20201221613

АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Врз основа на член 69 став (6) од Законот за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 42/20), директорот на Агенцијата за заштита на личните податоци донесе

ПРАВИЛНИК ЗА ОБУКА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

I. ОПШТА ОДРЕДБА

Член 1

Со овој правилник се пропишува начинот на спроведување на обука за вработените во контролорите, односно обработувачите, како и за офицерите за заштита на личните податоци од страна на Агенцијата за заштита на личните податоци (во натамошниот текст: Агенција), програмата за обука за заштита на личните податоци, формата и содржината на образецот за сертификатот, како и начинот на водење на евиденција за издадените сертификати.

II. НАЧИН НА СПРОВЕДУВАЊЕ НА ОБУКАТА

Член 2

Обуките утврдени согласно Годишната програма за обуки за заштита на личните податоци (во натамошниот текст: Годишна програма) ги организираат, подготвуваат и спроведуваат вработени административни службеници во Агенцијата (во натамошниот текст: обучувачи) определени од страна на директорот на Агенцијата.

Член 3

(1) Барањето за обука за заштита на личните податоци, контролорот, обработувачот, односно офицерот за заштита на личните податоци може да го поднесе:

- во писмена форма по пошта;
- на електронската пошта obuki@privacy.mk; или
- во писарницата на Агенцијата.

(2) Барањето за обука за заштитата на личните податоци ги содржи особено следните податоци:

- назив и седиште, односно име и презиме и адреса на живеење на контролорот, обработувачот, односно офицерот за заштита на личните податоци;
- бројот на учесниците што се пријавуваат за обуката;
- име и презиме на пријавените учесници за обуката и работно место;
- видовите на обука и модулите за обуката за која се пријавуваат учесниците;
- терминот на бараната обука;
- име и презиме на одговорното лице;
- телефон за контакт; и
- електронска пошта.

(3) По исклучок од ставот (2) на овој член, контролорот, односно обработувачот, податоците за учесниците може да ги достави и дополнително, но најдоцна до денот на отпочнување на обуката.

(4) Доколку контролорот, обработувачот, односно офицерот за заштита на личните податоци сака да присуствува на посебни обуки според барана програма, во барањето за обука за заштитата на личните податоци наместо модулите ги наведува темите, односно прашањата што бара да бидат предмет на обуката.

(5) Секое добиено барање за обука за заштита на личните податоци во Агенцијата се заведува во писарницата и се доставува до обучувачите.

(6) Образецот на барањето за обука за заштита на личните податоци е составен дел на овој правилник (Образец бр. 1).

Член 4

(1) Агенцијата ги евидентира податоците за пријавените контролори, обработувачи, односно офицери за заштита на личните податоци и го следи бројот на пријавени учесници за секој од модулите на обуките наведени во Годишната програма.

(2) Доколку контролорот, обработувачот, односно офицерот за заштита на личните податоци сака да присуствува на посебна обука според барана програма терминот за обуката договорно се утврдува.

(3) Контролорот, обработувачот, односно офицерот за заштита на личните податоци кој се пријавил за обука, најдоцна три работни дена пред одржувањето на обуката се известува за:

- терминот за одржување на обуката; и
- крајниот рок во кој треба да се уплати надоместокот за обуката.

(4) Известувањето од ставот (3) на овој член до контролорот, обработувачот, односно офицерот за заштита на личните податоци се доставува по електронски пат.

Член 5

Агенцијата за секој од модулите што се предмет на обука обезбедува презентација во електронска форма (медиум), како и канцелариски материјали за учество на обуката (прописи за заштитата на личните податоци, папка, хартија, пенкало и др.) кои на учесниците им се даваат пред отпочнување на обуката.

Член 6

(1) Уплатата на надоместокот за обуката се врши само преку трезорската сметка на Агенцијата. Правилно пополнетиот образец ПП-50 за плаќање на надоместокот за обуката се објавува на веб-страницата на Агенцијата.

(2) Контролорите, обработувачите, односно офицерите за заштита на личните податоци се должни да го извршат плаќањето на трошоците за обуката пред отпочнување на обуката за нивните пријавени учесници, но не подоцна од денот на одржување на обуката.

(3) Ако учесникот од било кои причини не присуствува на обуката и/или најмногу два пати го одложува присуството на обуката, Агенцијата определува нов термин за одржување на обуката.

(4) Во случаите од ставот (3) на овој член, доколку и на новиот термин учесникот не се појави на обуката, уплатените средства не се враќаат на контролорот, обработувачот, односно офицерот за заштита на личните податоци.

Член 7

(1) Агенцијата склучува договор за спроведување обука за заштита на личните податоци со контролорот, обработувачот, односно офицерот за заштита на личните податоци, а кои доставиле барање за спроведување на обука согласно Годишната програма.

(2) Образецот на Договорот за спроведување обука за заштита на личните податоци е составен дел на овој правилник (Образец бр. 2).

(3) По исклучок од ставот (1) на овој член, обуките за вработените во министерствата, органите на државната управа, управните организации и другите државни органи кои се целосни буџетски корисници, а кои доставиле барање за спроведување на обука согласно Годишната програма, се вршат без надомест, а по претходно склучен меморандум за соработка помеѓу Агенцијата и заинтересираниот контролор.

Член 8

(1) На обуката може да учествуваат само пријавените учесници за кои е уплатен надоместокот за обуката или кои биле ослободени од плаќањето на надоместокот.

(2) Доколку пријавениот учесник не се јави на определениот термин за одржување на обуката, истиот се вклучува во следните обуки што се одржуваат за истите модули.

(3) Пред отпочнување на обуката, секој учесник на обуката во евиденциониот лист за присуство ги внесува своите лични податоци (лично име) и своерачно се потпишува.

(4) Евиденциониот лист за присуство од ставот (3) на овој член ги содржи следните рубрики: реден број, контролор/обработувач, офицер за заштита на личните податоци, име и презиме, контакт телефон/електронска пошта и потпис. Во евиденциониот лист за присуство се внесува и датата и местото на одржување на обуката.

(5) Образецот на евиденциониот лист за присуство е составен дел на овој правилник (Образец бр. 3).

Член 9

(1) По завршување на обуката секој од учесниците анонимно пополнува прашалник за евалуација.

(2) Податоците од прашалникот за евалуација се користат само за анализи, извештаи, како и за унапредување на процесот за обука во Агенцијата.

(3) Образецот на прашалникот за евалуација е составен дел на овој правилник (Образец бр. 4).

III. ПРОГРАМА ЗА ОБУКА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 10

(1) Обуката за заштита на личните податоци се спроведува во согласност со:

- Програма за обука за заштита на личните податоци (Прилог бр. 1); и
- Програма за обука за офицерите за заштита на личните податоци (Прилог бр. 2).

(2) Програмите од ставот (1) на овој член се составен дел на овој правилник.

IV. ФОРМА И СОДРЖИНА НА ОБРАЗЕЦОТ ЗА СЕРТИФИКАТ

Член 11

(1) На секој учесник по завршувањето на обуката му се издава сертификат за учество на обука за заштита на личните податоци (во натамошниот текст: сертификат) од страна на директорот на Агенцијата.

(2) Во сертификатот се внесуваат податоци за: името и презимето на учесникот што учествувал на обуката, назив на контролорот, односно обработувачот, назив на обуката, место на одржување на обуката, период на важење на сертификатот, број и датум на сертификатот, место за печат и потпис на директорот на Агенцијата.

(3) Сертификатот се издава во случај ако учесникот присуствувал на генеричка обука и/или специјализирана обука.

(4) Сертификатот се издава и за учесниците на посебните обуки што се спроведуваат согласно Годишната програма.

(5) Образецот на сертификатот е составен дел на овој правилник (Образец бр. 5).

