

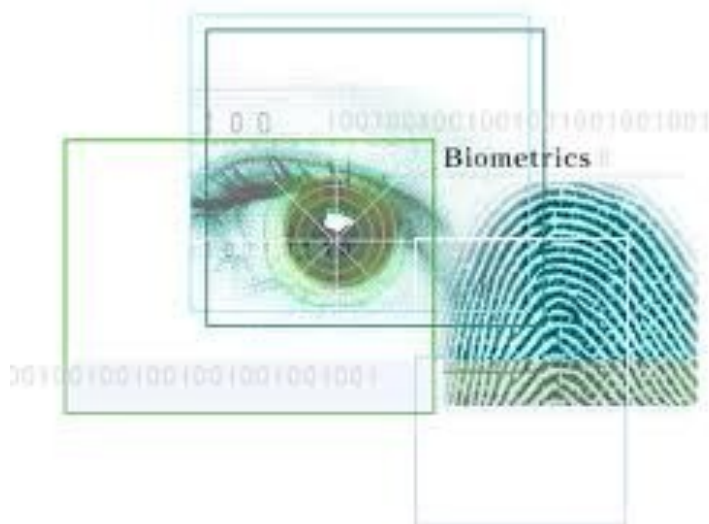


Поддршка на Дирекцијата за заштита на личните податоци

Проектот е финансиран од Европската унија

Прирачник

за обработка на биометриски
ПОДАТОЦИ



ДЗЛП

Дирекција за заштита на
личните податоци



Проектот е имплементиран Human Dynamics во соработка со :

IPS Institute

Almaviva S.p.A.

Czech Office for Personal Data Protection OPDP

Privacy International

“This publication has been produced with the assistance of the European Union. The contents of this publication are sole responsibility of the Directorate for Personal Data Protection and can in no way be taken to reflect the views of the European Union.”

“Оваа публикација е изготвена со помош на Европска унија. Содржината на оваа публикација е единствена одговорност на Дирекцијата за заштита на личните податоци и на никаков начин не ги рефлектира гледиштата на Европската унија .”

“Ky publikim është përgaditur me ndihmën e Unionit Evropian. Përmbajtja e këtij publikimi është përgjegjësi vetëm e Drejtoria për Mbrojtjen e të Dhënave Personale dhe në asnjë mënyrë nuk reflekton opinionin e Unionit Evropian.”

За издавачот:

Димитар Георгиевски

Издавач:

Дирекција за заштита на личните податоци

Печати :

МПЦ-ОА-Митрополија Скопска печатница "Синај"

Печатењето на публикацијата финансиски е поддржано од:

Проектот „Поддршка на Дирекцијата за заштита на личните податоци“ финансирано од Европската Унија

CIP - Каталогизација во публикација

Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

342.738.071.1(497.7)"2012/2016"

Прирачник за заштита обработка на биометриски податоци:

Дирекција за заштита на личните податоци, 2012. - 18 стр. :

табели ; 19 см

ISBN 978-608-4682-02-8

а) Заштита на лични податоци - Стратегија - Македонија - 2012-2016

COBISS.MK-ID 89777674



Содржина

I. ВОВЕД	3
ЦЕЛ НА ПРИРАЧНИКОТ	3
ЗА КОГО Е НАМЕНЕТ ОВОЈ ПРИРАЧНИК?	3
ШТО СЕ ВСУШНОСТ БИОМЕТРИСКИ ЛИЧНИ ПОДАТОЦИ?	4
ШТО ЗНАЛИ ОБРАБОТКА НА БИОМЕТРИСКИ (ЛИЧНИ) ПОДАТОЦИ?	4
II. ОСНОВНИ НАЧЕЛА ЗА ПРАВИЧНА ОБРАБОТКА	7
ПРИНЦИП ЗА ЦЕЛ НА ОБРАБОТКА И ПРОПОРЦИОНАЛНОСТ	7
ПРАВО НА СУБЈЕКТОТ/ГРАЃАНИНОТ ДА БИДЕ ИЗВЕСТЕН ЗА ОБРАБОТКАТА НА ЛИЧНИТЕ/БИОМЕТРИСКИ ПОДАТОЦИ	7
III. ДИРЕКЦИЈАТА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ (ДЗЛП)	8
Како да се поднесе Барање за добивање одобрение за обработка на биометриски податоци?	8
ДОДАТОК – Воведување на биометрија на работното место	13
1. СИСТЕМИ ЗА БИОМЕТРИЈА	13
2. НАЧЕЛА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ КОИ СЕ ОДНЕСУВААТ НА БИОМЕТРИСКИТЕ МЕРКИ НА РАБОТНОТО МЕСТО	13

I. ВОВЕД

Биометријата зазема значајно место во модерниот свет, сепак општеството се соочува со многу важни одлуки во однос на долгорочниот став за ова прашање. Употребата на биометријата се зголемува; може да се забележи во неколку области и е употребена за различни причини: одбрана, мерки за гранична контрола, имиграција, пасоши, банки и финансиски институции, информатички системи итн. Од гледна точка на граѓаните (поединците), биометријата има одредени практични предности. Како и секоја друга технологија биометријата може да се користи на начин кој е „пријателски“ во однос на приватноста на поединците, но од друга страна може да предизвика сериозни упади во приватноста на граѓаните.



