

ЈКП „Стандард“ Ада

Деловодни број: 26/ЈКР-1

Дана: 12. августа 2019. године

ПОЛИТИКА ЗАШТИТЕ ПОДАТКА О ЛИЧНОСТИ У ЈАВНОМ КОМУНАЛНОМ ПРЕДУЗЕЋУ „СТАНДАРД“ АДА

1. Намена, обим корисници

ЈКП „Стандард“ Ада (у даљем тексту: Предузеће) намерава да се усагласи са применљивим законима и регулативама Републике Србије који се односе на заштиту података о личности. Ова политика истиче основне принципе обраде личних података корисника услуга, добављача, пословних партнера, запослених и других појединаца или представника закона (у даљем тексту: Клијенти) и указује на одговорност Предузећа и запослених у активностима обраде података.

2. Дефиниције термина

Подаци о личности: Свака информација која се односи на идентификацију или личне идентификационе информације физичких лица (лица на које се подаци односе) која могу бити директно или индиректно идентификована, посебно на основу неког идентификатора као што је име, лични број, податак о локацији, или један или више фактора специфичних за физицки, психолошки, генетски, ментални, економски, културолошки или другтвени идентитет физицког лица.

Осетљиви подаци о личности: Подаци о личности који по својој природи, посебно осетљивости за права и слободе лица на која се подаци односе, заслужују специфичне мере заштите пошто контекст (активности) обраде података може изазвати висок ризик за фундаментална права и слободе физичких лица. Ови подаци укључују расну или етичку припадност, религијско или филозофска уверење, генетичке податке, биометријске податке за јединствену идентификацију физичких лица.

Руковалац података: Физичко или правно лице, представник јавне власти, агенција или друго тело које само или заједно одређује намену и средства обраде личних података.

Обрадивач података: Физичко или правно лице, представник јавне власти, агенција или друго тело које обрадује личне податке у име контролора.

Обрада: Свака операција или скуп операција које се извршавају над личним подацима или скупу личних података, мануелним или аутоматизованим средствима, као што су: скупљање, снимање, организација, структурирање, похрањивање,

адаптација или измена, извлачење, консултовање, употреба, откривање преносом, дистрибуција или стављање на располагање на други начин, усклађивање или комбиновање, рестрикција, брисање или уништавање података.

Анонимизација (синоним: шифровање): Неповратан процес накнадне идентификације личних података тако да физичко лице не може бити идентификовано у разумном времену, са разумним трошковима и технологијом било од стране руковођа или других лица за идентификацију тог лица. Принципи обраде личних података не примењују се на анонимизоване податке који нису висе подаци о личности лични.

Псеудонимизација (синоним: кодирање): Обрада личних података на такав начин да на даље не може бити повезан са специфичним физичким лицем без употребе додатних информација. Такве додатне информације морају да се држе одвојено и да су застичене техничким и организационим мерама које осигуравају да се подаци о личности не могу придружити физичком лицу. Псеудонимизација смањује, али не елиминисе потпуно способност повезивања личних података са физичким лицем на кога се подаци односе. Ови подаци су још увек лични подаци и на њих се односе начела обраде личних података.

3. Основна начела обраде података о личности

Начела (принципи) заштите података описују основне одговорности организације која рукује подацима о личности. Према члану 4(8) Закона руковођац (контролор) „је 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 руковођац или прописати услови за његово одређивање”.

3.1. Законитост, поштење и транспарентност

Подаци о личности морају се скупљати и обрађивати законито, поштено и транспарентно у односу на лице на које се подаци односе (ГДПР принцип „законитости, поштења и транспарентности”). Законита обрада је обрада која се врши у складу са овим Законом, члан 5(1), односно другим законом којим се уређује обрада.

3.2. Ограничење намене

Подаци о личности морају се прикупљати 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.

3.3. Минимизација података

Лични подаци скупљани, обрађивани и похрањивани у Предузећу морају бити адекватни, релевантни и ограничени на минималну количину која је неопходна за намене за које су скупљани, обрађивани и похрањивани. Предузеће мора применити анонимизацију или псеудонимизацију података о личности ако постоји висок ризик за права и слободе физичких лица и могућност да се смањи ризик за физичка лица.

3.4. Тачност

Подаци о личности скупљени у Предузећу морају бити тачни и, где је неопходно, ажурно одржавани. Предузеће ће предузети рационалне кораке да се нетачни лични подаци, имајући у виду намену за коју су скупљани и обрађивани, благовремено избришу или исправе (Закон, члан 5(4)).