V. НАЧИН НА ВОДЕЊЕ НА ЕВИДЕНЦИЈА ЗА ИЗДАДЕНИ СЕРТИФИКАТИ

Член 12

(1) Евиденцијата за издадените сертификати ги содржи следните податоци:

- реден број;
- име и презиме на учесникот на обуката;
- назив и седиште, односно име и презиме и адреса на живеење на контролорот, обработувачот, односно офицерот за заштита на личните податоци;
- вид на обуката;
- место на одржување на обуката;
- датум и број на издадениот сертификат;
- датум и број на издадена потврда;
- контакт-телефон и електронска адреса; и
- забелешка.

(2) Образецот на евиденцијата за издадените сертификати е составен дел на овој правилник (Образец бр. 6).

(3) Евиденцијата од ставот (1) на овој член се води електронски согласно прописите за архивски материјал.

Член 13

(1) На барање на контролорот, обработувачот, односно офицерот за заштита на личните податоци или на учесникот на обуката, директорот на Агенцијата или од него овластено лице им издава Потврда за учество на обука за заштита на личните податоци.

(2) Во Потврдата за учество на обука за заштита на личните податоци се внесуваат податоци за: името и презимето на учесникот што учествувал на обуката, назив контролорот, односно обработувачот, место каде е одржана, датум на спроведување на обуката, по чие барање се издава потврдата и причини за издавање.

(3) Образецот на Потврдата за учество на обука за заштита на личните податоци е составен дел на овој правилник (Образец бр. 7).

VI. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 14

Со денот на влегувањето во сила на овој правилник престанува да важи Упатството за начинот на организирање и спроведување на обуки за контролори и обработувачи бр. 02-283/1 од 8.2.2012, бр. 02-283/2 од 7.3.2012, бр. 01-283/3 од 6.4.2012 и бр. 02-2852/1 од 20.12.2013 година.

Член 15

Овој правилник влегува во сила осмиот ден од денот на објавувањето во „Службен весник на Република Северна Македонија“.

Бр. 01-602/1
11 мај 2020 година
Скопје

Директор,
Imer Aliu, с.р.

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT

Агенција за заштита на личните податоци
Agjencia për Mbrojtjen e të Dhënave Personale

Образец бр. 1

БАРАЊЕ ЗА ОБУКА
за заштита на личните податоци

1. Назив и седиште, односно име и презиме и адреса на живеење на контролорот, обработувачот, односно офицерот за заштита на личните податоци
_____;
2. Број на учесници што се пријавуваат за обуката _____;
3. Име и презиме на пријавените учесници за обуката и работно место:
   1. _____;
   2. _____;
   3. _____;
   4. _____;
   5. _____
4. Видови на обуки[1] и модули за обуки за кои се пријавувате:
   1. Генерички[2] модул 1, 2, 3 ☐
   2. Генерички и специјализирани обуки – 1 модул ☐
   3. Генерички обуки модул 4 (офицер за заштита на личните податоци) ☐
   4. Посебни обуки ☐
      - на тема _____;
5. Термин за бараната обука – ваш предлог _____;
6. Име и презиме на одговорното лице _____;
7. Телефон за контакт _____;
8. Електронска пошта _____.

Барањето за обука може да се поднесе:
- на obuki@privacy.mk;
- во писмена форма по пошта; или
- во писарницата на Агенцијата за заштита на личните податоци.

Скопје _____._____.202__ М.П. _____ (Одговорно лице)

[1] Генерички; Специјализирани и Посебни обуки согласно Годишната програма за обука на контролори и обработувачи

[2] **Генерички обуки** – сите модули се задолжителни: Модул: 1 Правни основи (Законот за заштита на личните податоци и подзаконските акти) во домашното законодавство и право на Европската Унија; Модул: 2 Поимник (објаснување на поимите од Законот за заштита на личните податоци); Модул: 3 Обврски и одговорности на контролорот и обработувачот; и Модул: 4 Положба, статус и работи кои ги врши офицерот за заштита на лични податоци.

[3] **Специјализирани обуки**: Модул: 1 – Органи за спроведување на законот; Модул: 2 – Правосудство; Модул: 3 – Државна безбедност и одбрана; Модул: 4 – Здравство; Модул: 5 – Образование; Модул: 6 – Социјална заштита; Модул: 7 – Финансии; Модул: 8 – Комунални дејности и енергетика; Модул: 9 – Локална самоуправа; Модул: 10 – Работни односи; Модул: 11 – Индустрија и транспорт; Модул: 12 – Градежништво; Модул: 13 – Телекомуникации и пошти; Модул: 14 – Медиуми; Модул: 15 – Маркетинг; Модул: 16 – Трговија; Модул: 17 – Туризам и угостителство; Модул: 18 – Лотарија и игри на среќа; Модул: 19 – Здруженија на граѓани; Модул: 20 – Политички партии; Модул: 21 – Осигурување; Модул: 22 - Технички и организациски мерки за обезбедување на тајност и заштита на обработката на личните податоци (генерално и посебно според област); Модул: 23 – Видеонадзор; Модул: 24 – Биометриски податоци; Модул: 25 – Пренос на лични податоци; Модул: 26 – Обработка на посебни категории на лични податоци; и Модул: 27 – Вршење на внатрешна контрола; или Посебен модул 1, 2, 3, 4 и 5.

бул. „Гоце Делчев“ бр. 18, П. фах 417, 1000 Скопје
bul. Goce Delçev nr. 18, F. Postar 417, 1000 Shkup
тел./tel.: ++ 389 2 3230-635; www.dzlp.mk; e-mail: info@privacy.mk

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT

Агенција за заштита на личните податоци
Agjencia për Mbrojtjen e të Dhënave Personale

Образец бр. 2

Бр. ____-_____/____
_____._____.2020

ДОГОВОР

за спроведување обука за заштита на личните податоци

Склучен во Скопје, на ден ____.____.2020 година, помеѓу:

1. **Агенцијата за заштита на личните податоци**, со седиште во Скопје на бул. „Гоце Делчев“ бр. 18, застапувана од директорот Имер Алиу, во својство на давател на услугата за спроведување обука за заштита на личните податоци (во натамошниот текст: Давател на услугата), од една страна и

2. _____, со седиште во _____ на адреса _____, застапуван/а од _____, во својство на корисник на услугата за обука за заштита на личните податоци (во натамошниот текст: Корисник на услугата), од друга страна.

Член 1

Предмет на овој договор е спроведувањето обука за заштита на обработката на личните податоци (генерички и специјализиран модул), која ќе се одржи во просториите на Давателот на услугата, на ден ____.____.202__ година, во траење од 6 часа.

Член 2

Давателот на услугата, за спроведување обука за заштита на личните податоци, согласно Годишната програма за обуки на контролори и обработувачи, преку определените вработени лица за спроведување обуки за заштита на личните податоци, се обврзува договорената обука да ја реализира совесно и во согласност со барањето на Корисникот на услугата, со вклучување на компетентни експерти од Давателот на услугата.

По исклучок од ставот 1 на овој член, Давателот на услугата може да вклучи и надворешни експерти од земјата или странство.

Член 3

Давателот на услугата за спроведената обука го определува надоместокот според висината на трошоците, зависно од видот и модулот на обуката, согласно одредбите од Одлуката за определување на висината на надоместоците за организирање и спроведување на обука за заштита на личните податоци („Службен весник на Република Северна Македонија“ бр. 58/2020).

Член 4

Корисникот на услугата е должен да му го плати надоместокот на Давателот на услугата за спроведување на обуката: ___.000,00 денари за 1 (еден) пријавен учесник, односно вкупно ____._____,00 денари за ____ (_____) пријавени учесници.