Практичните предности на биометријата по правило се веднаш видливи, спротивно од некои аспекти кои покажуваат дека биометријата не е совршена и не се видливи на прв поглед. Биометриските податоци по својата природа претставуваат упад во приватноста и достоинството на поединецот, поради тоа сите услови за нивна употреба треба да се толкуваат во поглед на заштита на приватноста и достоинството.

Цел на прирачникот

Овој прирачник ги објаснува правилата во однос на тоа кога и под кои услови контролорите може да воведат обработка на биометриски лични податоци, како и во однос на тоа кои се нивните обврски поврзани со ова прашање.

Целта на прирачникот е да ги објасни основните карактеристики на биометриските податоци, да разјасни некои од дилемите поврзани со обработката на биометриските податоци и да даде одговор на често поставуваните прашања од страна на јавниот и приватниот сектор во врска со воведувањето на биометриските мерки. Прирачникот исто така се осврнува и на воведување на биометриските мерки на работното место.

Со помош на овие објаснувања, одговори и насоки, компаниите и другите контролори и обработувачи на лични податоци ќе можат соодветно да се усогласат со одредбите и начелата од Законот за заштита на личните податоци („Службен весник“ бр. 7/05, 103/08, 124/10 и 135/11), меѓународните стандарди и принципи на регулативата на ЕУ (Директивата 95/46/ЕК на Европскиот парламент и Советот од 24.10.1995 година за заштита на поединците во однос на обработката на лични податоци и слободното движење на таквите податоци).

За кого е наменет овој прирачник?

Овој Прирачник е наменет за контролорите и обработувачите на лични податоци и кои било други компании или институции кој вршат обработка на биометриски лични податоци. Исто така, граѓаните и пошироката јавност можат да најдат бројни информации во врска со исполнување на нивните права кои им се дадени со Законот за заштита на личните податоци (ЗЗЛП).

Што се всушност биометриски лични податоци?

Едноставно дефинирано, **биометрија** е наука за идентификување на личност врз основа на физиолошки карактеристики и карактеристики на однесување, кои не се делат со ниту еден друг поединец и поради тоа се уникатни и постојани. Сите ние може да бидеме идентификувани преку ваквите мерливи карактеристики како што се отпечаток од прст, папиларните линии на прстот, ирисот, ретината, лицето, ушите, ДНК па дури и по нашиот типичен став и начинот на одење. Одредени физички, физиолошки карактеристики па дури одредени карактеристики на однесување се соодветни за идентификација на поединецот, ако овозможуваат веродостојни и точни биометриски податоци, кои можат да вршат функција на уникатна и индивидуална „лозинка“ за личноста.

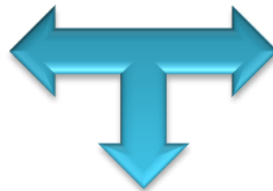
Следниве човечки карактеристики се најчесто користени во биометријата:

Карактеристики на однесување

како што е потписот, говорот, начинот на движење итн.

Физички карактеристики

како отпечаток од прст или рака, карактеристики на лицето, ирисот и ретината во окото, ушите, мирис, ДНК



По правило биометриските податоци се уникатни, непреносливи на други, не можат да се забораваат или изгубат, тешки се за репродуцирање или фалсификување, можат да се користат со или без знаење/согласност на поединецот, тешко можат да се менуваат или скријат.

Што значи обработка на биометриски (лични) податоци?

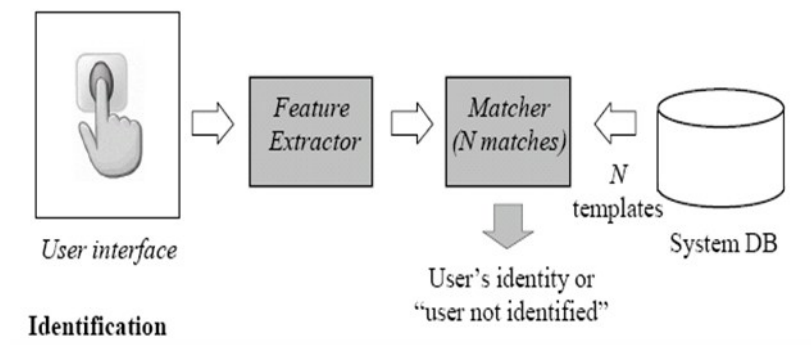
"Обработка на личните податоци" е секоја операција или збир на операции што се изведуваат врз лични податоци на автоматски или друг начин, како што е: собирање, евидентирање, организирање, чување, приспособување или промена, повлекување, консултирање, употреба, откривање преку пренесување, објавување или на друг начин правење достапни, изедначување, комбинирање, блокирање, бришење или уништување.

Биометриските податоци (како отпечаток од прстот, ирисот и ретината во окото, карактеристиките на лицето итн.) даваат извор на карактеристики кои се уникатни за секој поединец, а како карактеристики по кои поединецот може да се идентификува или барем да биде идентификуван, несомнено преставуваат лични податоци. Оттука, секое собирање, чување, делење, пренесување или уништување на таквите податоци ќе се смета за обработка на личните податоци, која е соодветно регулирана со одредбите на ЗЗЛП.