3.5. Ограничен период чувања

Лични подаци ће се чувати у Предузећу у облику који омогућава идентификацију лица само у року који је неопходан за остваривање сврхе обраде („ограничење чувања”, Закон, члан 5(5)).

3.6. Интегритет, поверљивост и расположивост

Узимајући у обзир последњу технологију и друге расположиве мере заштите података и информација, трошкове имплементације и вероватноћу и интензитет ризика за личне податке, Предузеће мора применити одговарајуће техничке и организационе мере за обраду личних података на начин који осигурава одговарајућу безбедност личних података, укључујући расположивост када су потребни и заштиту од случајног или незаконитог уништења, губитка, измене, неовилашћеног приступа или откривања (Закон, члан 5(6)).

3.7. Контролисана одговорност

Директор Предузећа као руковалац (контролор) података је одговоран и способан да демонстрира усаглашеност са горе описаним начелима Закона заштите података о личности.

4. Изградња система заштите података у пословним активностима Предузећа

Да би демонстрирало усаглашеност са начелима заштите података о личности Закона, Предузеће ће уградити систем заштите података у пословне процесе и активности.

4.1. Обавештавање физичког лица

Предузеће мора објавити Обавештење о приватности на веб сајту Предузећа и направити линк према овој Политици и истаћи обавештење у својим службеним просторијама. Обавештење о приватности треба да садржи све неопходне информације које се односе на скупљање података, активности обраде, мере заштите података, локацију обраде, одговорности итд.

4.2. Избор и пристанак физичког лица

У пословању Предузећа физичка и правна лица (лица на која се подаци односе) дају експлицитно свој пристанак за скупљање и обраду њихових личних података на законом одређен начин.

4.3. Скупљање података

Предузеће мора да настоји да скупља што је мању могућу количину личних података. Ако личне податке у име Предузећа скупља трећа страна Лице за заштиту података о

личноси у Предузећу, мора осигурати да се лични подаци скупљају на законској основи.

4.4. Употреба, задржавање и одлагање података

Намене и методи обраде, ограничено похрањивање и задржавање личних података мора бити конзистентно са информацијама садржаним у Обавештењу о приватности. Предузеће ће одржавати тачност, интегритет, поверљивост, расположивост и релевантност података о личности кроз све активности намењене обраде.

Адекватни механизми техничке и организационе заштите пројектовани су у Предузећу да штите личне податке од крађе, погрешне употребе или злоупотребе и спрече пробој личних података. Директор Предузећа је одговоран за усаглашеност наведену у овој секцији:

- Копирање или дуплирање података никада се не сме вршити без знања Директора Предузећа, са изузетком стварања резервних копија, осим док је неопходно за осигурање намењене обраде, као и за регулаторно задржавање података.
- После закључивања рада по уговору, или раније по захтеву Предузећа, а најкасније по завршетку уговорних обавеза, Предузеће ће на захтев претходног пристанка клијента, избрисати, или шифровати (анонимизовати) податке и архивирати заједно са уговорима за чување у законском периоду.
- Документација која је коришћена да демонстрира регуларну обраду података у складу са уговором, Предузеће ће похранити и чувати дуже од периода трајања уговора у складу са одговарајућим законским периодом задржавања.

4.5. Откривање података трећим странама

Кад год Предузеће користи поверљиву трећу страну (добављача или пословног партнера) да обрађује податке о личности у њено име, Лице за заштиту података о личности, мора осигурати да ће обрађивач обезбедити адекватне техничке и организационе мере заштите података о личности које су пропорционалне процењеном ризику. За ову сврху могу се користити Политика заштите приватности треће стране (добављача или пословног партнера) и усаглашен упитник о захтевима заштите за трећу страну.

Предузеће мора уговором захтевати од треће стране (добављача или пословног партнера) да обезбеди исти ниво заштите приватности и безбедносних мера за заштиту личних података. Добављач или пословни партнер морају обрађивати личне податке само да испуне своје уговорне обавезе према Предузећу или на основу инструкције која може садржавати законске, легитимне и друге интересе Предузећа и никако за друге сврхе. Ако добављач обрађује личне податке заједно са независном трећом страном од поверења, Предузеће мора експлицитно спецификовати њихове одговорности, а трећа страна добављача мора потписати релевантан уговор или други правно обавезујући документ, као што је Споразум о обради података са добављачем.

4.6. Прекогранични пренос података о личности

Пре преноса личних података изван европске економске зоне (ЕЕА) као и из Републике Србије (члан 63, Закона) морају се користити адекватне мере самозаштите обезбеђене у стандардном члану Уговора, укључујући потписивање

Уговор о преносу података, како ЕУ ГДПРи Закон захтевају, и у ситуацијама где то други прописи захтевају, са добијеним овлашћењем локалног надлежног тела за заштиту података (Повереник за заштиту података о личности у Србији). Ентитет који прима личне податке мора се усагласити са скупом принципа обраде личних података описаних у процедури Прекограничног преноса података коју прописује Повереник.

