

1. Препорука CM/Rec(2015)5 Комитета министара државама чланицама о обради личних података у контексту запошљавања

(Усвојио Комитет министара 1. априла 2015, на 1224. седници заменика министара)

Незваничан превод

Комитет министара, у складу са чланом 15.6 Статута Савета Европе,

Сматрајући да је циљ Савета Европе постизање већег јединства међу својим члановима;

Свестан све већег коришћења нових технологија и средстава електронске комуникације у односима између послодаваца и запослених, и одговарајућих предности истих;

Верујући, ипак, да послодавци приликом коришћења метода за обраду података треба да се руководе принципима дизајнираним да минимализују све ризике које би те методе могле представљати за права и основне слободе запослених, нарочито њихово право на приватност;

Имајући у виду одредбе Конвенције о заштити лица у односу на аутоматску обраду личних података од 28. јануара 1981. (ЕТС 108, у даљем тексту: Конвенција бр. 108) и њеног Додатног протокола у вези с надзорним органима и прекограничним протоком података од 8. новембра 2001. (ЕТС 181), и да је пожељно применити принципе на секторе запошљавања;

Препознајући чињеницу да су интереси приликом развијања принципа за сектор запошљавања индивидуални или колективни, приватни или јавни;

С обзиром на то да лични подаци у званичним документима који су у поседу јавне власти или јавних органа могу бити објављени од стране власти или органа у складу с домаћим законом у чијој је надлежности власт или орган, тиме измирујући приступ тим званичним документима с правом на заштиту личних података у складу с принципима ове препоруке;

Свестан различитих традиција које постоје у државама чланицама у погледу регулисања различитих аспеката односа послодавца и запосленог и имајући у виду да је закон само једно од средстава за регулисање таквих односа;

Свестан промена које су се догодиле у активностима сектора запошљавања и сродних односа на међународном нивоу, посебно због повећаног коришћења информационо-комуникационих технологија (ИКТ-ови) и глобализације запошљавања и услуга;

Имајући у виду да, у светлу тих промена, треба прегледати Препоруку Rec(89)2 Комитета министара државама чланицама о заштити личних података коришћених у сврхе запошљавања како би се наставио адекватан ниво заштите појединаца у контексту запошљавања;

Подсећајући да члан 8. Европске конвенције о људским правима (ЕТС бр. 5), штити право на приватни живот, укључујући активности професионалне и пословне природе, по тумачењу Европског суда за људска права;

Подсећајући на примену постојећих принципа из других релевантних препорука Комитета министара Савета Европе државама чланицама, нарочито из Препоруке CM/Rec(2010)13 о заштити појединаца у погледу аутоматске обраде личних података у контексту профилисања, Препоруке Rec(97)5 о заштити медицинских података и Препоруке Rec(92)3 о генетичком тестирању и скринингу за потребе здравствене неге;

Подсећајући на Водеће принципе за заштиту појединаца у погледу сакупљања и обраде података путем видео-надзора, које је усвојио Европски комитет за правну сарадњу (ЦДЦЈ) Савета Европе у мају 2003, из Резолуције 1604 (2008) о видео-надзору јавних површина Парламентарне скупштине Савета Европе, који су нарочито релевантни;

Подсећајући на Европску социјалну повељу (ЕТС бр. 163), ревидирану 3. маја 1996, и на Правилник Међународне организације рада из 1997, о пракси за заштиту личних података радника,

Препоручује да владе држава чланица:

- осигурају да се принципи садржани у додатку овој препоруци, која замењује поменућу препоруку Rec(89)2, огледају у примени домаћег законодавства о заштити података у сектору запошљавања, као и у другим гранама закона које имају утицаја на употребу личних података у сврхе запошљавања;

- у ту сврху, осигурају да се на ову препоруку и њен додатак скрене пажња органа успостављених у оквиру домаћег законодавства за заштиту података, а који су надлежни да надгледају спровођење тог законодавства;

- промовишу прихватање и спровођење принципа садржаних у додатку ове препоруке путем комплементарних инструмената, као што је кодекс понашања, како би осигурало да су принципи добро познати, схваћени и примењени од стране свих учесника у секторима запошљавања, укључујући представничке органе и послодаваца и запослених, те да су узети у обзир у дизајну и употреби ИКТ-ова у сектору запошљавања.