За подобро разбирање на обработката на личните податоци, неопходно е да се прави разлика помеѓу верификација и идентификација. Разликата помеѓу овие две полиња на примена е значајно бидејќи верификацијата и идентификацијата како апликации се користат за различни задачи во неспоредливи полиња.

Што е биометриска идентификација?

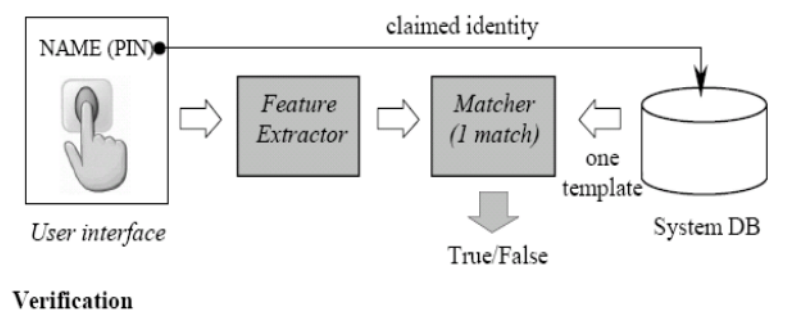
Биометриски потпис (т.н. темплејт) на непознато лице се внесува во системот. Системот за биометрија го споредува овој темплејт со темплејтите на познати личности кои се собрани во база на податоци. По процесот на компарација системот дава одговор дали темплејтот на непознатото лице се наоѓа во базата на податоци. Кога компарацијата е позитивна – непознатото лице се идентификува. Овој модел е познат како „еден-кон-сите“.



Што е биометриска автентикација (верификација)?

Кај биометриската верификација темплејтот на поединецот се споредува со веќе претходно дадени карактеристики. За оваа операција лицето мора прво да даде пример од одредена карактеристика за верификација. Овој процес (наречен „запишување“) ја конвертира/претвора карактеристиката, користејќи математички методи, во дигитална форма – темплејт – (пр. слика од отпечаток на прст) која понатаму може да биде зачувана на компјутерска датотека или во меморијата на SMART CARD. Темплејтот се користи кога е потребно да се направи споредба со ново дадени сет на карактеристики за верификација.

Системот споредува два темплејта – едниот даден на лице место (вистинската карактеристика) и вториот претходно внесен во токен кој поединецот го покажува како дел од неговиот идентитет. Кога споредбениот процес е идентичен тогаш системот утврдува дека идентитетот е точен. Овој модел е познат како „еден-на-еден“.



На пример

Во модот за верификација, биометриската технологија врши една споредба на презентираниот податок со темплејт кој е претходно зачуван. Пример за ова е скенер за отпечаток на прст на електронски сеф. Во модот на идентификација, се користи биометриска база на податоци. Се презентира одреден биометриски податок и системот проверува дали овој податок се совпаѓа со друг податок од веќе постоечките податоци во базата. Пример за биометриска идентификација е базата на отпечатоци на сторители на кривични дела.

Обработката на биометриски лични податоци денеска често се користи при автоматизирани процедури за верификација и идентификација, особено за контрола на пристапот како во физички така и во виртуелни простории (т.е. пристап до одреден електронски систем или услуга).

Земајќи го во предвид брзиот развој на технолошката еволуција и зголемена грижа за безбедност, многу од биометриските системи работат преку комбинирање на различни биометриски модалитети на корисникот со други технологии за идентификација и верификација. Некои системи, на пример комбинираат препознавање на лице и препознавање на глас.

Собирањето на биометриски примероци, т.н. биометриски податоци (пр. слика на отпечаток од прст, слика од ирисот или ретината, снимањето на гласови) се врши во фазата наречена „запишување“ преку користење на сензор специфичен за секој вид на биометрија. Биометрскиот систем екстрактира од биометрскиот податок карактеристики специфични за корисникот за да направи биометриски „темплејт“. Темплејтот е структурирана редукција од биометриската слика: зачуваната биометриска „мерка“ на поединецот. Темплејтот, даден во дигитализирана форма, ќе биде зачуван, а не и самиот биометриски елемент. Покрај тоа, биометриските податоци можат да се обработат и како сурови податоци (слики) зависно од функционалноста на биометрскиот систем кој се користи. Ова се однесува и за други биометриски системи, како што се оние кои се базираат на анализа на ракопис или далечно препознавање на ликот на сметка на специфичните карактеристики на технологијата. Проблематичниот аспект, од една страна, е тоа дека собирањето и обработката на овие податоци може да се изврши без знаење на субјектот на лични податоци, а од друга страна без разлика на нивната моментална сигурност, овие биометриски технологии си дозволуваат да ја покријат употребата за сметка на нивното „наметнување на ниско ниво“. Поради тоа е потребно да се постават специфични заштитни мерки.”¹

Постои одредена загриженост во областа на биометриските технологии и чувањето на биометриски податоци во големи размери. На пример, податоците подоцна можат да се користат за други цели за кој поединецот не дал согласност, како и можноста истите да бидат украдени. Друго прашање е загриженоста дека зачуваните биометриски податоци можат да бидат злоупотребени за дискриминација на одредени сектори од популацијата.