4.7. Права приступа физичког лица подацима

Када ради као руковалац (контролор) података, Директор Предузећа је одговоран да обезбеди лицу на које се подаци односе погодан механизам за приступ који му омогућава да приступи својим личним подацима и дозволи му да ажурира, исправи, избрише или пренесе своје податке о личности, ако одговара или се захтева по закону.

4.8. Преносивост података о личности

На писани захтев лица на које се подаци односе, Предузеће ће бесплатно доставити копију података које је добила од лица, у структурираном формату, или је пренети другом руковаоцу. Лице за заштиту података о личности или лице именовано за послове заштите података о личности ће такав захтев обрадити у року од месец дана од дана подношења писаног захтева, ако захтев није прекомеран (свакодневан) и ако не утиче на права и податке о личности других лица.

4.9. Право на заборав (брисање података)

Физичко лице на које се подаци односе може захтевати брисање својих личних података (члан 30, Закона). Када Предузеће ради као руковалац, Лице за заштиту података о личности предузеће неопходне акције (укључујући и техничке мере) да о захтеву информише све треће стране које користе или обрађују податке и у разумном року (8 до 16 дана) избрише захтеване податке.

4.10. Одговорност и надокнада штете

У случају приговора или нанете штете за права и слободе физичких лица, Предузеће и клијент (добавијач, партнер) ће бити одговорни лицу на које се подаци односе, у складу са Законом (чланови 82 до 86, Закона).

5. Смернице за поштену обраду података о личности

Подаци о личности се у Предузећу морају обрађивати само када су експлицитно овлашћени од Лица за заштиту података о личности у Предузећу и одобрени од Директора Предузећа као руковалаца података.

Предузеће мора да процени и одлучи да ли да изврши Процену утицаја обраде на заштиту података за сваку активност обраде у складу са смерницама (члан 54, Закона).

5.1. Обавештење о приватности за физичка лица

У време скупљања или пре скупљања података о личности за сваку врсту активности обраде, Лице за заштиту података о личности је одговорно да прописно обавести

лица на које се подаци односе о следећем: врсти скупљених података о личности, наменама обраде, методама обраде, правима лица на које се подаци односе, периоду задржавања, потенцијалном међународном преносу података, дељењу података са трећим странама и мерама Предузећа за заштиту података о личности. Ове информације се обезбеђују кроз документ Обавештење о приватности.

Ако се подаци о личности деле са трећом страном, Лице за заштиту података о личности Предузећа мора осигурати да је лице на које се подаци односе обавештено о томе кроз Обавештење о приватности.

Када се лични подаци преносе у трећу земљу према Политици прекограничног преноса и Закону, у Обавештењу о приватност треба јасно навести државу у коју се подаци преносе и ентитет којем се подаци преносе.

5.2. Добијање пристанка

Кад год је обрада личних података заснована на пристанку физицког лица, или на другом законском основу, Лице за заштиту података о личности у Предузећу је одговорно за евидентирање и одржавање записа о том пристанку, информисање физицких лица, обезбеђивање опције за достављање пристанка, и осигурање да њихов пристанак (кад год се пристанак за обраду даје на законској основи) може бити у свако време повучен, на основу писаног захтева.

Када се захтева корекција, допуна или уништавање записа података о личности, Лице за заштиту података о личности, или лице именовано за послове заштите података о личности осигураће да се ови захтеви изврше у разумном времену, региструју и чувају логови записа о захтевима.

Подаци о личности се у Предузећу обрађују само за намене за које су оригинално скупљени. У случају да Предузеће жели обрађивати податке за другу намену, Предузеће же тражити експлицитан пристанак од лица на које се подаци односе у јасном и концизном писаном формату. Сваки такав захтев ће укључивати оригиналну намену(е) за коју су се подаци скупљали, нову или додатну намену(е) обраде, као и разлог за промену намене(а) обраде. Лице за заштиту података о личности у Предузећу одговорно је за усаглашеност са правилима у овој секцији.

Метод скупљања података о личности у Предузећу усаглашен је и биће усаглашаван убудуће са Законом о заштити података о личности, добром праксом и стандардима заштите података и информација.

Лице за заштиту података о личности је одговорно за креирање и одржавање Регистра обавештења о приватности.

6. Организација и одговорности

Одговорност за осигурање одговарајуће обраде података о личности је сваког ко ради за или са Предузећем и има приступ подацима о личности које Предузеће обрађује.

