20101583365

ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ

Врз основа на член 23 став 5 од Законот за заштита на личните податоци („Службен весник на Република Македонија“ бр. 7/05, 103/08 и 124/10), директорот на Дирекцијата за заштита на личните податоци донесе

П Р А В И Л Н И К
ЗА ИЗМЕНУВАЊЕ И ДОПОЛНУВАЊЕ НА ПРАВИЛНИКОТ ЗА ТЕХНИЧКИТЕ И ОРГАНИЗАЦИСКИТЕ МЕРКИ ЗА ОБЕЗБЕДУВАЊЕ ТАЈНОСТ И ЗАШТИТА НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Член 1

Во Правилникот за техничките и организациските мерки за обезбедување тајност и заштита на обработката на личните податоци („Службен весник на Република Македонија“ бр.38/09) во членот 2 во точката 3 зборовите „телекомуникациска мрежа“ се заменуваат се зборовите „електронско комуникациска мрежа“.

Во точката 6 по зборовите „со кој“ се додаваат зборовите „може да“. Во точката 10 зборот „збир“ се заменува со зборот „множество“. Точката 12 се менува и гласи:

„12. Офицер за заштита на личните податоци е лице овластено од контролорот за самостојно и независно вршење на работите во смисла на член 26-а од Законот за заштита на личните податоци“.

Член 2

Во членот 3 по ставот (1) се додава нов став (2) кој гласи:

„Одредбите од членот 25 на овој правилник соодветно се применуваат и при проверката на постапувањето на обработувачот при обработката на личните податоци во смисла на член 26 став 3 од Законот за заштита на личните податоци.“

Член 3

Во членот 4 во алинејата 2 по зборот „друга“ се додава зборот„рачна“.

Член 4

Во член 6 ставот (5) се менува и гласи:

„(5) За документите кои се пренесуваат преку електронско комуникациска мрежа, а содржат посебни категории на лични податоци и/или матичен број на граѓанинот задолжително се применуваат технички и организациски мерки кои се класифицирани на основно, средно и високо ниво.“

Член 5

По членот 9 се додава нов наслов и нов член 9-а кои гласат:

„Пренос на лични податоци во други држави“

Член 9-а

Во случај на хардверско и/или софтверско одржување или на други активности на информацискиот систем може да се врши пренос на лични податоци во други држави само согласно условите утврдени во прописите за заштита на личните податоци“.

Член 6

Во членот 10 став (2) во алинејата 3 зборот „корисниците“ се заменува со зборовите „администраторот на информацискиот систем и на овластените лица“.

Во ставот (3) зборовите „организационата поставеност на“ се бришат.

Член 7

Во членот 11 во точката 2 зборовите „секој корисник“ се заменуваат со зборовите „секое овластено лице“.

Член 8

Во членот 12 во ставот (2) зборовите „секој корисник“ се заменуваат со зборовите „секое овластено лице“.

Член 9

Во членот 13 во ставот (2) зборовите „овластени лица“ се заменуваат со зборовите „лица посебно овластени“.

Во ставот (3) зборовите „овластено лице“ се заменуваат со зборот „лицето“.

По ставот (4) се додаваат два нови става (5) и (6) кои гласат:

„(5) По исклучок од ставот (1) на овој член, серверите на кои се инсталирани софтверски програми за обработка на личните податоци, можат да бидат физички лоцирани, хостирани и администрирани надвор од просториите на контролорот.

(6) Во случајот од ставот (5) на овој член, меѓусебните права и обврски на контролорот и правното, односно физичкото лице кај кое се физички лоцирани, хостирани и администрирани серверите, треба да бидат уредени со договор во писмена форма, кој задолжително ќе содржи технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци.“

Член 10

Во членот 14 по ставот (6) се додава нов став (7) кој гласи:

„(7) Контролорот задолжително врши континуирано информирање на овластените лица за непосредните обврски и одговорности за заштита на личните податоци“.