Според ова многу е важно да се почитуваат начелата за обработка на личните податоци за цел на законска и правична обработка во согласност со одредбите утврдени во ЗЗЛП:

¹ Работен документ за биометрија 12168/02/EN WP 80 – ЧЛЕН 29 – Работна група за заштита на личните податоци

II. ОСНОВНИ НАЧЕЛА ЗА ПРАВИЧНА ОБРАБОТКА

Биометриските лични податоци согласно одредбите од ЗЗЛП се сметаат за посебни категории на лични податоци, па поради тоа специјални обврски за правична обработка се утврдени во ЗЗЛП. Контролорите и обработувачите може да обработуваат биометриски податоци само доколку таквиот вид на обработка е специфично утврдена со закон. Во други случаи, генерално, обработката на биометриските податоци е забранета, но како исклучок може да се обработуваат врз основа на изречно дадена согласност од субјектот на личните податоци (граѓанинот) за обработка на такви податоци, освен кога со закон е предвидено дека забраната за обработка на такви податоци не може да се отповика со изречна согласност од субјектот на личните податоци. Но иако контролорот сака да врши обработка на биометриски податоци врз основа на согласноста на граѓанинот мора да добие одобрение од Дирекцијата за заштита на личните податоци (ДЗЛП) за обработка на биометриски податоци пред самиот почеток на обработката. (види член 29 од ЗЗЛП)

Принцип за цел на обработка и пропорционалност

Почитувањето на овој принцип првенствено подразбира јасно утврдување на целта заради која се собираат и обработуваат биометриските податоци. Покрај тоа, неопходна е евалуација на принципот за пропорционалност и законитост земајќи ги во предвид ризиците врз фундаменталните права и слободи на граѓаните, особено фактот дали целта заради која се врши обработката на биометриските податоци може да се постигне на помалку „нападен“ начин. Затоа, контролорите и обработувачите мораат прво да ја утврдат правната основа за обработка на биометриски податоци. Ако не постои правна основа за обработка на биометриските податоци, тогаш оваа обработка е забранета. Иако согласноста од граѓанинот за обработка на биометриски податоци претставува правна основа за обработка мора да се има во предвид, како што е наведено и претходно, дека контролорите и обработувачите сепак треба да добијат одобрение од ДЗЛП пред почетокот на обработката на биометриските податоци и формирањето на Збирка на лични/биометриски податоци.

На пример, за цели на контрола на пристап (верификација), биометрискиот систем кој користи физички карактеристики кој не оставаат трага (пр. отпечаток на дланката, но не и отпечаток од прст) или биометриски систем кој користи физички карактеристики кои оставаат траги, но не се потпираат на меморирање на податоците за некој друг освен за поединецот

Со други зборови, податоците не се меморираат во уредот за контролирање на пристапот или во друга централна база на податоци. Овие системи креираат помал ризик за приватноста на граѓаните и зависно од целта може да се сметаат за соодветна обработка на биометриски податоци.

Право на субјектот/граѓанинот да биде известен за обработката на личните/биометриски податоци

Кога се врши обработка на биометриски податоци, граѓанинот треба да биде известен/информиран за целите на обработка, идентитетот на контролорот, категориите/видот на биометриски податоци кои се обработуваат, корисниците и категоријата на корисници на податоците кои се чуваат. Каде што е потребно и други информации треба да му бидат дадени на граѓанинот за да се гарантира правична обработка.

Граѓанинот може во секое време да побара од контролорот да го извести за обемот на лични податоци или категориите на лични податоци кои се обработени, а се однесуваат за него, за целта/ите за обработка на личните податоци, начините на обработка (види членови 10, 11, 12 од ЗЗЛП).

Информациите на граѓанинот треба да му бидат дадени во разбирлива форма, користејќи јасен и едноставен јазик, особено кога некоја обработка се однесува на малолетници.

Кога личните податоци се обработувани преку биометриски систем, граѓанинот треба да биде известен/алармиран (пр. звучен сигнал) освен ако веќе ја има добиено оваа информација.

III. ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ (ДЗЛП)

Во поширока смисла на зборот, Дирекцијата за заштита на личните податоци е надлежна за соодветна примена на Законот за заштита на личните податоци. Ова значи дека ДЗЛП се грижи за заштита на личните податоци на граѓаните и ја заштитува нивната приватност.

Оваа улога ДЗЛП ја врши преку:

- ⇒ Решавање на претставките и жалбите на граѓаните за повреда на нивните права преку вршење на вонреден инспекциски надзор и
- ⇒ Вршење на инспекциски надзори по службена должност за да провери дали се врши правилна примена на начелата за заштита на личните податоци.

Меѓутоа, мора да се потенцира дека ДЗЛП нема само репресивна улога, односно не решава само проблемите кога ќе се случат. Напротив, улогата на ДЗЛП е поблиску да ги запознае граѓаните со нивните права.



Како да се поднесе Барање за добивање одобрение за обработка на биометриски податоци?

