДПР чл.8	+	
20	Формулар родитељског повлачења пристанка	ГДПР чл.8	+	
21	Процедура решавања захтева за приступ подацима о личности	ГДПР чл.7(3),15,16,17,18,20,21,22		
22	Формулар захтева за приступ подацима о личности	ГДПР чл.15		
23	Формулар обавештења	ГДПР чл.15		
	7. Процена и третман ризика			
24	Методологија менаџмента ризика	ИСМ 6.1.2, 6.1.3, 8.2 и 8.3		+
25	Прилог 1-Табела процене ризика	ИСМС 6.1.2 и 8.2		+
26	Прилог 2- Табела третмана ризика	ИСМС 6.1.3 и 8.3		+
27	Прилог 3-Извештај о процени и третману ризика	ИСМС 8.2 и 8.3		+
	8. Процена утицаја заштите података			
28	Методологија процене утицаја заштите података (ДПИА)	ГДПР чл.35		
29	ДПИА регистар	ГДПР чл.35	+	
	9. Применљивост контрола заштите			
30	СоА	ИСМС 6.1.3(д)		+
	10. План имплементације			
31	План третмана ризика	ИСМС 6.1.3, 6.2 и 8.3		+
	11. Контроле заштите			
32	Политика БУОД	ИСМС А.6.2.1, А.6.2..2, А.13.2.1, ГДПР Чл.32		
33	Политика мобилних уређаја и рада на даљину	ИСМС А.6.2, А.11.2.6, ГДПР чл.32		
34	Изјава о поверљивости запосленог/снабдевача	ИСМС А.7.1.2, А.13.2.4, А.15.1.2		+*
35	Изјава запосленог о прихватљивости ИСМС докумената	ИСМС А.7.1.2		+*
36	Инвентар имовине	ИСМС А.8.1.1, А.8.1.2		+*
37	ИТ политика заштите (збирна)	ИСМС А.6.2.1, А.6.2.2, А.8.1.2, А.8.1.3, А.8.1.4, А.9.3.1, А.11.2.5, А.11.2.6,		+*

Бр	Документ	ГДПР чл./ИСМС	Обавезан по ГДПР	Обавезан по ИСМС
		A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2,A.A.13.2.3, A.18.1.2, ГДПА чл. 32		
38	Политика класификације информација	ИСМС A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3, ГДПР чл.32		
39	Политика контроле приступа	ИСМС A.9.1.1, A.9.1.2, A.9.2.1,A.9.2.2, A.9.2.3,A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3, ГДПР чл.32		+*
40	Политика пасворда (може бити део Политике контроле приступа)	ИСМС A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3, ГДПР чл. 32		
41	Политика употребе криптозаштите	ИСМС A.10.1.1, A.10.1.2, A.18.1.3, A.18.1.5, ГДПР чл.32		
42	Политика анонимизације и псеудонимизације	ИСМС A.10.1.1, A.18.1.3, A.18.1.5, ГДПР чл.32		
43	Политика чист сто, чист екран (може бити део ИТ политике заштите)	ИСМС A.11.2.8, A.11.2.9, ГДПР чл.32		
44	Политика одлагања и уништења (може бити имплементирана ка Процедура заштите за ИТ департман)	ИСМС A.8.3.2, A.11.2.7 ГДПР чл.32		
45	Процедуре за рад у заштићеним просторима	ИСМС A.11.1.5, ГДПР чл.32		
46	Безбедносна процедура за ИТ сектор	ИСМС A.8.3.2, A.11.2.7, A.12.1.1, A12.1.1, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.14.2.4, ГДПР чл.32		+*
47	Политика менаџмента промена (може се имплементирати као део Процедуре безбедности ИТ сектора)	ИСМС A.12.1.2, A.14.2.4, ГДПР чл.32		
48	Политика бекаповања (може се имплементирати као део Процедуре безбедности ИТ сектора)	ИСМС A.12.3.1		
49	Процедура прекограничног преноса података о личности	ИСМС A.13.2.1, A.13.2.2, ГДПР чл. 1(3), 44,45,46,47,49		
50	Прилог 1-Уговорне обавезе у вези са преносом података о личности	ИСМС 13.2.2, ГДПР чл.46(5)	+	+*
51	Прилог 2- Стандард уговорних обавеза за пренос података о личности	ИСМС A.13.2.2, ГДПР чл.46(5)	+	+*
52	Политика безбедности развоја	ИСМС A.14.1.2, A.14.1.3, A.14.2.1, A.14.2.2, A.14.2.5,		

Бр	Документ	ГДПР чл./ИСМС	Обавезан по ГДПР	Обавезан по ИСМС
		A.14.2.8, A.14.2.9, A.14.3.1, ГДПР чл.32		
53	Прилог-Спецификација захтева за ИС	ИСМС A.14.1.1, ГДПР чл.32		+*
54	Политика заштите клијената	ИСМС A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.152.1, A.15.2.2, ГДПА чл.28,32		
55	Упитник за ГДПР усаглашеност обрађивача	ИСМС A.7.1.1, ГДПР чл.28		
56	Уговори о заштити података о личности са руковаоцима, обрађивачима и корисницима	ИСМС A.7.1.2, A.15.1.2, A.15.1.3, ГДПР чл.28,32,82	+	+*
57	Безбедносне клаузуле за добављаче и партнере	ИСМС A.7.1.2, A.14.2.7, A.15.1.2, A.15.1.3		+*
58	Процедура за одговор и обавештење о пробоју података о личности	ИСМС A.7.2.3, A.16.1.1, A.6.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7, ГДПР чл.4(12), 33, 34	+	+*
59	Регистар пробоја података о личности	ИСМС A.16.1.6, ГДПР чл.33(5)	+	
60	Формулар обавештења супервизора о пробоју података	ИСМС A.7.4, A.16.1.5, ГДПР чл. 33	+	
61	Формулар обавештења о продору у безбедност података	ИСМС 7,4, A.16.1.5, ГДПР чл.34	+	
62	План опоравка од ВД	ИСМС A.17.1.2, ГДПР чл.32		+*
	12. Обука и свест			
63	План обуке и подизања свести	ИСМС клаузуле 7.2, 7.3, ГДПР чл.39(1)		+
	13. Интерна котрола (провера, *аудит*)			
64	Процедура интерне контроле	ИСМС клаузула 9.2, ГДПР чл.32		
65	Прилог 1- Програм годишње интерне контроле	ИСМС клаузуле 9.2, ГДПР чл.32		+
66	Прилог 2- Извештај о интерној контроли	ИСМС клаузула 9.2, ГДПР чл. 32		+
67	Прилог 3-Чеклиста за интерну контролу	ИСМС клаузула 9.2, ГДПР чл.32		
	14. Менаџерска контрола			
68	Извештај о мерењима	ИСМС клаузуле 6.2, 9.1		+
69	План менаџерске контроле	ИСМС клаузула 9.3		+
	15. Корективне акције			
70	Процедура за корективне акције	ИСМС клаузула чл. 10.1		
71	Прилог-Форма корективне акције	ИСМС клаузула 10.1		+

+* Ова документа су обавезна:

(а) само ако су односне контроле идентификоване и одобрене у СоА документу.

+ Ова документа су обавезна ако:**

(а) обраду врши орган јавне власти осим судова који раде у правосудном систему, или

(б) се кључне активности друштва састоје од операција обраде које по својој природи, опсегу и/или намени, захтевају регуларан и систематичан надзор великог обима података о личности, или

(ц) су кључне активности друштва је обрада великог обима посебних категорија података о личности.