Додатак Препоруци CM/Rec(2015)5

I део – Општи принципи

1. Обим

1.1. Принципи из ове препоруке примењују се на сваку обраду личних података у сврху запошљавања, у јавним и у приватним секторима.

1.2. Уколико домаћи закон не предвиђа другачије, принципи ове препоруке такође се односе и на активности агенција за запошљавање, било у јавном или приватном сектору, које обрађују личне податке како би омогућиле да се један конкурентни уговор или више конкурентних уговора о запошљавању, укључујући уговоре са скраћеним радним временом, успостави између заинтересованих појединаца и потенцијалних послодаваца, или да се помогне послодавцима у обављању њихових дужности у вези с овим уговорима.

2. *Дефиниције*

За сврхе ове препоруке:

Лични податак значи било коју информацију која се односи на физичко лице на основу које је утврђен или се може утврдити идентитет тог лица („лице на које се подаци односе“);

Обрада података подразумева било коју радњу или скуп радњи које се врше над личним подацима, посебно прикупљање, складиштење, чување, измена, преузимање, откривање, стављање на располагање, брисање, или уништавање података, или спровођење логичких и/или аритметичких операција над подацима; где се не користи аутоматска обрада, обрада података подразумева операције које се спроводе без структурисаног скупа успостављеног у складу с било којим критеријумом који дозвољава претрагу личних података;

Информациони систем подразумева сваки уређај или групу међусобно повезаних или везаних уређаја, од којих један или више, у складу с програмом, врши аутоматску обраду компјутерских података, као и компјутерских података ускладиштених, обрађених, преузетих или пренесених од стране тих уређаја, за сврху њиховог рада, употребе, заштите и одржавања;

Сврхе запошљавања тичу се односа између послодаваца и запослених, а који се односе на запошљавање, испуњење уговора о раду, управљање, укључујући извршавање обавеза утврђених законом или колективним уговорима, као и на планирање и ефикасно вођење неке организације и престанак радног односа. Последице уговорног односа могу се продужити и после рока уговора о раду;

Послодавац означава свако физичко или правно лице, јавни орган или агенцију која је засновала радни однос са запосленим или разматра такав однос у погледу пријаве за посао и има законску одговорност за предузимање или успостављање;

Запослени означава свако заинтересовано физичко лице ангажовано у радни однос од стране послодавца.

3. *Поштовање људских права, достојанства и основних слобода*

Поштовање људског достојанства, приватности и заштите личних података треба да буде осигурано у обради личних података у сврху запошљавања, посебно како би се омогућио

слободан развој личности запосленог, као и могућности појединачног и друштвеног односа на радном месту.

4. *Примена принципа обраде података*

4.1. Послодавци треба да минимализују обраду личних података само на податке неопходне за жељени циљ у појединачним разматраним случајевима.

4.2. Послодавци треба да развију одговарајуће мере, како би се осигурало да у пракси поштују принципе и обавезе у вези с обрадом података у сврху запошљавања. На захтев надзорног органа, послодавци треба да покажу своју усклађеност с тим принципима и обавезама. Ове мере треба прилагодити обиму и природи обрађених података, типу активности које се предузимају и, такође, треба узети у обзир могуће импликације по основна права и слободе запосленог.

5. *Сакупљање и складиштење података*

5.1. Послодавци треба да сакупљају личне податке директно од конкретног лица на које се подаци односе. Када је потребно и законито да се обрађују подаци сакупљени од трећих страна, на пример, да се добију професионалне препоруке, лице на које се подаци односе треба да буде унапред прописно обавештено.

5.2. Лични подаци сакупљени од стране послодавца у сврху запошљавања треба да буду релевантни и не смеју бити прекомерни, имајући у виду врсту запошљавања, као и измењене информационе потребе послодавца.