Кључне одговорности за обраду података о личности у Предузећу имају следеће организационе улоге:

Директор Предузећа: Одобрава општу стратегију Предузећа и доноси одлуке о скупљању, обради и заштити података о личности клијената у Предузећу, ради као руковалац активности обраде, одређује намену обраде, организује и води евиденцију о активностима обраде података о личности у Предузећу (Члан 47(5) Закона).

Лице за заштиту података о личности: Одговорно је за менаџмент програма за заштиту података о личности, за развој и промоцију политике заштите приватности крајњим корисницима и за друге активности дефинисане у опису послова Лица за заштиту података о личности (чланови 56, 57 и 58 Закона);

Правник Предузећа: Мониторише и анализира законе о заштити података о личности, прати промене законских регулатива, развија захтеве за усаглашеност и помаже секторима Предузећа у достизању циљева Политике заштите приватности.

ИТ сектор Предузећа: Одговоран је да осигура да сви системи, сервиси и опрема која се користи за обраду и похрањивање података о личности достигну прихватљиве стандарде информационе безбедности и заштите података о личности. Извршава регуларне провере и скенирања да осигура да техничке мере заштите хардвера и софтвера, И организационе мере функционишу прописно.

7. Одговор на инцидент повреде података о личности

Када Предузеће, тј. Лице за заштиту података о личности уочи или посумња, или идентификује инцидент стварне повреде личних података, мора да предузме интерну проверу, спречи ширење инцидента и захтева благовремене мере опоравка система заштите, у складу са овом Политиком. Где постоји ризик, посебно висок ризик за права и слободе лица на која се подаци односе, Предузеће (тј. Лице за заштиту података о личности) ће обавестити надлезно надзорно тело (Повереника) и Национални ЦЕРТ без одлагања, а најкасније у року од 72 сата, а у најкраћем могућем року власнике података (до 15 дана).

8. Провера и одговорност

Предузеће ће настојати да проверава квалитет имплементације ове Политике, да унапређује техничке и организационе мере заштите и контроле података о личности клијената.

Сви запослени у Предузећу, који обрађује податке о личности морају бити упознати и обучени о подацима о личности, о системима контроле и начину прикупљања и обраде, законским прописима и одговорностима који произилазе из Закона. Ако запослени у Предузећу повреди права и слободе лица на које се подаци односе, према овој Политици, биће подвргнути дисциплинским, прекршајним или кривичним мерама, зависно од нанете штете пословном систему Предузећа.

9. Конфликт закона

- Ако су лични подаци клијената у Предузећу предмет претраге и привременог одузимања (нпр. у случају инцидента и дигиталне форензицке истраге),

конфисковања у току банкротства или процедуре несолвентности, или сличних догађаја или мера треће стране док је под контролом Предузећа, Предузеће ће обавестири клијента о таквим акцијама без икаквог одлагања.

- Предузеће ће обавестити без кашњења све заинтересоване стране о тим акцијама и то, да је било који погођен податак само у власништву и зони одговорности Предузећа, да је податак на располагању једино Предузећу, и да је Предузеће одговорно тело у смислу захтева Закона о заштити података о личности.
- Трајање саопштења ове Политике одговарају трајању пословних уговора и осталих уговора које Предузеће закључује за потребе обавијања редовних делатности.
- У случају било којег сукоба прописа, Закон о заштити података о личности ће имати предност над захтевима ове Политике. Где индивидуални захтеви секција ове политике нису валидни или применљиви, то неће утицати на валидност и применљивост других захтева ове Политике.
- Политика се усаглашава са законом Републике Србије. Само надлезни судови у Републици Србији ће имати јурисдикцију у односу на било који неспоразум, контраверзност или потраживању у вези права и слобода физичких лица на која се подаци односе, или сваког следећег анекса уговора са клијентима, укључујући, без ограничавања, његова формирања, валидацију, обавезујући ефекат, интерпретацију, извршавање, повреду или укидање, као и не уговорне захтеве.

9.1. Обавезе добављача према Предузећу

Адекватне техничке и организационе мере (Прилог 1), које Предузеће примењује за заштиту података о личности, подложне су техничком прогресу и даљем развоју. У том смислу, Предузећу је дозвољено да имплементира алтернативне адекватне мере заштите података о личности, при чему ниво безбедности дефинисаних мера заштите не сме бити смањен, а битне промене морају бити документоване.