Член 11

По членот 14 се додава нов наслов и нов член 14-а кои гласат:

„Обврски и одговорности на администраторот на информацискиот систем

Член 14-а

(1) Обврските и одговорностите на администраторот на информацискиот систем, контролорот ги дефинира и утврдува во Правилата за определување на обврските и одговорностите на администраторот на информацискиот систем и на овластените лица при користење на документите и информатичко комуникациската опрема.

(2) Контролорот задолжително врши периодична контрола над работата на администраторот на информацискиот систем и изработува извештај за извршената контрола.

(3) Во извештајот од ставот (2) на овој член треба да се содржани констатираните неправилности и предложените мерки за отстранување на тие неправилности“.

Член 12

Во членот 15 во ставот (1) зборовите „секој кориник кој“ се заменуваат со зборовите „секое овластено лице кое“, а зборот „корисниците“ се заменува со зборовите „администраторот на информацискиот систем и на овластените лица“.

Член 13

Во членот 18 во ставот (3) зборовите „секој корисник“ се заменуваат со зборовите „секое овластено лице“.

Член 14

Во членот 19 во ставот (1) зборовите „овластените корисници„ се заменуваат со зборовите „овластените лица“.

Член 15

Во членот 20 во ставот (4) по зборот „член“ се додава зборот „комисиски“.

Член 16

Во членот 21 ставот (3) се менува и гласи:

„(3) Сигурносни копии задолжително се прават секој работен ден и на крајот од работната седмица, а по потреба и секој последен работен ден во месецот.“

По ставот (3) се додаваат два нови става (4) и (5) кои гласат:

„(4) Сигурносните копии задолжително се прават на начин со кој ќе се гарантира постојана можност за реконструирање на личните податоци во состојба во која биле пред да бидат изгубени или уништени.

(5) Контролорот задолжително ја проверува функционалноста на сигурносните копии за вршење на реконструкција на личните податоци согласно ставот (4) на овој член“.

Член 17

Членот 22 се менува и гласи:

„Сигурносните копии се чуваат надвор од просторијата во која се наоѓаат серверите и треба да се физички и криптографски заштитени, заради оневозможување на каква било модификација.“

Член 18

Во членот 23 зборовите „за овластување на одговорно лице за заштита на личните податоци,“ се бришат.

Член 19

Насловот пред членот 24 и членот 24 се бришат.

Член 20

Во членот 25 во ставот (3) по зборот „трето“ се додава зборот „правно“.

Во ставот (6) зборовите „одговорното лице“ се заменува со зборот „офицерот“. По ставот (7) се додава нов став (8) кој гласи:

„(8) Образецот на извештајот од ставот (4) на овој член е составен дел на овој правилник.“

Член 21

Во членот 26 зборовите „секој корисник кој пристапил“ се заменуваат со зборовите „секое овластено лице кое пристапило“, а зборовите „секој корисник“ се заменуваат со зборовите „секое овластено лице“.

Член 22

Во членот 27 во ставот (3) зборовите „одговорното лице“ се заменуваат со зборот „офицерот“.

Во ставот (4) зборот „десет“ се заменува со зборот „пет“.

Во ставот (5) зборовите „Одговорното лице“ се заменуваат со зборовите „Офицерот“.

Член 23

Членот 31 се менува и гласи:

„(1)Сигурносните копии задолжително се прават секој работен ден, на крајот од работната седмица и секој последен работен ден во месецот.

(2) Сигурносните копии се чуваат надвор од објектот во која се наоѓаат серверите или персоналните компјутери во кои се сместени збирките на лични податоци за кои се прави сигурносна копија.

(3) Сигурносните копии кои се чуваат на друга оддалечена локација од местото каде е сместен информацискиот систем треба да бидат обезбедени со соодветни технички и организациски мерки, согласно документацијата за технички и организациски мерки.

(4) Во случајот од ставот (3) на овој член, меѓусебните права и обврски на контролорот и правното, односно физичкото лице каде се чуваат сигурносните копии, треба да бидат уредени со договор во писмена форма, кој задолжително ќе содржи технички и организациски мерки за обезбедување тајност и заштита на обработката на личните податоци.“

Член 24

Во членот 32 во ставот (2) по зборот „трето“ се додава зборот „правно“.