5.3. Послодавци не треба да од запосленог или апликанта за посао захтевају или траже приступ информацијама које он или она деле са осталима на интернету, посебно путем друштвених мрежа.

5.4. Здравствени подаци се могу сакупљати само у сврхе наведене у принципу 8.2. ове препоруке.

5.5. Складиштење личних података у сврху запошљавања дозвољено је само ако су подаци сакупљени у складу са захтевима наведеним у начелима 4, 9. и од 14. до 20. ове препоруке и само за време неопходно за испуњавање легитимног циља обраде. Ови подаци треба да буду релевантни, одговарајући и не смеју бити прекомерни. Када се евалуација података у вези с учинком или могућностима запосленог ускладишти, ти подаци треба да се користе само у сврхе процене професионалних вештина.

6. *Интерна употреба података*

6.1. Личне податке прикупљене за сврхе запошљавања треба да обрађују само послодавци за те сврхе.

6.2. Послодавци треба да усвоје политику заштите података, правила и/или друге инструменте интерне употребе личних података у складу с принципима ове препоруке.

6.3. Под изузетним околностима, када се подаци обрађују у сврхе запошљавања које су другачије од сврха за које су првобитно сакупљени, послодавац треба да предузме адекватне мере како би избегао злоупотребу података за те различите сврхе и да информише запосленог. У случају када треба донети важне одлуке засноване на обради података, а које утичу на запосленог, истог треба обавестити о томе.

6.4. Не доводећи у питање принцип 8, у случају корпоративних промена, спајања и преузимања, нарочиту пажњу треба посветити принципима пропорционалности и спецификацији сврхе у наредном коришћењу података. Сваку битну промену у обради треба проследити заинтересованим лицима.

7. *Прослеђивање података и употреба ИКТ-ова у сврхе заступања запосленог*

7.1. У складу с домаћим законом и праксом или условима колективних уговора, лични подаци могу се проследити заступницима запосленог, али само у обиму у којем су ти подаци неопходни да им се омогући прописно заступање интереса запосленог или ако су ти подаци неопходни за испуњавање и надзор обавеза утврђених колективним уговором.

7.2. У складу с домаћим законом и праксом, употреба информационих система и технологија за прослеђивање података заступницима запослених треба да буде у надлежности посебних споразума који унапред постављају јасна правила која прописују њихову употребу и сигурносне мере за заштиту поверљиве комуникације, у складу с принципом 10.

8. *Екстерно прослеђивање података*

8.1. Лични подаци сакупљени у сврху запошљавања треба да се проследе само јавним органима који обављају званичне функције, и у сврхе спровођења истих, и само у границама законских обавеза послодаваца или у складу с другим одредбама домаћег закона.

8.2. Прослеђивање личних података јавним органима у сврхе другачије од оних које су потребне за обављање њихових званичних функција, или странама које нису јавни органи, укључујући ентитете у истој групи, треба да се изврши само:

а. где је то потребно у сврхе запошљавања, а сврхе нису неспојиве са сврхама за које су подаци првобитно сакупљени и ако је одређени запослени или његови/њени заступници, као што може бити случај, информисани о овоме унапред;

б. уз изричит, слободан и информисани пристанак конкретног запосленог;

в. ако је прослеђивање предвиђено домаћим законом, нарочито када је то неопходно у сврхе остваривања законских обавеза или у складу с колективним уговорима.

8.3. Одредбе које регулишу откривање личних података како би се осигурала транспарентност у јавном сектору (влада и други орган јавне власти или тело), укључујући надзор правилне употребе јавних ресурса и средстава, треба да осигурају одговарајуће мере заштите за права запосленог на приватност и заштиту личних података.

8.4. Послодавци треба да предузму одговарајуће мере како би осигурали да се само релевантни, тачни и ажурирани подаци екстерно прослеђују, нарочито у односу на податке који су постављени онлајн и доступни широј јавности.