Како што е наведено и претходно, доколку контролорот планира да обработува биометриски податоци врз основа на согласноста на субјектот/граѓанинот, мора за истото да добие одобрение од ДЗЛП пред почетокот на обработката. Не постои посебен образец за Барањето, но ДЗЛП ги утврдува податоците кои треба да ги содржи истото. Задолжително е за контролорот да ги наведе следниве податоци со цел да добие одобрение од ДЗЛП за обработка на биометриски податоци:



Податоци кои мора да ги содржи Барањето	Објаснување
1. Назив на збирката на лични податоци	Едноставно, се наведува само називот на збирката пр. Збирка на биометриски податоци за
2. Назив односно лично име на контролорот и неговото седиште, односно адреса, како и називот и адресата на неговиот претставник, доколку го има	
3. Цел или цели на обработка	Целта на обработка е многу важна па поради тоа контролорот треба јасно да ја утврди целта како и да ја објасни оправданоста на целта за обработка. Пр. Влегување или пристап до сеф во банка, влез во простории кои содржат сензитивна или скапа опрема или простории кои се сметаат за осетливи за целокупната безбедност на просторот итн.
4. Правна основа за воспоставување збирка на лични податоци	Контролорот ја наведува правната основа за обработка на биометриски податоци, односно дека обработката се врши врз основа на согласност на субјектот. <u>ВАЖНО: Доколку правната основа за обработка на биометриски податоци е утврдена со закон тогаш не постои обврска за барање одобрување за обработка на биометриски податоци</u>
5. Категорија или категории на субјектите на личните податоци и лични податоци, односно категории на личните податоци кои се однесуваат на него или нив	Категориите/видот на биометриски податоци кои се предмет на обработка мора да бидат наведени пр. Отпечаток од прст, отпечаток од рака, карактеристики на лицето, ирис или ретината во окото, увото, ДНК итн.
6. Корисниците или категориите на корисници на кои можат да им се дадат на користење личните податоци	Ако контролорот планира да ги пренесува биометриските податоци до трето лице или да ги даде на обработувач мора да го наведе називот т.е. името на корисникот <u>ВАЖНО: За да можат биометриските податоци да бидат дадени на користење за истото мора да постои законска основа. Во овој случај контролорот ја наведува и законската причина</u>
7. Рок на чување на лични податоци	Биометриските податоци може да бидат чувани само во рок кој е доволен за да се исполни целта заради која се собрани и понатаму обработени. Контролорот ја утврдува и специфицира временската рамка на рокот.
8. Пренос на лични податоци во други држави	Контролорот мора да наведе доколку врши пренос на биометриските податоци во други држави, но во овој случај мора да ги земеме во предвид и одредбите од ЗЗЛП кои се однесуваат за пренос на лични
9. Општ опис со кој ќе се овозможи првична оценка на соодветноста на преземените технички и организациски мерки за заштита на личните податоци и на нивната обработка	Бидејќи биометриски податоци се сметаат за чувствителна категорија на лични податоци контролорот мора да наведе целосно детално објаснување за преземените технички и организациски мерки за безбедност <u>ВАЖНО: Техничките и организациските мерки мора да бидат усогласени со безбедносните мерки утврдени со Правилникот за технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци</u>

ЧПП - Често поставувани прашања

Дали темплејтите кои се користат во современите биометриски системи се сметаат за лични податоци?

Личен податок (согласно член 2 став 1 алинеја 1 од ЗЗЛП) е секоја информација која се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува, а лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на матичен број на граѓанинот или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, ментален, економски, културен или социјален идентитет.

По својата природа, биометриските податоци се податоци кои се однесуваат на идентификувано физичко лице или физичко лице кое може да се идентификува, пр. отпечаток од прст припаѓа на одредено именувано лице. Прашањето е: дали ова се однесува на биометриски податоци зачувани во намлена, дигитализирана форма – темплејт? Извештај издаден од Советот на Европа нотираше дека дилемата дали биометриските податоци се секогаш лични податоци, или само кога одредени услови се исполнети е нерелевантно. Имено, ако биометриските податоци се собрани за цел за понатамошна автоматска обработка тогаш постои можност таквите податоци да бидат поврзани со идентификувано физичко лице, што е во согласност со дефиницијата за лични податоци.

Она што се применува и важи за биометриските карактеристики, важи и ќе се применува за дигиталните записи од истите тие карактеристики, без разлика на фактот за природата на дериватот или колку пати таквиот запис бил изменет. Иако, квалитетот на деталите може да се намалува во процесот на трансформација сепак останува потенцијална уникатна конекција со личноста: формата, форматот, начинот на снимање или други измени не се значителни фактори.

Врз основа на горенаведеното, може да се каже дека биометриските податоци, иако зачувани во намалена дигитализирана форма, сепак се сметаат за лични податоци бидејќи ексклузивно се однесуваат за одреден – идентификуван – поединец.

Зошто биометријата е регулирана со Законот за заштита на личните податоци (ЗЗЛП)?

Биометриските податоци (како отпечаток од прст, ирисот и ретината во око, цртите на лицето итн.) даваат извор на карактеристики кои се единствени/уникатни и кои се однесуваат само за секое лице посебно, и како карактеристики по кои физичкото лице се идентификува, тие несомнено преставуваат лични податоци. Оттука, секое собирање, чување, давање на користење или уништување на таквите податоци ќе се смета за обработка на лични податоци и поради тоа е соодветно регулирана со одредбите на ЗЗЛП.

Зошто биометријата е предмет на одобрување?