Член 25

Во насловот пред членот 35 и во членот 35 зборовите „телекомуникациска мрежа“ се заменуваат со зборовите „електронско комуникациска мрежа“.

Член 26

По членот 35 се додава нова глава IV-а, девет нови наслови и девет нови члена 35-а, 35-б, 35-в, 35-г, 35-д, 35-ѓ, 35-е, 35-ж и 35-з кои гласат:

„Глава IV - а. Друга рачна обработка на личните податоци

1. Основно ниво на технички и организациски мерки

Примена

Член 35-а

Одредбите од членовите 3, 5, 6, 7, 10, 12, 14, 15 и 16 соодветно се применуваат и при друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел на збирка на лични податоци.

Пристап до документите

Член 35-б

(1) Пристапот до документите треба биде ограничен само за овластени лица на контролорот.

(2) За пристапувањето до документите задолжително треба да се воспостават механизми за идентификација на овластените лица и за категориите на личните податоци до кои се пристапува.

(3) Доколку е потребен пристап на друго лице до документите тогаш треба да бидат воспоставени соодветни процедури за таа цел во документацијата за техничките и организациските мерки.

Правило „чисто биро“

Член 35- в

Контролорот задолжително го применува правилото „чисто биро“ при обработката на личните податоци содржани во документите за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Чување на документи

Член 35-г

(1) Чувањето на документите треба да се врши на начин со што ќе се применат соодветни механизми за попречување на секое неовластено отворање.

(2) Кога физичките карактеристики на документите не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки кои што ќе го спречат секој неовластен пристап до документите.

(3) Ако документите не се чуваат заштитени на начин определен во ставовите (1) и (2) на овој член, тогаш контролорот треба да ги примени сите мерки за нивна заштита за време на целиот процес на обработка од пристап на неовластени лица.

Уништување на документи

Член 35-д

(1) Уништувањето на документите се врши со ситнење или со друг начин, при што истите повторно да не можат да бидат употребливи.

(2) Во случајот од ставот (1) на овој член комисиски се составува записник кој ги содржи сите податоци за целосна идентификација на документот како и за категориите на личните податоци содржани во истиот.

2. Средно ниво на технички и организациски мерки

Контрола

Член 35-ѓ

Одредбите од членовите 23 и 25 соодветно се применуваат и при друга рачна обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел на збирка на лични податоци.

Начин на чување на документите

Член 35-е

(1) Плакарите (орманите), картотеките или другата опрема за чување на документи задолжително треба да бидат сместени во простории заклучени со соодветни заштитни механизми. Просториите треба да бидат заклучени и за периодот кога документите не се обработуваат од овластените лица.

(2) Кога физичките карактеристики на просториите не дозволуваат примена на мерките од ставот (1) на овој член, контролорот треба да примени други мерки за да се спречи секој неовластен пристап до документите.

3. Високо ниво на технички и организациски мерки

Копирање или умножување на документите

Член 35-ж

(1) Копирањето или умножувањето на документите може да се врши единствено со контрола на овластени лица определени со претходно писмено овластување од страна на контролорот.

(2) Уништувањето на копиите или умножените документи треба да се изврши на начин што ќе оневозможи понатамошно обновување на содржаните лични податоци.

Пренесување на документи

Член 35-з

Во случај на физички пренос на документите контролорот задолжително презема мерки за нивна заштита од неовластен пристап или ракување со личните податоци содржани во документите кои е пренесуваат“.

Член 27

Во целиот текст на Правилникот зборот „корисникот“, „корисник“, односно „корисниците“ во било кој род и број се заменува со зборот „овластеното лице“, „овластено лице“, односно „овластените лица“.

Член 28

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

Бр. 02-1586/1
6 декември 2010 година
Скопје

Директор,
Димитар Ѓеорѓиевски, с.р.

Образец

Извештај од извршената _____ (внатрешна или надворешна) контрола на информацискиот систем и информатичката инфраструктура

1. **Назив и седиште/име и презиме и адреса на живеење на контролорот**

   .....