бул. „Гоце Делчев“ бр. 18, П. фах 417, 1000 Скопје
bul. Goce Delçev nr. 18, F. Postar 417, 1000 Shkup
тел./tel.: ++ 389 2 3230-635; www.dzlp.mk; e-mail: info@privacy.mk

Надоместокот за обуката од став 1 на овој член се уплатува најдоцна до денот на одржувањето на обуката за која Корисникот на услугата се пријавил.

Средствата треба да се уплатат на Буџетот на РСМ на трезорската сметка со број 100-0000000630-95 која се води на НБРСМ, сметка на буџетски корисник број 0200660143-631-14 на Агенцијата за заштита на личните податоци, приходна шифра 723612, потпрограма 20.

Член 5

Во случај да настанат спорови во врска со реализацијата на овој договор, договорните страни се согласни да ги решат спогодбено.

Доколку не се постигне спогодбено решавање на спорот/вите, надлежен е Основниот граѓански суд Скопје.

Член 6

Овој договор влегува во сила со денот на потпишувањето.

Член 7

Овој Договор е составен во два истоветни примероци, од кои еден примерок за Давателот на услугата и еден примерок за Корисникот на услугата.

Давател на услугата,
Директор,
Imer Aliu

Корисник на услугата,

ЕВИДЕНЦИОНЕН ЛИСТ ЗА ПРИСУСТВО НА ОБУКА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

_____, ___.___.20___ година

Образец бр. 3

Ред. бр.	Контролор/обработувач, офицер за заштита на личните податоци	Име и презиме	Контакт-телефон Електронска пошта	Потпис
1.			_____ _____	
2.			_____ _____	
3.			_____ _____	
4.			_____ _____	
5.			_____ _____	
6.			_____ _____	
7.			_____ _____	
8.			_____ _____	
9.			_____ _____	
10.			_____ _____	

Обука за заштита на личните податоци
_____, ___.___.20___ година

Образец бр. 4

ПРАШАЛНИК ЗА ЕВАЛУАЦИЈА

Ред. бр.	Содржина на прашањето	Оценка				
I Евалуација за обуките						
1.	Која е Вашата оценка за организацијата на обуката?	1	2	3	4	5
2.	Колку обуката ги исполни предвидените цели?	1	2	3	4	5
3.	Колку обуката ги исполни вашите очекувања?	1	2	3	4	5
4.	Во која мера сте задоволни од методологијата на обуката?	1	2	3	4	5
5.	Колку сте задоволни со времетраењето на обуката?	1	2	3	4	5
6.	Колку сте задоволни од добиените материјали за обуката (презентации, прописи и др.)	1	2	3	4	5
7.	Колку сте задоволни од условите за одржување на обуката (сала, опрема, техничка поддршка)?	1	2	3	4	5
8.	Со која оценка ја оценувате можноста за поставување на прашања?	1	2	3	4	5
II Евалуација за обучувачите (име и презиме на обучувачот)						
1.	I	1	2	3	4	5
2.	II	1	2	3	4	5
3.	III	1	2	3	4	5
4.	IV	1	2	3	4	5
5.	V	1	2	3	4	5
6.	VI	1	2	3	4	5
III Евалуација за трансферот на знаења						
1.	Дали стекнатите знаења може да ги примените за подобрување на вашето работење?	да	не	делумно		
2.	Дали добиените материјали ќе ги доставите на вашите колеги?	да	не	делумно		
3.	Дали планирате да одржите презентација за стекнатото искуство пред вашите колеги ?	да, за _____ лица			не	
4.	Дали имате обврска за подготвување извештај од учеството на обуката	да	не			

Ваши дополнителни забелешки, коментари или предлози:

_____
_____
_____

Ви благодариме на соработката

Образец бр. 5

АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

Врз основа на член 69 став (5) од Законот за заштита на личните податоци, а во врска со член 11 од Правилникот за обука за заштита на личните податоци, директорот на Агенцијата за заштита на личните податоци

ИЗДАВА

СЕРТИФИКАТ

за учество на обука за заштита на личните податоци

На лицето _____ кое во својство на претставник на контролорот, односно обработувачот _____, учествуваше на обука за заштита на личните податоци _____

во_____

Овој сертификат е со важност од три години од денот на неговото издавање.

Бр. _____ М.П. Директор,

Дата _____ Imer Aliu

АГЕНЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

ЕВИДЕНЦИЈА ЗА СПРОВЕДЕНИ ОБУКИ

Образец бр. 6

Ред. бр.	Име и презиме на учесникот на обуката	Контролор, обработувач, односно офицер за заштита на личните податоци (назив и седиште, име и презиме и адреса на живеење)	Вид на обуката	Место на одржување на обуката	Датум и број на издадениот сертификат	Датум и број на издадена потврда	Контакт-телефон и електронска адреса	Забелешка
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
REPUBLIKA E MAQEDONISË SË VERIUT

Агенција за заштита на личните податоци
Agjencia për Mbrojtjen e të Dhënave Personale

Образец бр. 7

Бр. ____-_____/____
_____._____.202___

Врз основа на член 63 став (1) алинеја 8 од Законот за заштита на личните податоци, а во врска со член 13 од Правилникот за обука за заштита на личните податоци, Агенцијата за заштита на личните податоци издава

П О Т В Р Д А
за учество на обука за заштита на личните податоци

На лицето _____, кое во својство на претставник на контролорот, односно обработувачот _____ присуствуваше на обука за заштита на личните податоци во период од __ до __ на ден _____.20__ година, одржана во просториите на Агенцијата за заштита на личните податоци.

Потврдата се издава на барање на _____.

Потврдата се издава заради _____.

Директор,
Imer Aliu

бул. „Гоце Делчев“ бр. 18, П. фах 417, 1000 Скопје
bul. Goce Delçev nr. 18, F. Postar 417, 1000 Shkup
тел./tel.: ++ 389 2 3230-635; www.dzlp.mk; e-mail: info@privacy.mk

Прилог бр. 1

Програма за обука за заштита на личните податоци

Модул еден		
Име на модулот	**Преглед на правната рамка за заштита на личните податоци**	
Придобивка од учењето	Учесникот: • го разбира значењето на клучните поими дефинирани со Законот • подготвен е да ги почитува начелата за заштита на лични податоци и да ги примени во пракса, како и да ги запознае соработниците со нив преку внатрешни обуки • способен е да ја анализира усогласеноста на обработката на податоците со Законот • запознаен е со обврската на контролорт да демонстрира почитување на овие начела • детално е запознаен со статусот, надлежностите, задачите и овластувањата на Агенцијата • способен е да го застапува контролорот при вршење на надзор од страна на надзорниот орган • запознаен е со управните постапки што контролорот ги покренува пред надзорниот орган и со управните постапки што субјектот на лични податоци ги поведува пред надзорниот орган против контролорот	
Тема	**Што ќе опфати темата?**	**Материјал[1]**