Треба да бидеме свесни дека биометријата не е само метод за утврдување или потврдување на идентитет, но технологија која го користи човечкото тело – впрочем нашите физички карактеристики или карактеристики на однесување – како инструмент. Постои цврста тенденција на производителите и дистрибутерите на биометриските системи кон маргинализирање на собирањето на човечките физички карактеристики и карактеристики на однесување. Не-критикуваното или неконтролираното собирање може да има вистински и сериозни последици за поединците. Нашата приватност може сериозно да биде загрознена како последица на непотребното и неовластено собирање, употреба, несоодветно чување или пренесување на биометриските податоци.

ДЗЛП е обврзана да врши испитувања на планираните биометриски мерки и да оцени дали нивното воспоставување е во согласност со начелата и правилата за заштита на личните податоци. Кога оценува одредена технологија, покрај целта поставена од контролорот, ДЗЛП исто така треба да ги земе во предвид и техничките карактеристики на биометрискиот систем, особено и нивото на ризик за дадената биометриска технологија, како што е можноста за спојување и можноста за контрола врз своите лични податоци.

ДОДАТОК – Воведување на биометрија на работното место

Овој додаток го надополнува прирачникот и се фокусира на обработката на биометриските податоци на работното место. Овие насоки се наменети за работодавците со цел да ги охрабри да размислат дали биометрискиот систем е усогласен со начелата за заштита на личните податоци утврдени во ЗЗЛП.

Реална и оправдана причина мора да биде основата за секоја потреба од правење идентификација или верификување на идентитет, а исто така треба да биде поткрепено со фактот дека целта заради која работодавецот врши контрола не може да биде задоволително остварена преку користење на други (не биометриски) начини за идентификација и верификација кои би немале влијание врз приватноста и достоинството на поединците. Работодавецот мора да утврди зошто воведувањето на биометриски мерки е неопходно, односно која е крајната цел. Причините и намерите треба да бидат сериозни, основани и поддржани со докази; покрај тоа, мора да се направи и оценка во однос на прашањето дали воведувањето на биометриски мерки е неопходен предуслов за оперативни причини, за безбедноста на вработените или сопственоста или заштита на доверливи деловни податоци.



Пред воведувањето на биометриски мерки, работодавецот е обврзан да ја анализира можноста во однос на тоа дали постои некој друг соодветен не-биометриски метод за утврдување или проверка на идентитетот кој може задоволително да ги оствари своите потребите или обврски.

Пред да се направи било какво доставување на Барање за одобрение за обработка на биометриски податоци до ДЗЛП, неопходно е да се одлучи каков вид на систем е потребен, и како се планира да биде имплементиран. Колку повеќе системот се „меша“ во приватноста на поединецот (вклучувајќи и оние прашања за можноста за злоупотреба) толку пореална и пооправдана треба да биде причината за воведување на системот за биометрија. Аргументите исто така мора да ги покријат и техничките аспекти.

Ако компанијата сака да воведат систем со биометриски мерки и успее да докаже дека биометриските мерки не се само неопходни туку и се предуслов, и дека потребната цел не може да се постигне преку друг помалку интрузивен или штетен начин од перспектива на приватноста и достоинството тогаш употребата на однапред утврдените и однапред пропишаните биометриски мерки можат да бидат дозволени на работното место. Меѓутоа, практиката покажува дека контролорите имаат тенденција да воведат биометриски системи само затоа што е попрактично отколку систем со картички и само сакаат да ја спречат злоупотребата која настанува како резултат на позајмување на картичките помеѓу вработените. Работодавецот мора да докаже апсолутна потреба од воведување биометриски мерки на работното место за суштински оперативни причини, за безбедност на вработените или сопственоста или да заштити доверливи податоци и деловни тајни.

Само наведувањето на причини за воведување на биометрија без соодветна поткрепа, поддржана од докази, не ги исполнува правните предуслови.

1. Системи за биометрија

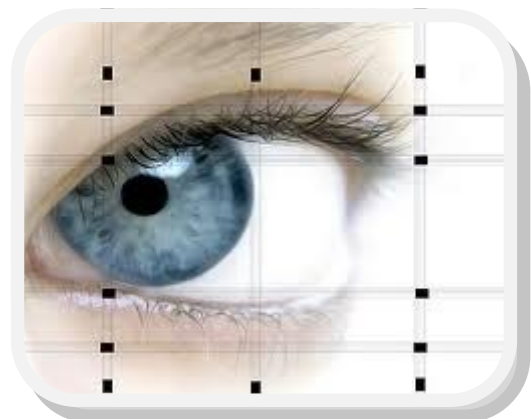
Биометриските системи работата со автоматска обработка на лични податоци за идентификација верификација на поединци (субјекти на лични податоци).

Биометриските податоци можат да се креираат од физички и физиолошки карактеристики како и од карактеристики на однесување на личноста (на пример отпечаток од прст, ирисот и ретината на окото, отпечаток од раката, цртите на лицето, гласот, ДНК, мирисот на телото, ракописот итн.). Дигитализиран темплејт е креиран преку користење на специјален софтвер. Потоа, темплејтот се споредува со биометрскиот податок на вработениот кој го презентира на читачот во реално време.

Во многу од биометриските системи, применети на работните места, се користат делумно енкриптирани податоци (направени од оригиналната слика, меѓутоа не може да бидат употребени за да се реконструира целосната оригинална слика на биометрскиот податок).