Предузеће ће у уговору тражити од пословних партнера, да примењују адекватне техничке и организационе мере заштите података о личности које у уговорима, или анексима уговора, добију од Предузећа:

- Пословни партнери ће подржати Предузеће/Руковаоца у испуњавању права и приговора физичких лица према Закону о заштити података о личности и у складу са овом Политиком.
- Пословни партнери ће даље подржати Предузеће/Руковаоца у усаглашавању са обавезама које се односе на заштиту података о личности, захтеве за извештавање о повредама података о личности, процену утицаја обраде података на заштиту података о личности и на претходне консултације са надлежним надзорним телима.
- Пословни партнери гарантују да ће свим запосленим укљученим у уговор о обради података о личности Предузећа, као и другим таквим лицима која могу бити укључена у Уговор о обради података са Предузећем, у оквиру обима одговорности клијента, бити забрањено да обрађују податке изван обима обраде датог инструкцијама Предузећа. Даље, клијент гарантује да ће свако лице које обрађује податке у име руковаоца предузети мере за чување тајности или спроводити статутарну обавезу за чување тајности. Све обавезе за чување тајности треба да остану на снази и по прекиду или истеку Уговора о обради података Предузећа.

- Пословни партнери ће благовремено обавестити контактну особу у Предузећу о сваком питању које се односи на заштиту података.
- Ако физичка лица поднесу било који захтев против Предузећа у складу са чланом 82 Закона о заштити података о личности, пословни партнери ће подржати Предузеће у одбрани против таквих захтева, где је могуће и оправдано.

10. Менаџмент одржавања записа политике

Име записа	Локција складиштења	Лице одговорно за складиштење	Контроле за заштиту записа	Време чувања
Формулар пристанака власника података	Интерни сервер за похрањивање фајлова	Лице за заштиту података о личности	Само овлашћено лице може приступити формулару	10 година
Формулар за повлачење пристанка лица чији се подаци обрађују	Интерни сервер за похрањивање фајлова	Лице за заштиту података о личности	Само овлашћено лице може приступити формулару	10 година
Уговор о преносу података о личностима	Интерни сервер за похрањивање фајлова	Лице за заштиту података о личности	Само овлашћено лице може приступити формулару	5 година од престанка важности споразума
Регистар обавештења о приватности	Интерни сервер за похрањивање фајлова	Лице за заштиту података о личности	Само овлашћено лице може приступити формулару	Трајно

11. Валидација и менаџмент документа

Валидацију ове политике врше директор Предузећа и Лице за заштиту података о личности који морају контролисати и проверавати примену политике о заштити приватности, а Лице за заштиту података о личности по потреби и ажурирати документ по потреби.

Ова политика ступа на снагу даном доношења.

Милан Попов
директор ЈКП „Стандард“ Ада



Прилог 1: ТЕХНИЧКЕ И ОРГАНИЗАЦИОНЕ МЕРЕ ЗАШТИТЕ АКТИВНОСТИ ОБРАДЕ ПОДАТАКА О ЛИЧНОСТИ

Заштита поверљивости активности обраде података о личности	
Физички приступ просторијама за обраду података	Кључеви, видео надзор
Електронски приступ системима за обраду и похрањивање података	Безбедносна лозинка, шифровање носача податка
Процес обраде податка о личности	Псеуднимизација: Обрада података о личности на такав начин да се подаци не могу повезати са специфичним лицем без помоћи додатних информација, под условом да су ове информације складишне одвојено и предмет су одговоарајућих техничких и организационих мера заштите.
Заштита интегритета активности обраде података о личности	
Пренос података о личности	Адекватне техничке мере заштите укључују шифровање, ВПН взе, дигитални потпис.
Тачност уноса податка о личности	Контрола логовања и документ менаџмент система.
Заштита расположивости и отпорности личних података	
Контрола расположивости и спречавање случајне или немерне деструкције или губитка података о личности	Стратегија бекаповања, UPS систем, антивирусна заштита, firewall
Брз опоровак после инцидента	Из система за бекаповање
Организационе мере заштите	
Процедуре за регуларно тестирање, процену и евалуацију	
Менаџмент заштите приватности	Политика заштите приватности, регистар активности обраде
Менаџмент одговора на инцидент	Политика управљања инцидентом,

Подразумевана и уграђена заштита података о личности	Имплементирана псудонимизација и минимизација видљивости података о личности за имплементацију начела заштите податка о личности, интеграција неопходне мере заштите у порцесу обраде. Ова контрола се односи на количину скупљања податка, обим обраде период складиштења и приступ одацима о личности. Осигурати да подразумевано подаци о личности нису доступни физичким лицима без интервнције човека за неки неодређен број лица који траже приступ својим подацима, п је мануелна помоћадминистратора неопходна
---	---