• Општа регулатива за заштита на лични податоци на Европскиот парламент и Советот на ЕУ и нејзино транспонирање во новиот Закон за заштита на личните податоци	• Воведен краток осврт на:
	  • Европска конвенција за заштита на човековите права
	  • Конвенција 108/81 на Совет на Европа
	  • Конвенција 108/81+
	• Преглед на Општата регулатива за заштита на податоци
	• Закон за заштита на личните податоци
		• Европска конвенција за заштита на човековите права (ЕКЧП)
		• Судска практика во однос на член 8 од ЕКЧП (CASE OF TYRER v. THE UNITED KINGDOM, чување на податоци за приватниот живот CASE OF LEANDER v. SWEDEN, надзор и пресретнување на телефонска и писмена комуникација CASE OF KLASS AND OTHERS v. GERMANY, надзор на работно место Copland v. the United Kingdom, примена на CCTV (видеонадзор) Chamber judgment Peck v. United Kingdom, заштита на нечиј имиџ Grand Chamber judgments Springer and Von Hannover v. Germany - German и Von Hannover v. Germany, репутација PFEIFER v. AUSTRIA, NIEMIETZ v. GERMANY,
		Ограничување на правото да е утврдено со закон AMANN v. SWITZERLAND, ROTARU v. ROMANIA, ограничување во однос на легитимната цел PECK v. THE UNITED KINGDOM, мешањето во правото е неопходно во едно демократско општество LEANDER v. SWEDEN, позитивни обврски на државата K.U. v. FINLAND, поле на слободна проценка GARDEL v. FRANCE.
		• Конвенција 108/81 на Совет на Европа
		• Повелба на Европската унија за основните права
		Ограничување на повелбата
		• Општа регулатива за заштита на лични податоци (ОРЗЛП)
		• EC What does the General Data Protection Regulation (GDPR) govern?
		• Реформски пакет 2018
		• Закон за заштита на личните податоци
		• Мислења и препораки на Работната група 29
		• Мислења на Европскиот супервизор за заштита на личните податоци
		• ICO Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now
		• FRA Прирачник за европското законодавство за заштита на податоците
		• Protecting the right to respect for private and family life under the European Convention on Human Rights
		Судска практика – Европски суд за човекови права
		• ECHR Factsheet personal data protection (DNA information and fingerprints, GPS data, Health data, Interception of communications, phone tapping and secret surveillance, Monitoring of employees' computer use, Voice samples, Video surveillance, In the context of criminal justice, In the context of health, In social insurance proceedings, Storage in secret registers, Telecommunication service providers' data, Disclosure of personal data, Access to personal data, Erasure or destruction of personal data)

[1] Во програмата, во колоната „Материјал“, за Општата регулатива за заштита на лични податоци се користи кратенката ОРЗЛП.

		• ECHR Factsheet new technologies(Electronic data, E-mail, GPS (Global Positioning System), Internet, Telecommunications, Use of hidden cameras, Video surveillance)
Примена на законот	• Територијална примена на Законот • Исклучоци од примена на Законот	• Закон за заштита на личните податоци
Клучни поими и дефиниции	• Главни аспекти на поимот личен податок • Обработка на личните податоци • Контролор на лични податоци • Посебни категории на лични податоци • Нови поими и дефиниции • Анономизирани и псевдонимизирани податоци	• Закон за заштита на личните податоци • Судска практика обработка на личните податоци Bodil Lindqvist • Судска практика за опфатот на поимот личен податок AMANN v. SWITZERLAND, Volker und Markus Schecke GbR (C-92/09), Hartmut Eifert (C-93/09) • Судска практика: здравствени податоци Z v. FINLAND, • ICO Anonymization code • EC What is personal data? • EC Rules for business and organisations • WP29 Opinion 1/2010 on the concepts of "controller" and "processor" • WP29 Working Document on Genetic Data WP 91 • WP29 Working document on biometrics WP 80 • EDPS Guidelines concerning the processing of health data in the workplace by Community institutions and bodies
Начела за заштита на личните податоци и нивното значење	• „Законитост, правичност и транспарентност“ • „Ограничување на целите“ • „Минимален обем на податоци“ • „Точност“ • „Ограничување на рокот на чување“ • „Интегритет и доверливост“ • Демонстрирање усогласеност со начелата за заштита на личните податоци (отчетност)	• Закон за заштита на личните податоци • Судска практика: правична и транспарентна обработка на податоците HARALAMBIE v. ROMANIA, K.H. AND OTHERS v. SLOVAKIA, период на чување S. AND MARPER v. THE UNITED KINGDOM • Водич за ОРЗЛП • Отчетност ИКО • EDPS обука • ENISA Privacy, Accountability and Trust – Challenges and Opportunities • ENISA Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments • WP 29 Opinion 3/2010 on the principle of accountability WP 173 • EDPS Accountability on the ground: Provisional guidance on documenting processing operations for EU institutions, bodies and agencies Summary • EDPS Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments • EDPS Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation • WP 29 Guidelines on transparency under Regulation 2016/679 WP260
Агенција за заштита на лични податоци како надзорен орган	• Надлежности, задачи и овластувања ○ Супервизија над заштитата на личните податоци	• Закон за заштита на личните податоци • ОРЗЛП чл. 51, 52, 53, 54, 55, 57, 58 • EC What are Data Protection Authorities (DPAs)?

Модул два		
Име на модулот	**Комуникација на контролорот со субјектот на лични податоци**	
Придобивка од учењето	Учесникот: • ги познава правата на субјектот • способен е да води постапки и да одлучува за правата на субјектот на лични податоци • знае да процени како треба да биде формулирана секоја одделна согласност за обработка на лични податоци со јасно дефинирање на целта на обработката на личните податоци и обезбедување на лесен начин за нејзино повлекување • знае да даде конкретни насоки и работни инструкции на вработените кај контролорот кој што вршат директен маркетинг	
Тема	**Што ќе опфати темата?**	**Материјал**
Права на субјектите на лични податоци	• Информираност (транспарентност) • Пристап и исправка на личните податоци • Бришење („право да се биде заборавен“) • Ограничување на обработката на личните податоци • Преносливост на личните податоци • Право на приговор • Автоматска обработка на податоците (вклучително и профилирање)	• Закон за заштита на личните податоци • ОРЗЛП чл. 17, 20, 22 • Прашања и одговори поврзани со реформскиот пакет • Едукативно видео за правото на пристап до личните податоци • Образец на барање за пристап и исправка на личните податоци • Fact sheet EU Data Protection Reform: better data protection rights for European citizens • I-scoop Data subject rights and personal information: data subject rights under the GDPR • Matheson GDPR in Context: Data Subject Rights • ICO - Guide to the General Data Protection Regulation (GDPR) • Обрасци EU GDPR Academy Managing Data Subject Rights • ICO subject-access-request-checklist • ICO privacy-notices-transparency-and-control • EC Rights for citizens • ENISA The right to be forgotten - between expectations and practice • ICO Personal information online small business checklist • ICO Protecting personal data in online services: learning from the mistakes of others • WP 29 Guidelines on transparency under Regulation 2016/679 WP260 • WP 29 Guidelines on Consent under Regulation 2016/679 WP259 • EDPS Guidelines on the Rights of Individuals with regard to the Processing of Personal Data • ОРЗЛП- чл. 20 и рец. 68 • WP242 ANNEX –Frequently Asked Questions • WP29 WP 242 rev.01 Guidelines on the right to data portability • ОРЗЛП – чл. 22, рец.71, рец. 91 • Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling • WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 WP251 Судска практика – Европски суд за човекови права • ECHR Factsheet personal data protection (DNA information and fingerprints, GPS data, Health data, Interception of communications, phone tapping and secret surveillance, Monitoring of employees' computer use, Voice samples, Video surveillance, In the context of criminal justice, In the context of health, In social insurance proceedings, Storage in secret registers, Telecommunication service providers' data, Disclosure of personal data, Access to personal data, Erasure or destruction of personal data) • ECHR Factsheet new technologies(Electronic data, E-mail, GPS (Global Positioning System), Internet, Telecommunications, Use of hidden cameras, Video surveillance)