9. *Обрада осетљивих података*

9.1. Обрада осетљивих података из члана 6. Конвенције 108 дозвољена је само у одређеним случајевима, где је неопходно за запошљавање на посебан посао или за испуњавање законских обавеза везаних за уговор о раду у границама утврђеним домаћим законом и у складу с одговарајућим мерама заштите, као допуна онима из Конвенције 108 и из ове препоруке. Одговарајуће мере заштите треба да имају за циљ спречавање ризика које обрада таквих података може представљати за интересе, права и основне слободе запосленог, посебно ризик од дискриминације. Обрада биометријских података треба да буде могућа под условима из принципа 18. ове препоруке.

9.2. У складу с домаћим законом, запосленом или апликанту за посао могу се поставити само питања у вези с његовим/њеним здравственим стањем и/или се може извршити медицински преглед како би се:

- а.* указало на његове/њене подобности за садашње или будуће запослење;
- б.* испунили захтеви превентивне медицине;
- в.* гарантовала одговарајућа рехабилитација или усклађеност са условима неког другог радног окружења;
- г.* заштитили витални интереси носиоца података или других запослених и појединаца;
- д.* омогућила додела социјалних бенефиција;
- ђ.* одговорило у судским поступцима.

9.3. Генетски подаци не могу се обрађивати, на пример, како би се одредила професионална подобност запосленог или апликанта, чак ни уз пристанак лица на које се подаци односе. Обрада генетских података може се дозволити само у изузетним околностима, на пример, како би се избегло наношење озбиљне штете по здравље лица на које се подаци односе или трећих страна, и само ако је то прописано домаћим законом и ако подлеже одговарајућим сигурносним мерама.

9.4. Здравствене податке и, где је њихова обрада законита, генетске податке треба сакупљати само од запосленог, када је то прописано законом и када подлеже одговарајућим сигурносним мерама.

9.5. Здравствени подаци обухваћени обавезом медицинске поверљивости треба да буду доступни и обрађивани само од стране особља које је везано таквом обавезом или другим правилима професионалне тајности или поверљивости. Такви подаци морају:

- а. се односити директно на способност одређеног запосленог да оствари његове дужности;
- б. бити неопходни за подршку мера за заштиту здравља запосленог;
- в. бити неопходни за спречавање ризика по друге.

Када се овакви подаци прослеђују послодавцима, обраду треба да изврши лице с одговарајућим овлашћењем, као што је неко у кадровској администрацији или неко одговоран за здравље и сигурност на послу, и информације треба прослеђивати само ако је то неопходно за доношење одлука кадровске администрације и у складу с одредбама домаћег закона.

9.6. Здравствене податке обухваћене обавезом медицинске поверљивости и, где је њихова обрада законита, генетске податке треба складиштити одвојено од других категорија личних података у поседу послодаваца. Техничке и организационе мере сигурности треба предузети како би се спречило да лица која не припадају медицинској служби послодавца имају приступ тим подацима.

9.7. Здравствене податке који се односе на треће стране не треба обрађивати ни под којим околностима осим, ако лице на које се подаци односе да потпуни, недвосмислени, слободан и информисани пристанак, или ако је такву обраду одобрио надзорни орган за заштиту података, или је обавезна у складу с домаћим законом.

10. *Транспарентност обраде*

10.1. Информације у вези с личним подацима у поседу послодавца треба да буду доступне запосленом кога се тичу директно или путем посредника његових/њених заступника, или да их се о њима обавести на одговарајући начин.

10.2. Послодавци запосленима треба да осигурају следеће информације:

- категорије личних података које се обрађују и опис сврхе обраде;
- примаоци, или категорије прималаца личних података;
- средства којима запослени остварују права из принципа 11. ове препоруке, без прејудуцирања повољнијих предвиђених домаћим законом или у њиховом правном систему;
- све друге информације неопходне да осигурају правичну и закониту обраду.

10.3. Неопходно је осигурати посебно јасан и комплетан опис категорија личних података које могу сакупљати ИКТ-ови, укључујући видео-надзор и њихово могуће коришћење. Овај принцип се, такође, примењује на посебне облике обраде из II дела додатка ове препоруке.