2. **Информации за збирката на лични податоци врз која е извршена контролата**

   .....

Назив на збирка/и на личните податоци	
Ниво на технички и организациски мерки:	
Начин на обработка на личните податоци:	

3. **Идентификација на контролата**

Датум на започнување:	
Датум на завршување:	
Спроведено од страна на (назив и седиште на правното лице кое врши надворешна контрола):	

4. **Резултати од контролата**

I. Целосно и делумно автоматизирана обработка на личните податоци

Ниво	Мерка на усогласеност	Степен на усогласеност	Констатирани недостатоци	Предложени корективни или дополнителни мерки за отстранување на констатираните недостатоци
Основно	Документација за технички и организациски мерки (член 10)			
Основно	Технички мерки (член 11)			
Основно	Организациски мерки (член 12)			
Основно	Физичка сигурност на информацискиот систем (член 13)			
Основно	Информирање за заштитата на личните податоци (член 14)			
Основно	Обврски и одговорности на администраторот на информацискиот систем (член 14-а)			
Основно	Обврски и одговорности на овластените лица (член 15)			
Основно	Евидентирање на инциденти (член 16)			
Основно	Идентификација и проверка, како и законска обработка на личните податоци (член 17)			
Основно	Контрола на пристап (член 18)			
Основно	Управување со медиуми (член 19)			

Основно	Уништување, бришење или чистење на медиумот (член 20)			
Основно	Сигурносни копии и повторно враќање на зачуваните лични податоци (член 21)			
Основно	Начин на чување на сигурносните копии (член 22)			
Средно	Дополнителни правила за технички и организациски мерки (член 23)			
Средно	Контрола на информацискиот систем и информатичката инфраструктура (член 25)			
Средно	Идентификација и проверка (член 26)			
Средно	Евидентирање на авторизираниот пристап и законска обработка на личните податоци (член 27)			
Средно	Контрола на физички пристап (член 28)			
Средно	Управување со медиуми (член 29)			
Средно	Евидентирање на инциденти (член 30)			
Средно	Сигурносни копии (член 31)			
Средно	Тестирање на информацискиот систем (член 32)			
Високо	Сертификациони постапки (член 33)			
Високо	Пренесување на медиуми (член 34)			
Високо	Пренесување на личните податоци преку електронско комуникациска мрежа (член 35)			

II. Друга рачна обработка на лични податоци што се дел од посебна збирка на лични податоци или се намети да бидат дел од збирка на лични податоци

Ниво	Мерка на усогласеност	Степен на усогласеност	Констатирани недостатоци	Предложени корективни или дополнителни мерки за отстранување на констатираните недостатоци
Основно	Документација за технички и организациски мерки (член 10)			
Основно	Организациски мерки (член 12)			
Основно	Информирање за заштитата на личните податоци (член 14)			
Основно	Обврски и одговорности на овластените лица (член 15)			
Основно	Евидентирање на инциденти (член 16)			
Основно	Пристап до документи и законска обработка на личните податоци (член 35-б)			
Основно	Правило „чисто биро“ (член 35-в)			
Основно	Чување на документи (член 35-г)			
Основно	Уништување на документи (член 35-д)			
Средно	Дополнителни правила за технички и организациски мерки (член 23)			
Средно	Контрола на информацискиот систем и информатичката инфраструктура (член 25)			
Средно	Начин на чување на документите (член 35-е)			
Високо	Копирање или умножување на документите (член 35 - ж)			
Високо	Пренесување на документи (член 35 - з)			

III. Податоци и факти врз основа на кои е изготвен извештајот и се предложени мерките за отстранување на констатираните недостатоци

➢ ➢

IV. Тим кој ја вршел контролата:

Име и презиме	Работно место	Потпис

V. Офицер за заштита на личните податоци кој го примил и ја потврдил содржината на извештајот (и)

Име и презиме	Потпис

VI. Одговорно лице, односно функционер на контролорот, кој е запознаен со содржината на извештајот

Име и презиме	Потпис

_____, _____, 20_____ година М.П.
(место) (датум)