Услови за согласност	• Услови што треба да бидат исполнети за да се смета за валидна согласноста на субјектот за обработка на неговите лични податоци	• Закон за заштита на личните податоци Судска практика: • Согласност за обработка на здравствени податоци во поставка за вработување European Data Protection Supervisor, represented by M. V. Pérez Asinari and by H. Kranenborg, acting as Agents, intervener, v European Parliament, represented by K. Zejdová and S. Seyr, acting as Agents • Недостиг на согласност за медицински податоци L.L. v. FRANCE, RADU v. THE REPUBLIC OF MOLDOVA • Јавен интерес AVILKINA AND OTHERS v. RUSSIA • Fact sheet EU Data Protection Reform: better data protection rights for European citizens • I-sccop Data subject rights and personal information: data subject rights under the GDPR • Matheson GDPR in Context: Data Subject Rights • ICO - Guide to the General Data Protection Regulation (GDPR) Практични примери • Обрасци EU GDPR Academy Managing Data Subject Rights
Услови кои што се применуваат за согласност на дете во однос на услугите на информатичкото општество	• Користење на услугите на информатичкото општество од страна на децата е појава која што е застапена на глобално ниво. Во овој сегмент, неопходно е нормирање на обработката на личните податоци на децата.	• Закон за заштита на личните податоци • ОРЗЛП чл. 8 • ICO – Guide to the General Data Protection Regulation (GDPR) • Обрасци EU GDPR Academy Managing Data Subject Right • WP 29 Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) WP 160 • WP 29 Working Document 1/2008 on the protection of children's personal data (General guidelines and the special case of schools) WP 147

Модул три		
Име на модулот	**Информациска сигурност**	
Придобивка од учењето	Учесникот: • свесен е за значењето на техничките аспекти за безбедност на обработката на личните податоци • знае кои информации му се потребни за да ги идентификува операциите на обработка на лични податоци • способен е да препознае ризик при одредени операции на обработка на личните податоци • знае што е безбедносен инцидент • запознат е со обврската за известување за нарушување на безбедноста на личните податоци • способен е да напише правилник за технички и организациски мерки за сигурност и тајност при обработката на личните податоци • способен е да подготви Договор за обработка на лични податоци со вклучени одредби кои гарантираат дека обработувачот ќе преземе потребни технички и организациски мерки за заштита и тајност на личните податоци • способен е да оцени кои области треба да бидат предмет на внатрешна или надворешна ревизија/контрола, • способен е да настапи со свој совет при спроведување на „Data Protection Impact Assesment“ • го разбира концептот на Privacy by design & by default и способен е да дава совети за негова примена	
Тема	**Што ќе опфати темата?**	**Материјал**
Безбедност на обработката	• Технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • Едукативно видео за техничките и организациски мерки за заштита и тајност на личните податоци • ICO IT_security_practical_guide • UK GOV Cyber security guidance for business • HM Government Small businesses: What you need to know about cyber security • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • EDPS Guidance Security Measures for Personal Data Processing Article 22 of Regulation 45/2001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance Судска практика - Европски суд за човекови права • ECHR Factsheet personal data protection (DNA information and fingerprints, GPS data, Health data, Interception of communications, phone tapping and secret surveillance, Monitoring of employees' computer use, Voice samples, Video surveillance, In the context of criminal justice, In the context of health, In social insurance proceedings, Storage in secret registers, Telecommunication service providers' data, Disclosure of personal data, Access to personal data, Erasure or destruction of personal data) • ECHR Factsheet new technologies(Electronic data, E-mail, GPS (Global Positioning System), Internet, Telecommunications, Use of hidden cameras, Video surveillance)
Нивоа на техничките и организациски мерки за заштита и тајност на личните податоци и	• Воспоставување одговорност за средства кои се во сопственост на контролорот • Нивоа на техничките и организациски мерки за заштита и тајност на личните	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци

контроли	податоци треба да се применат во зависност од категориите на личните податоци кои се обработуваат • Воспоставување контроли соодветни за секое ниво на техничките и организациски мерки за заштита и тајност на личните податоци	• ICO IT security practical guide • UK GOV Cyber security guidance for business • HM Government Small businesses: What you need to know about cyber security • ENISA Handbook on Security of Personal Data Processing • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Безбедносни инциденти и Известување за нарушување на безбедноста на личните податоци	• Обврските за безбедност и тајност на личните податоци да се опфатени во описот на работното место и во договорот за работа • Да се следи почитувањето на овие обврски во процесот на оценување на вработените • Како и каде да се пријави инцидент-нарушување на безбедноста на личните податоци • Обрасци и постапка за известување на нарушувањето на безбедноста на личните податоци • Лекција која може да се научи од настанат инцидент • Санкции и дисциплински постапки кај контролорот поврзани со инциденти	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Recommendations for a methodology of the assessment of severity of personal data breaches • ENISA Recommendations for technical implementation of Art.4 • ENISA Data breach notifications in the EU • WP 29 Opinion 03/2014 on Personal Data Breach Notification WP 213 • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance • WP 29 Guidelines on Personal data breach notification under Regulation 2016/679
Безбедност и приватност за услуги кои се пренесуваат на обработувачи (аутсорсинг)	• Примена на техничките и организациски мерки за заштита и тајност на личните податоци и во случаи кога тие се обработуваат од страна на обработувачот • Обврската за примена на техничките и организациски мерки за обезбедување заштита и тајност на личните податоци помеѓу контролорот и обработувачот да се предвиди со Договор.	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • CNIL General Data Protection Regulation GUIDE FOR PROCESSORS SEPTEMBER 2017 EDITION • DPC Data security guidance
Физичка безбедност	• Процедури и механизми за физичка безбедност • Физичка контрола на влезовите • Обезбедување на канцеларии, простории и објектите • Работење во безбедна околина • Обезбедување на компјутерската опрема	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Безбедност и приватност на работното место	• Заштита на просториите каде се обработуваат личните податоци со цел да се спречи нивно откривање или модификација од страна на неовластени лица или кражба • Контроли што треба да бидат поставени за да се минимизира загубата или штетата	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing

	• Политиката за чисто биро и чист екран	• ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Оперативни постапки и одговорности	• Воспоставување на одговорности и постапки за управување и работи со сите компјутери и мрежи • Документирани оперативни процедури • Процедури за управување со инциденти • Сегрегација на должности	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Планирање и прифаќање на системот	• Заштита од злонамерен софтвер • Контроли против малициозен софтвер • Процедури за сомневање за малициозен код (како на пример со е-пошта) • Заштита од злонамерен софтвер при користење на сајтовите за социјално вмрежување, инстант пораки, текстуални пораки и други технологии • Процедури за откриен и потврден малициозен код	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Сигурносни копии и логови	• Процедури за правење сигурносни копии на податоци • Процедури за логирање на настани и грешки • Логови на администратори • Пријавување на грешки • Постапка за периодично тестирање на ефикасноста на сигурносните копии	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance • DPC Back-up systems
Сигурност на мрежа и контрола на приватноста	• Управување со безбедноста на компјутерските мрежи • Заштита на информациите и на придружната инфраструктура • Одржување на безбедноста на мрежата и контрола на приватноста • Тестирање на ефикасноста на безбедноста на мрежата и на приватност	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO Wi-Fi location analytics • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Управување и безбедност на	• Контрола и физичка заштита на компјутерските медиуми, документи,	• Законот за заштита на личните податоци

медиуми	влезните и излезните податоци за да се спречи кражба, оштетување на средствата и прекин на деловните активности • Управување со преносливи медиуми • Уништење на медиумите • Постапки за ракување со податоци • Безбедност на документацијата	• ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Давање и размена на информации	• Контрола на давањето и размената на податоци за да се спречи загуба, модификација или злоупотреба на податоци • Барање за користење или размена на податоци • Безбедност на медиумите кои се пренесуваат • Безбедност на електронските пораки • Други форми на размена на информации	• Закон за заштита на личните податоци • Правилник за безбедност на личните податоци • ICO data sharing code of practice • ICO Data sharing checklists • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Контрола на пристап на системи	• Контрола на пристапот до компјутерски услуги и податоци • Политики за дисеминација на податоците и информациите • Политика за контрола на пристап	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Управување со корисниците	• Процедури за контрола на правата на пристап до ИТ системите и услугите • Регистрација на корисниците • Управување со привилегии • Управување со корисничките лозинки • Преглед на правата на пристап на корисниците • Процедури за отстранување на неактивни корисници и корисници кои повеќе не се потребни	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • CNIL Deliberation no. 2017-012 of 19 January 2017 on the adoption of a recommendation relating to passwords • DPC Data security guidance
Следење на системот за пристап и користење	• Следење на системот ○ за да се обезбеди усогласеност со политиката за пристап ○ за откривање на неовластени активности ○ за да се утврди ефективноста на безбедносни мерки • Логирање на настани	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001

		• CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Криптирање на податоците	• Употреба на криптографски системи и техники за заштита на доверливоста, автентичноста или интегритетот на податоците и за заштита на информациите што се сметаат за ризични (посебни категории на личните податоци и ЕМБГ) • Дигитален потпис • Управување со клучеви	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Study on cryptographic protocols • ENISA Recommended cryptographic measures - Securing personal data • ENISA Algorithms, Key Sizes and Parameters Report - 2013 • ENISA Algorithms, key size and parameters report 2014 • ENISA The Use of Cryptographic Techniques in Europe • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • CNIL GUIDE SECURITY OF PERSONAL DATA • DPC Data security guidance
Алатки за приватност и безбедност на податоците (PETs - Технологии кои треба да ја подобрат приватноста)	• Криптирање • Систем за контрола на пристап • Печат за приватност на веб страниците • Дигитален потпис • Биометрија • Фаервол • Спам филтри • HTML филтри • Системи за псеводонимизација и анонимизиација	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA On the security, privacy and usability of online seals • ENISA Study on cryptographic protocols • ENISA Recommended cryptographic measures - Securing personal data • ENISA Algorithms, Key Sizes and Parameters Report - 2013 • ENISA Algorithms, key size and parameters report 2014 • ENISA The Use of Cryptographic Techniques in Europe • ENISA Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies • ENISA Privacy Enhancing Technologies: Evolution and State of the Art • ENISA PETs controls matrix - A systematic approach for assessing online and mobile privacy tools • ENISA Recommendations on European Data Protection Certification • ENISA Challenges of security certification in emerging ICT environments • ENISA Privacy and data protection in mobile applications • ENISA Privacy considerations of online behavioural tracking • ENISA Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments • WP29 Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC WP 90 • WP29 Opinion 1/2008 on data protection issues related to search engines WP 148 • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001
Технологии кои се опасни по приватност	• Cookies (Колачиња) • Лог фајлови • Спајвеар • Спам и фишинг	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • COOKIE SWEEP COMBINED ANALYSIS – REPORT

		• Working Document 02/2013 providing guidance on obtaining consent for cookies • Opinion 04/2012 on Cookie Consent Exemption • ICO Guide to the Privacy and Electronic Communications Regulations • Directive 2009/136/EC (ePrivacy Directive) • Factsheet – Stronger ePrivacy rules • Proposal for a Regulation on Privacy and Electronic Communications • Directive 2002/22/EC of the European Parliament and of the Council • ENISA Bittersweet cookies. Some security and privacy considerations • ENISA Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments • ENISA Smartphones: Information security risks, opportunities and recommendations for users • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001 • DPC Data security guidance
Социјален инженеринг	• Заеднички методи и цели на социјалниот инженеринг • Проверка на идентитетот на барателите • Признавање на можни напади на социјален инженеринг • Процедури за реагирање на потенцијални обиди за социјално инженерство	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • US-CERT Avoiding Social Engineering and Phishing Attacks • WEBROOT What is Social Engineering? • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001
Бришење на податоци	• Безбедно уништување на доверливите и посебните категории на лични податоци во хартиена форма • Неповратно бришење на податоците кои електронски се чуваат • Безбедно уништување на електронските медиуми за складирање на податоци	• Законот за заштита на личните податоци • ОРЗЛП чл. 32, рец. 75, 76, 77, 78, 79, 83 • Правилник за безбедност на личните податоци • ENISA Guidelines for SMEs on the security of personal data processing • ICO IT security practical guide • ISO/IEC 27001:2013(E) • Academy27001 Clause-by-clause explanation of ISO 27001
Проценка на влијанието на планираните операции на обработка на податоците врз заштитата на личните податоци „Data Protection Impact Assesment“	• Идентификување и разрешување на проблеми во раните фази на развој на нови системи и продукти, како и дефинирање на улогата на офицерот во овој процес – давање конкретни совети и следење дали истите се прифатени при неговото спроведување.	• ОРЗЛП чл. 35 • WP 29 WP 248 rev.01 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 • WP 29 Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (‘DPIA Template’) prepared by Expert Group 2 of the Commission’s Smart Grid Task Force WP209 • ICO PIA-Code-of-practice • Smart Grid Task Force 2012-14 - Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems • CNIL PRIVACY IMPACT ASSESSMENT (PIA) Methodology (how to carry out a PIA) • CNIL PRIVACY IMPACT ASSESSMENT (PIA) Tools (templates and knowledge bases) • CNIL Good practices MEASURES FOR THE PRIVACY RISK TREATMENT • CNIL INFOGRAFICS - DPIA • DPC Data Protection Impact Assessments (DPIA)
Privacy by design & by default	• Пренесување на главната порака до учесниците во однос на овој нов	• ОРЗЛП чл. 25

	концепт, а тоа е дека Privacy by design & by default се реализира преку техничките и организациски мерки, како компонента на "Data Protection Impact Assessment" • **Privacy by design** - примена на соодветни технички и организациски мерки при дизајнирање на системите во кои се врши обработка на лични податоци и при самата обработка на лични податоци, како што е псевдонимизацијата, сведувањето на минимален обем на податоците и вклучување на потребните заштитни мерки во процесот на обработка, со цел да се исполнат барањата од Закон и да се обезбеди заштита на правата на субјектите на личните податоци. • **Privacy by default** - примена на соодветни технички и организациски мерки со кои се обезбедува интегрирана обработка само на оние лични податоци кои се неопходни за конкретна цел на обработката, како и гаранција дека интегрираните лични податоци без индивидуална интервенција не се автоматски достапни за неограничен број на физички лица.	• Privacy by Design – Information & Privacy Commissioner of Ontario • ENISA Privacy and Data Protection by Design • ENISA Privacy by design in big data • ENISA Study on data collection and storage in the EU • ENISA Privacy Enhancing Technologies: Evolution and State of the Art • ENISA PETs controls matrix – A systematic approach for assessing online and mobile privacy tools • ENISA Online privacy tools for the general public • ENISA Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies

Модул четири		
Име на модулот	**Обврски и одговорности на контролорот**	
Придобивка од учењето	• запознаен е со постапката за водење на Евиденција за активностите на обработка на лични податоци и знае кои информации му се потребни за проверка на оваа евиденција • запознаен е со воспоставените механизми за сертификација на контролорите • има претстава кои елементи треба да ги содржат Кодексот на однесување и Задолжителните корпоративни правила за заштита на приватност • го разбира системот на прекршочни санкции на полето на заштитата на личните податоци	
Тема	**Што ќе опфати темата?**	**Материјал**
Евиденција на активностите на обработка	• Обврска на контролорот да води евиденција на операциите на обработка на лични податоци • Информации што ги содржи евиденцијата	• ОРЗЛП чл. 30, рец. 13
Кодекси на однесување	• Потреба од донесување на Кодекси на однесување, нивно одобрување од Агенцијата и мониторинг на одобрените кодекси	• ОРЗЛП чл. 40, 41
Сертификација	• Услови и начин на сертификација на контролорите за демонстрирање усогласеност со Законот • Сертификациони тела	• ОРЗЛП чл. 42, 43 • ENISA Recommendations on European Data Protection Certification • ENISA Challenges of security certification in emerging ICT environments • ENISA Security certification practice in the EU – Information Security Management Systems - A case study • Законот за заштита на личните податоци • Упатство за начинот на вршење на надворешна контрола 1, 2, 3
Задолжителни корпоративни правила	• Задолжителните корпоративни правила кои се почитуваат од страна на контролорот при пренос на лични податоци во трети земји во рамките на група на друштва (поврзани друштва) или група на правни лица кои вршат заедничка економска дејност	• WP 29 Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules WP 155 rev.04 • WP 29 Working Document Setting up a framework for the structure of Binding Corporate Rules WP 154 • WP 29 Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents WP 212 • WP 29 Explanatory Document on the Processor Binding Corporate Rules WP 204 rev.01 • WP 29 Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules WP 256 • WP 29 Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules WP 257
Прекршоци за постапување спротивно на одредбите на Закон	• Прекршоците, одмерувањето на глоба, надлежност за водење на прекршочна постапка и судската заштита во прекршочната постапка	• WP29 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679