10.4. Информације треба достављати у приступачном облику и редовно. У сваком случају, те информације треба доставити пре него што запослени почне обављати одређене активности или радње и учинити их доступним путем информационих система које запослени иначе користи.

11. *Право на приступ, исправку и приговор*

11.1. Запослени треба да, на захтев, у разумном временском року и без сувишног одлагања добије потврду о обради личних података у вези с њим/њом. Комуникација треба да буде у разумљивом облику, укључујући све информације о пореклу података, као и све друге информације које се захтевају од руковођа, како би се осигурала транспарентност обраде, посебно информација из принципа 10.

11.2. Запослени треба да има право да личне податке у вези с њим/њом исправи, блокира или обрише уколико су они нетачни и/или уколико су подаци обрађени у супротности са законом или с принципима из ове препоруке. Такође, треба да, у сваком тренутку, има право на приговор на обраду својих личних података, осим уколико је обрада неопходна у сврху запошљавања или на други начин предвиђена законом.

11.3. Право на приступ, такође, треба гарантовати у погледу података за евалуацију, укључујући и то када се ти подаци односе на процену учинка, продуктивности или способности запосленог када је процес процене најкасније завршен, не доводећи у питање право на одбрану послодавца или треће заинтересоване стране. Иако такви подаци не могу бити исправљени од стране запосленог, чисто субјективна процена треба да буде отворена за изазове у складу с домаћим законом.

11.4. Запослени не треба да буде предмет одлуке која значајно утиче на њега/њу, засноване само на аутоматској обради података без узимања у обзир његовог/њеног мишљења.

11.5. Запослени, такође, треба да буде у могућности да на захтев добије информације о образложењу за обраду података, чији се резултати примењују на њега/њу.

11.6. Одступања од права наведених у ст. 10, 11.1, 11.2, 11.4 и 11.5 могу се дозволити уколико је то прописано законом и представља неопходну меру у демократском друштву ради заштите државне сигурности, јавне сигурности, важних економских и финансијских интереса државе или спречавања и сузбијања кривичних дела, заштиту лица на које се подаци односе или права и слобода других.

11.7. Надаље, у случају унутрашње истраге коју спроводи послодавац, остваривање права из ст. 10. и од 11.1 до 11.5 може се одложити до затварања истраге уколико би остваривање тих права угрозило истрагу.

11.8. Уколико одредбе домаћег закона не предвиђају другачије, запослени треба да има право да одабере и именује лице које ће му/јој помагати у остваривању његових/њених права на приступ, исправку и приговор или ће остваривати ова права у име њега/ње.

11.9. Домаћи закон треба да осигура правни лек у случају одбијања приступа подацима, или одбијања захтева за исправку, или брисања неких од тих података.

12. Сигурност података

12.1. Послодавци или правна лица која могу обрађивати податке у њихово име, треба да спроведу адекватне техничке и организационе мере као одговор на повремене контроле процене ризика организације и сигурносних политика и да их ажурирају на одговарајући начин. Такве мере треба да буду дизајниране како би заштитиле сигурност и поверљивост личних података, који се обрађују у сврхе запошљавања, од случајних или неовлашћених измена, губитка или уништавања личних података, као и од неовлашћеног приступа, ширења и откривања тих података.

12.2. У складу с домаћим законом, послодавци треба да осигурају адекватну сигурност података приликом употребе ИКТ-ова за сваку операцију обраде личних података у сврхе запошљавања, укључујући и њихово складиштење.

12.3. Стручни кадар, као и свако друго лице које се бави обрадом ових података, треба да буде обавештено о тим мерама, о потреби поштовања истих и о потреби одржавања поверљивости у вези с тим мерама.

13. Чување података

13.1. Послодавац не треба да задржава личне податке дуже него што је оправдано у сврхе запошљавања наведене у принципу 2, односно онолико колико то захтевају интереси садашњег или бившег запосленог.