Постојат два основни видови на биометрски системи:

- ⇒ систем за идентификација: системот го утврдува идентитетот на поединецот (за ваков систем е потребно да се креира централна база со лични биометрски податоци. Централната база на податоци го зачувува темплејтот на централен систем кој се пребарува секој пат кога вработениот ќе го претстави својот биометрски податок на читачот. Овој систем е наречен „еден кон сите“).
- ⇒ систем за верификација: системот потврдува дека биометрскиот податок кој е презентира од едно лице во дадениот момент е идентичен со темплејтот кој е претходно зачуван на електронска картичка (системот ги споредува двата биометрски податоци; наречен е „еден кон еден“).



2. Начела за заштита на личните податоци кои се однесуваат на биометриските мерки на работното место

Пропорционалност

Член 5 од ЗЗЛП наведува дека „Личните податоци ќе бидат: соодветни, релевантни и не преобемни во однос на целта заради кои се собираат и обработуваат“.

Најважниот и клучен збор во оваа реченица е „**преобемни**“. Кога се размислува за имплементација на биометриски систем првото прашање е – за што е потребен истиот? Дали постојат други помалку „нападни“ алтернативни системи кои го имаат истиот ефект и ги даваат истите резултати? Дали работодавецот е свесен за фундаменталните права на работниците кои се заштитени со Уставот, Конвенцијата за фундаментални слободи и права и Законот за заштита на личните податоци. Поради тоа работодавецот треба да направи оценка на потребата од биометриски систем и да ги анализира различните видови на алтернативно воведување на одреден биометриски систем.

Други важни критериуми кои треба да бидат земени во предвид – околностите (средината), целите, ефикасноста и веродостојноста.

Околности – работодавецот ќе ја анализира природата на работното место (дали работното место навистина има потреба од такво високо ниво на заштита?). Дали е неопходно да се обработуваат посебни категории на лични податоци (биометриски податоци)?

Цел – работодавецот треба да го даде одговорот на прашањето „Може ли целта да се постигне на помалку „нападен“ начин кон достоинството на вработениот?“

Ефикасност – работодавецот треба да одговори на прашањето „Дали сме подготвени да ги исполниме сите административни чекори кои се неопходни за воведување на овој систем?“

Правично собирање и обработка

Член 5 од ЗЗЛП пропишува „Личните податоци ќе бидат обработени правично и во согласност со закон“.

Со цел да се постигне усогласеност со член 5, најмалку една од одредбите од член 6 од ЗЗЛП треба да биде исполнет:

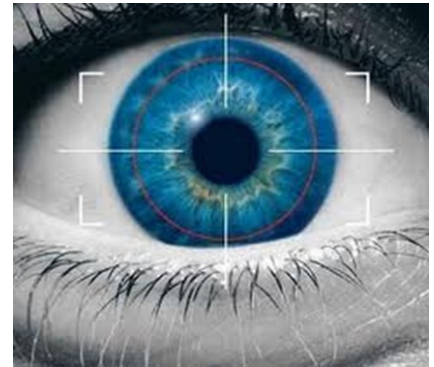
- ⇒ Согласност на вработениот;
- ⇒ За извршување на договор во кој вработениот е договорна страна или на барање на вработениот, пред негово пристапување кон договорот;
- ⇒ За исполнување на законска обврска на работодавецот;
- ⇒ Каде што обработката е неопходна за заштита на животот и суштинските интереси на вработените;
- ⇒ Каде што обработката е неопходна за извршување на работи од јавен интерес или на службено овластување на работодавецот;
- ⇒ Каде што обработката е неопходна за исполнување на легитимни интереси на работодавецот или на трето лице на кое му се откриени податоците, освен ако слободите и правата на вработените не преовладуваат над таквите интереси.

Мора да се наведе дека согласноста од вработените генерално не е задоволително легитимна во контекст на вработувањето ако не е слободно дадена. Само кога работодавецот ја нуди обработката на биометриски податоци како опција, само тогаш може да се смета дека согласноста е дадена слободно, односно доброволно (т.е. работникот има право на избор).

Правично собирање на чувствителни податоци

Мора да се потенцира дека во согласност со одредбите од членот 2 од Законот за заштита на личните податоци, биометриските податоци се сметаат за „посебна категорија на лични податоци“ (т.е. чувствителни податоци).

Член 2 став 10 пропишува - *“Посебни категории на лични податоци” се лични податоци кои го откриваат расното или етничко потекло, политичко, верско, филозофско или друго уверување, членството во синдикална организација и податоци што се однесуваат на здравјето на луѓето, вклучувајќи ги и генетските податоци, биометриски податоци или податоци кои се однесуваат на сексуалниот живот.*



За обработка на биометриски податоци (како чувствителни податоци), најмалку една одредба од член 8 од ЗЗЛП мора да биде исполнета:

- ⇒ Изречна согласност на вработениот;
- ⇒ Обработката е неопходна заради спроведување на конкретните права и обврски кои се наметнати или утврдени со Трудовото право;
- ⇒ Обработката е неопходна за заштита на суштински интереси на вработените или други лица;
- ⇒ Обработката е неопходна заради утврдување или остварување на поединечни правни интереси;
- ⇒ Обработката е неопходна заради стекнување, остварување и заштита на права на субјектот на лични податоци во постапка пред надлежни органи.