Модул пет		
Име на модулот	**Пренос на лични податоци**	
Придобивка од учењето	Учесникот: • Запознаен е со основните претпоставки и постапката за пренос на лични податоци	
Тема	**Што ќе опфати темата?**	**Материјал**
• Општо начело за пренос	• Услови за пренос во земји членки на ЕУ и ЕЕП • Услови за пренос во трети земји	• Законот за заштита на личните податоци • ОЗЛП чл. 44, 45, 46, 47 • Decision (EU) 2016/1250 • Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decisio • WP 29 Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor) WP 161 • EU-U.S. Privacy Shield: Frequently Asked Questions • EC GUIDE TO THE EU-U.S. PRIVACY SHIELD • WP29 Adequacy Referential (updated) WP 254 • DPC Cross-border processing and the one stop shop • OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data • OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 2013 • THE OECD PRIVACY FRAMEWORK
• Пренос врз основа на одлука за соодветност	• Елементи врз основа на кои се врши оценка на степенот на соодветност на заштита на личните податоци • Пренос на лични податоци врз основа на одлука за соодветност	• Decision (EU) 2016/1250 • Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decisio • WP 29 Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor) WP 161 • EU-U.S. Privacy Shield: Frequently Asked Questions • EC GUIDE TO THE EU-U.S. PRIVACY SHIELD • WP29 Adequacy Referential (updated) WP 254 • DPC Cross-border processing and the one stop shop
• Пренос кој подлежи на соодветни заштитни мерки	• Соодветни заштитни мерки што треба да се обезбедат за да се изврши пренос на лични податоци без одлука за соодветност.	• Decision (EU) 2016/1250 • Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decisio • WP 29 Opinion 3/2009 on the Draft Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor) WP 161 • EU-U.S. Privacy Shield: Frequently Asked Questions • EC GUIDE TO THE EU-U.S. PRIVACY SHIELD • WP29 Adequacy Referential (updated) WP 254 • DPC Cross-border processing and the one stop shop

Модул шест		
Име на модулот	**Видеонадзор**	
Придобивка од учењето	Учесникот: • Запознаен е со условите под кои може да се врши обработка на личните податоци преку систем за вршење на видеонадзор	
Тема	**Што ќе опфати темата?**	**Материјал**
Видеонадзор	• Целите заради кои може да се врши обработка на лични податоци преку системот за вршење видеонадзор • Обврски на контролорот при поставување на систем за вршење на видеонадзор	• Законот за заштита на личните податоци • Правилник за видеонадзор • Судска практика: Снимки од домашен видеонадзор во František Ryneš • Видеонадзор од страна на полиција • Видеонадзор и судска практика PECK v. THE UNITED KINGDOM, • Nevenka ANTOVIĆ and Jovan MIRKOVIĆ against Montenegro • Working Document on the Processing of Personal Data by means of Video Surveillance • Opinion 4/2004 • The EDPS video-surveillance guidelines • Едукативно видео за видеонадзор • Едукативно видео за правото на пристап до личните податоци • ICO CCTV Code of practice (In the picture: A data protection code of practice for surveillance cameras and personal information • WP29 Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance WP 89 • DPC Data Protection and CCTV Судска практика – Европски суд за човекови права • ECHR Factsheet personal data protection (DNA information and fingerprints, GPS data, Health data, Interception of communications, phone tapping and secret surveillance, Monitoring of employees' computer use, Voice samples, Video surveillance, In the context of criminal justice, In the context of health, In social insurance proceedings, Storage in secret registers, Telecommunication service providers' data, Disclosure of personal data, Access to personal data, Erasure or destruction of personal data) • ECHR Factsheet new technologies(Electronic data, E-mail, GPS (Global Positioning System), Internet, Telecommunications, Use of hidden cameras, Video surveillance)
Барање за утврдување повреда на правото на заштита на личните податоци преку вршење на видеонадзор	• Специфики на Барањето • Постапување по истото	• Образец на барање • Е-пријава

Модул седум		
Име на модулот	**Улогата на офицерот за заштита на личните податоци – „Размислувај и постапувај како офицер“**	
Придобивка од учењето	Учесникот: • запознаен е со новата положба што треба да ја има кај контролорот • способен е да го информира, советува и да му дава соодветни препораки на контролорот • способен е самостојно да ја организира работата и да ги извршува задачите пропишани со Закон • способен е да организира и спроведе обука за вработените и менаџерите, како и да процени каков вид на обука да се обезбеди и на кои операции на обработка да посвети најмногу време и ресурси • стекнува поголемо искуство, пракса и вештини за вршење на оваа функција односно го продлабочува стекнатото искуство	
Тема	**Што ќе опфати темата?**	**Материјал**
Критериуми за определување на офицер	Оваа тема ги опфаќа персоналните и професионалните квалитети што треба да ги исполнува офицерот во согласност со Закон	• Законот за заштита на личните податоци • Прирачник за офицерите за заштита на личните податоци • WP 29 WP 243 rev.01 Guidelines on Data Protection Officers ('DPOs') • EDPS Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 • EDPS The DPO at work • EDPS What the decision appointing a DPO should contain • EDPS Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8) • EDSP WP243 ANNEX – FREQUENTLY ASKED QUESTIONS • Едукативно видео за офицерите за заштита на личните податоци • Обрасци
Положба и статус на офицерот (гарантирање на независност)	Оваа тема е срцето на модулот, заради што треба да и се посвети особено внимание. • Темата ги опфаќа сите важни аспекти врз основа на кои се гарантира независната положба на офицерот.	• Законот за заштита на личните податоци • Прирачник за офицерите за заштита на личните податоци • WP 29 WP 243 rev.01 Guidelines on Data Protection Officers ('DPOs') • EDPS Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 • EDPS The DPO at work • EDPS What the decision appointing a DPO should contain • EDPS Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8) • EDSP WP243 ANNEX – FREQUENTLY ASKED QUESTIONS • Едукативно видео за офицерите за заштита на личните податоци • Обрасци
Работи што ги врши офицерот согласно новиот Закон	Оваа тема е исто така клучна за сите учесници во обуката. • Детален опис на работите односно задачите што ги врши офицерот согласно Закон	• Законот за заштита на личните податоци • Прирачник за офицерите за заштита на личните податоци • WP 29 WP 243 rev.01 Guidelines on Data Protection Officers ('DPOs') • EDPS Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 • EDPS The DPO at work • EDPS What the decision appointing a DPO should contain • EDPS Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (Article 24.8) • EDSP WP243 ANNEX – FREQUENTLY ASKED QUESTIONS • Едукативно видео за офицерите за заштита на личните податоци • Обрасци • Е-пријава
„Размислувај и постапувај како офицер“ • Организирање на работата • Управна и судска пракса во областа на заштитата на личните	Организирање на работата од страна на офицерот • Да се даде одговор на прашањата: ○ Како да се зајакне функцијата на офицерот? ○ Како да се организира работата на офицерот за да биде поефикасен? Обучувачите да ги упатат на редовна посета на Катчето за офицери на интернет страницата на ДЗЛП, накратко да ги запознаат и со обрасците наменети за офицерите, но и да им препорачаат да ги користат алатките е-форум и е-конференција. • Анализа на управна и судска пракса во областа на заштитата на личните податоци	• Законот за заштита на личните податоци • Прирачник за офицерите за заштита на личните податоци • WP 29 WP 243 rev.01 Guidelines on Data Protection Officers ('DPOs') • EDPS Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 • EDPS The DPO at work • EDPS What the decision appointing a DPO should contain • EDPS Implementing rules concerning the tasks, duties and powers of the Data Protection Officer (cArticle 24.8) • EDSP WP243 ANNEX – FREQUENTLY ASKED QUESTIONS • Едукативно видео за офицерите за заштита на личните податоци • Обрасци • Е-форум • Е-пријава • Е-конференции • Катче за офицери Судска практика - Европски суд за човекови права • ECHR Factsheet personal data protection (DNA information and fingerprints, GPS data, Health data, Interception of communications, phone tapping and secret surveillance, Monitoring of employees' computer use, Voice samples, Video surveillance, In the context of criminal justice, In the context of health, In social insurance proceedings, Storage in secret registers, Telecommunication service providers' data, Disclosure of personal data, Access to personal data, Erasure or destruction of personal data) • ECHR Factsheet new technologies(Electronic data, E-mail, GPS (Global Positioning System), Internet, Telecommunications, Use of hidden cameras, Video surveillance)