13.2. Лични подаци коју су достављени уз пријаву за посао обично се бришу чим постане јасно да неће бити понуде за запослење или да апликант не прихвата понуду. Уколико се ти подаци чувају с циљем даљих прилика за посао, лице на које се подаци односе треба да буде обавештено о томе и на његов/њен захтев треба обрисати те податке.

13.3. Где је неопходно чување података достављених уз пријаву за посао за сврхе предузимања правних радњи или за неку другу легитимну сврху, податке треба складиштити само на временски период неопходан за испуњавање те сврхе.

13.4. Лични подаци који се обрађују у сврху унутрашње истраге коју спровode послодавци, а која није довела до усвајања негативних мера у вези с било којим запосленим, треба да се обришу након разумног периода, не доводећи у питање права на приступ запосленог док се одвија то брисање.

II део – Посебни облици обраде

14. Употреба интернета и електронских комуникација на радном месту

14.1. Послодавци треба да избегавају неоправдано и неразумно уплитање у право на приватни живот запосленог. Овај принцип се односи на све техничке уређаје и ИКТ-ове које користи запослени. Предметна лица треба да буду правилно и периодично информисана у примени јасне политике приватности, у складу са принципом 10. ове препоруке. Информације треба ажурирати и треба да обухватају сврху обраде, периода чувања или *back-up*-а саобраћаја података и архивирање професионалних електронских комуникација.

14.2. У случају обраде личних података везаних за интернет или интранет странице којима приступа запослени, посебну предност треба дати усвајању превентивних мера, као што је употреба филтера који спречавају одређене операције, као и оцењивању могућег праћења личних података, дајући предност неиндивидуалним насумичним проверама података које су анонимне или, на неки начин, прикупљене.

14.3. Приступ послодаваца професионалним електронским комуникацијама њихових запослених који су унапред информисани о постојању такве могућности, може се догодити само када је то неопходно за сигурност или из других легитимних разлога. У случају одсутности запослених, послодавац треба да предузме неопходне мере и предвиди одговарајуће поступке с циљем омогућавања приступа професионалним електронским комуникацијама само када је такав приступ за професионалне потребе. Приступ треба да се догоди на најмање могуће наметљив начин и само након обавештења предметних запослених.

14.4. Садржај, слање и примање приватне електронске комуникације на послу не треба да се надзиру ни под којим околностима.

14.5. По одласку запосленог из неке организације, послодавац треба да предузме неопходне организационе и техничке мере да аутоматски деактивира налог за електронске поруке запосленог. Ако послодавци треба да врате садржај налога запосленог, у циљу ефикасног управљања организацијом, то треба да ураде пре његовог/њеног одласка и, где је то изводљиво, у његовом/њеном присуству.

15. Информациони системи и технологије за надзор запослених, укључујући и видео-надзор

15.1. Увођење и коришћење информационих система и технологија за директну и принципијелну сврху надзора активности и понашања запослених не би требало дозволити. Где њихово увођење и употреба за друге легитимне сврхе, као што су заштита производње, здравља и сигурности или осигурање ефикасног вођења неке организације, има за индиректну последицу могућност надзора активности запослених, то би требало да буде предмет додатних сигурносних мера из принципа 21, нарочито консултације заступника запослених.

15.2. Информациони системи и технологије којима се индиректно надзиру активности и понашање запослених треба да буду посебно дизајнирани и лоцирани тако да не

нарушавају њихова основна права. Употреба видео-надзора за надзор просторија које су део најинтимније области живота запослених није дозвољена у било којој ситуацији.

15.3. У случају спора или судског поступка, запослени треба да буду у могућности да добију копије свих снимака, када је то потребно и у складу с домаћим законом. Складиштење снимака треба да буде временски ограничено.

16. *Опрема која открива локације запослених*

16.1. Опрема која открива локације запослених треба увести само ако се то покаже неопходним за постизање легитимне сврхе коју спроводе послодавци и њихова употреба не треба да води континуираном надзору запослених. Наиме, надзор не треба да буде главна сврха, већ само индиректна последица радње која је потребна за заштиту производње, здравља и сигурности, или за осигурање ефикасног вођења неке организације. С обзиром на могуће кршење права и слобода предметних лица употребом ових уређаја, послодавци треба да осигурају све неопходне гаранције за права на приватност и заштиту личних података запослених, укључујући и додатне сигурносне мере из принципа 21. У складу са принципима 4. и 5, послодавци треба да обрате посебну пажњу на сврху за коју се такви уређаји користе и на принципе минимализације и пропорционалности.