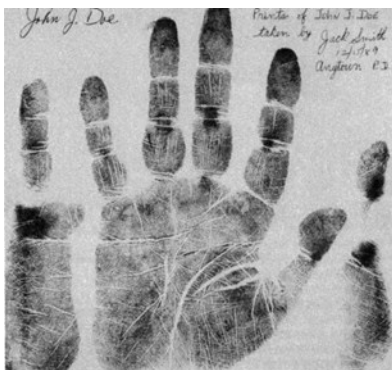
Мора да се напомени дека клучниот збор во споменатите одредби е „неопходна“.

Транспарентност

Членот 10 од ЗЗЛП утврдува дека субјектот на лични податоци мора да биде „информиран“ за неколку аспекти од обработката на личните податоци.

Во согласност со членот 10, работодавецот ќе ги даде најмалку следните информации на вработените за обработката на нивните лични податоци:

- ⇒ Идентитетот на работодавецот (или неговите овластени претставници);
- ⇒ Целта на обработката;
- ⇒ Трети страни на кои биометриските податоци можат да бидат откриени. (Откривањето на податоци се јавува во случај кога друга компанија го администрира, одржува и управува со системот. Откривање исто така подразбира праќање на биометриски податоци на матичната компанија).



Суштинската идеја е дека вработените треба да бидат свесни за целта поради која биометриските податоци се собираат и обработуваат. Ова значи дека работодавецот треба внимателно да размисли и да ја разгледа секоја цел. Транспарентноста е многу важна во случај кога за биометрискиот систем не е потребно знаење или активно учество на вработените (на пр. систем за препознавање на ликови може да направи и обработи слики од вработените без нивно знаење).



Точност

Членот 5 од ЗЗЛП наведува дека „Личните податоци ќе бидат точни, целосни и каде што е потребно ажурирани при што ќе се преземаат сите соодветни мерки за бришење или коригирање на податоците кои што се неточни или нецелосни, имајќи ги во предвид целите заради кои се собрани или обработени“.

Секој биометриски систем мора прецизно да ги идентификува личностите чии што податоци се обработени од системот. Ако некои физички или физиолошки карактеристики на вработениот се сменети истите потребно е да бидат изменети и во темплејтот. Темплејтот не смее да биде застарен. Процедурата за измена на темплејтот мора да обезбеди податоците да бидат ажурирани.

Безбедност

Член 23 од ЗЗЛП наведува „со цел да се обезбеди тајност и заштита на обработката на личните податоци на субјектот, контролорот и обработувачот треба да применат соодветни технички и организациски мерки за заштита од случајно или незаконско оштетување на личните податоци, или нивно случајно губење, изменување неовластено откривање или пристапување, особено кога обработката вклучува пренос на податоците преку мрежа и заштита од било какова незаконска форма на обработка“.

Работодавецот ќе оцени и реши кои ќе бидат соодветните безбедносни мерки. За да го направи тоа, најмалку четири фактори треба да бидат земени во предвид:

- ⇒ состојбата на технолошкиот развој;
- ⇒ трошоците за имплементација на технологијата;
- ⇒ природата на личните податоци кои се штитат;
- ⇒ штетите и ризиците кои може да резултираат од незаконската обработка на лични податоци.

Постојат минимум стандарди за безбедност кои треба да ги исполнува системот за обработка на биометриски податоци:

- ⇒ пристапот до биометрискиот систем ќе биде ограничен само за овластен персонал (на принцип “need -to-know” во согласност со внатрешно дефинираната политика);
- ⇒ компјутерски систем заштитен со лозинки;
- ⇒ техничките документи, информациите од екраните, техничките упатства треба да бидат скриени од личности кои не се овластени да ги гледаат;
- ⇒ редовна процедура за правење на копија; чување на копијата на друго оддалечена локација;
- ⇒ вработените се свесни за режимот на мерките за безбедност на работното место и се придржуваат на истите;
- ⇒ сите документи, треба да се користат под внимателен режим на употреба;
- ⇒ назначено е лице надлежно за безбедноста на системот;
- ⇒ се прави периодична ревизија на режимот за безбедност, мерките и практиката на истите.
- ⇒ работните простории се соодветно заштитени после работното време;
- ⇒ ако обработката се врши од страна на обработувачот за сметка на работодавецот, потребен е писмен договор за истото.

Рок на чување

Член 5 од ЗЗЛП наведува дека обработените лични податоци можат да бидат „чувани во форма која овозможува идентификација на субјектот на личните податоци, не подолго од што е потребно да се исполнат целите поради кои податоците се собрани за натамошна обработка“.

Во контекст на биометрискиот систем на работното место, неопходно е да се развие и утврди политика за рокот на чување на личните податоци, особено за биометриските податоци. Оваа политика треба да се донесе пред пуштање на системот во употреба. Исто така мора да се осигура дека кога вработениот трајно ќе го напушти работното место, неговите/нејзините биометриски податоци ќе бидат веднаш избришани.



www.privacy.mk

Email: info@dzlp.mk; info@privacy.mk; contact@dzlp.mk и contact@privacy.mk

Тел: ++ 389 (2) 3230 635

Факс: ++ 389 3230 635