Прилог бр. 2

Програма за обука за офицерите за заштита на лични податоци

Број	Модул	Придобивка од обуката	Теми
1	**Преглед на правната рамка за заштита на личните податоци**	Учесникот: • го разбира значењето на клучните поими дефинирани со Законот • подготвен е да ги почитува начелата за заштита на лични податоци и да ги примени во пракса, како и да ги запознае соработниците со нив преку внатрешни обуки • способен е да ја анализира усогласеноста на обработката на податоците со Законот • запознаен е дека контролорот има обврска да демонстрира почитување на овие начела • детално е запознаен со статусот, надлежностите, задачите и овластувањата на Агенцијата • способен е да го застапува контролорот при вршење на надзор од страна на надзорниот орган • запознаен е со управните постапки што контролорот ги покренува пред надзорниот орган и со управните постапки што субјектот на лични податоци ги поведува пред надзорниот орган против контролорот	Општа регулатива за заштита на лични податоци на Европскиот парламент и Советот на ЕУ и нејзино транспонирање во новиот Закон за заштита на личните податоци
			Примена на Законот
			Клучни поими и дефиниции
			Начела за заштита на личните податоци и нивното значење
			Агенција за заштита на лични податоци како надзорен орган • Надлежности, задачи и овластувања ○ Супервизија
2	**Комуникација на контролорот со субјектот на лични податоци**	Учесникот: • ги познава правата на субјектот • способен е да води постапки и да одлучува за правата на субјектот на лични податоци • знае да процени како треба да биде формулирана секоја одделна согласност за обработка на лични податоци со јасно дефинирање на целта на обработката на личните податоци и обезбедување на лесен начин за нејзино повлекување • знае да даде конкретни насоки и работни инструкции на вработените кај контролорот кој што вршат директен маркетинг	Права на субјектите
			Услови за согласност
			Услови кои што се применуваат за согласност на дете во однос на услугите на информатичкото општество
3	**Информациска сигурност**	Учесникот: • свесен е за значењето на техничките аспекти за безбедност на обработката на личните податоци • знае кои информации му се потребни за да ги идентификува операциите на обработка на лични податоци • способен е да препознае ризик при одредени операции на обработка на личните податоци • знае што е безбедносен инцидент • запознат е со обврската за известување за нарушување на безбедноста на личните податоци • способен е да напише правилник за технички и организациски мерки за сигурност и тајност при обработката на личните податоци • способен е да подготви Договор за	Безбедност на обработката (Технички и организациски мерки за обезбедување заштита и тајност на обработката на личните податоци)
			Нивоа на техничките и организациски мерки за заштита и тајност на личните податоци и контроли
			Безбедносни инциденти и известување за нарушување на безбедноста на личните податоци
			Безбедност и приватност за услуги кои се пренесуваат на обработувачи (аутсорсинг)
			Физичка безбедност
			Безбедност и приватност на работното место
			Оперативни постапки и одговорности

		• обработка на лични податоци со вклучени одредби кои гарантираат дека обработувачот ќе преземе потребни технички и организациски мерки за заштита и тајност на личните податоци • способен е да оцени кои области треба да бидат предмет на внатрешна или надворешна ревизија/контрола, • способен е да настапи со свој совет при спроведување на „Data Protection Impact Assesment“ • го разбира концептот на Privacy by design & by default и способен е да дава совети за негова примена	Планирање и прифаќање на системот
			Сигурносни копии и логови
			Сигурност на мрежа и контрола на приватноста
			Управување и безбедност на медиуми
			Давање и размена на информации
			Контрола на пристап на системи
			Управување со корисниците
			Следење на системот за пристап и користење
			Криптирање на податоците
			Алатки за приватност и безбедност на податоците
			Технологии кои се опасни по приватност
			Социјален инженеринг
			Бришење на податоци
			Проценка на влијанието на планираните операции на обработка на податоците врз заштитата на личните податоци “Data Protection Impact Assesment”
			Privacy by design & by default
4	**Обврски и одговорности на контролорот**	Учесникот: • запознаен е со постапката за водење на Евиденција за активностите на обработка на лични податоци и знае кои информации му се потребни за проверка на оваа евиденција • запознаен е со воспоставените механизми за сертификација на контролорите • има претстава кои елементи треба да ги содржат Кодексот на однесување и Задолжителните корпоративни правила за заштита на приватност • го разбира системот на прекршочни санкции на полето на заштитата на личните податоци	Евиденција на активностите на обработка
			Кодекси на однесување
			Сертификација
			Задолжителни корпоративни правила за заштита на приватност
			Прекршоци за постапување спротивно на одредбите на Законот
5	**Пренос на лични податоци**	Учесникот: • запознаен е со основните претпоставки и постапката за пренос на лични податоци	Општо начело за пренос
			Пренос врз основа на одлука за соодветност
			Пренос кој подлежи на соодветни заштитни мерки
6	**Видеонадзор**	Учесникот: • запознаен е со условите под кои може да се врши обработка на личните податоци преку систем за вршење на видеонадзор	Видеонадзор
			Барање за утврдување повреда на правото на заштита на личните податоци преку вршење на видеонадзор

7	**Улогата на офицерот за заштита на личните податоци** - **„Размислувај и постапувај како офицер“**	Учесникот: • запознаен е со новата положба што треба да ја има кај контролорот • способен е да го информира, советува и да му дава соодветни препораки на контролорот • способен е самостојно да ја организира работата и да ги извршува задачите пропишани со Закон • способен е да организира и спроведе обука за вработените и менаџерите, како и да процени каков вид на обука да се обезбеди и на кои операции на обработка да посвети најмногу време и ресурси • стекнува поголемо искуство, пракса и вештини за вршење на оваа функција односно го продлабочува стекнатото искуство	Критериуми за определување на офицер (професионални и персонални квалитети)
			Положба и статус на офицерот (гарантирање на независност)
			Работи што ги врши офицерот согласно Законот
			„Размислувај и постапувај како офицер“: • читање и анализирање на управна и судска пракса во Македонија, но и меѓународна пракса – одлуки на Судот на правдата на ЕУ и Европскиот суд за човекови права • студија на случаи • вежби • споделување на индивидуални искуства • организирање на работата од страна на офицерот