16.2. Послодавци треба да примене одговарајуће интерне процедуре у вези с обрадом ових података и о њима треба унапред да обавесте предметна лица.

17. *Механизам интерног извештавања*

17.1. Где су послодавци обавезни по закону или интерним правилима да имплементирају механизме интерног извештавања, као што су СОС линије, треба да осигурају заштиту личних података свих укључених страна. Нарочито, послодавац треба да осигура поверљивост запосленог који извештава о незаконитом или неетичком понашању (као што су узбуњивачи – корупција). Лични подаци укључених страна треба да се користе само у сврхе одговарајућих интерних процедура везаних за извештај и у складу са законом или када је то потребно за накнадне судске поступке.

17.2. У изузетним околностима, послодавци могу да омогуће анонимно извештавање. Интерне истраге не треба спроводити само на основу анонимног извештаја, осима ако тако захтевају околности и тиче се озбиљних повреда домаћег закона.

18. *Биометријски подаци*

18.1. Сакупљање и даљу обраду биометријских података треба предузети само онда када је то неопходно за заштиту легитимних интереса послодаваца, запослених или трећих страна, само уколико друга мање наметљива средства нису на располагању и само уз одговарајуће заштитне мере, укључујући додатне заштитне мере из принципа 21.

18.2. Обрада биометријских података треба да се заснива на научно признатим методама и треба да буде предмет захтева строге сигурности и пропорционалности.

19. *Психолошки тестови, анализе и слични поступци*

19.1. Прибегавање психолошким тестовима, анализама и сличним поступцима које спроводе специјализовани стручњаци, у зависности од медицинске поверљивости, који су дизајнирани за процену карактера или личности запосленог или апликанта за посао, треба дозволити само уколико су законити и неопходни за врсту активности која се обавља на послу, уколико домаћи закон предвиђа сигурносне мере.

19.2. Запосленог или апликанта за посао треба унапред информисати о употреби резултата ових тестова, анализа и сличних поступака и, потом, о садржају истих. У складу с тим, примењују се принципи 11.1 и 11.2.

20. *Друга обрада која представља ризике за права запослених*

20.1. Послодавци, или где је то могуће, обрађивачи треба да спроведу анализу ризика могућег утицаја било које планиране обраде података на права и основне слободе запослених и да дизајнирају операције обраде података тако да спрече или бар минимализују ризик од мешања у та права и основне слободе.

20.2. Осим ако домаћи закон или пракса обезбеђују друге одговарајуће сигурносне мере, сагласност представника запослених треба тражити пре увођења или адаптације ИКТ-ова, где се анализама открије ризик од мешања у права и основне слободе запослених.

21. *Додатне сигурносне мере*

За посебне облике обраде из II дела ове препоруке, послодавци треба да осигурају поштовање следећих заштитних мера, нарочито следеће.

а. Да обавесте запослене пре увођења информационих система и технологија које омогућавају праћење њихових активности. Дате информације треба редовно ажурирати и у обзир треба узети принцип 10. ове препоруке. Информације треба да укључују сврху операције, периода чувања или *back-up*-а, као и постојање или непостојање права на приступ и исправку и како се та права могу остварити.

б. Да предузму одговарајуће интерне мере везане за обраду тих података и да унапред обавесте запослене.

в. Да консултују представнике запослених у складу с домаћим законом или праксом, пре могућности увођења било ког система за надзор или у околностима где се тај надзор може променити. Када се у поступку консултација открије могућност нарушавања права на приватност и људског достојанства запослених, треба прибавити сагласност заступника запослених.

г. Да о обради личних података, у складу с домаћим законом, консултују државни надзорни орган.