



**Инструкция за техническите и организационни мерки за защита на личните
данни, събиращи, обработвани и съхранявани в регистрите и базите данни,
поддържани от ДПП «Шуменско плато»**

**Раздел I
Общи положения**

Чл. 1. С настоящата инструкция се определят:

1. реда и условията за събиране, обработване и съхраняване на личните данни в регистрите и базите данни, поддържани в ДПП «Шуменско плато» и реда за достъп до тях;

2. задълженията на длъжностните лица в ДПП «Шуменско плато», които работят с лични данни или имат достъп до такива;

3. необходимите технически и организационни мерки за защита на личните данни в ДПП «Шуменско плато» от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни).

Чл. 2. (1) ДПП «Шуменско плато» обработва само законно събрани лични данни, необходими за конкретни, точно определени и законни цели. Личните данни, които ДПП «Шуменско плато» събира и обработва следва да бъдат точни и при необходимост да се актуализират. Личните данни се заличават или коригират, когато се установи, че са неточни или несъответстващи на целите, за които се обработват.

(2). Обработването на лични данни в ДПП «Шуменско плато» се извършва когато:

1. това е необходимо за изпълнение на нормативно установлено задължение;
2. физическото лице, за което се отнасят данните е дало своето изрично съгласие;
3. физическото лице е подало заявление за извършване на административна услуга;
4. физическото лице е подало заявление за сключване на договор;
5. обработването е необходимо за изпълнението на задълженията по договор.

Чл. 3. Създаването и поддържането на регистрите и базите данни в ДПП «Шуменско плато», видът на личните данни, целите и средствата за обработване, както и получаването на данни от други институции са определени със Закона за горите, Закона за защита на личните данни, Кодекса на труда, Закона за държавния служител и други приложими нормативни актове.

Чл. 4. Поддържането на данните в регистрите и базите данни в ДПП «Шуменско плато» включва дейности, осигуряващи тяхното актуално състояние, точност, пълнота, взаимообвързаност, съхранение и пазене на хронология на промените в данните.

Чл. 5. (1) Въз основа на данните, съдържащи се в регистрите и базите данни, се представят административни услуги, свързани с дейността и функциите на ДПП «Шуменско плато», предоставяне и удостоверяване на информация, когато такава се изискват от други институции и организации, във връзка с тяхната компетентност и правомощия.

(2) Административните услуги по ал. 1 се предоставят при спазване разпоредбите на Закона за защита на личните данни, Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

Чл. 6. Личните данни в ДПП «Шуменско плато» се събират и обработват неавтоматизирано /хартиен носител/.

Раздел II

ОПИСАНИЕ НА ПОДДЪРЖАННИТЕ РЕГИСТРИ И БАЗИТЕ ДАННИ, ТЕХНОЛОГИЯ НА ОБРАБОТВАНЕ И СРОК ЗА СЪХРАНЕНИЕ

Чл. 7. ДПП «Шуменско плато» поддържа следните регистри и бази данни:

1. База данни „Управление на човешките ресурси“;
2. Регистър „Ведомости и заплати“;
3. Регистър „Деловодство“.

Чл.8(1). В база данни „Управление на човешките ресурси“, на основание Кодекса на труда, Закона за държавния служител и подзаконовите актове по прилагането им, се събират, обработват и съхраняват следните видове лични данни:

1. физическа идентичност – имена, ЕГН, адрес, телефон, данни от личната карта;
2. семеен положение- наличие на брак, развод, брой членове на семейството, в това число деца до 18 години;
3. образование – документ за придобито образование, квалификация, правоспособност;
4. трудова дейност – съгласно приложените документи за трудов стаж и професионална биография;
5. медицински данни – карта за предварителен медицински преглед за постъпване на работа, удостоверения за намалена работоспособност;
- 6 имотно и финансово състояние;
7. свидетелство за съдимост, когато се изисква;

(2) Личните данни в базата данни по ал.1 се събират при подаване на документи за постъпване на работа по трудово и служебно правоотношение на хартиен носител и по електронен път /защитен/ и периодично, когато нормативен акт изисква това.

(3) Събирането, обработването и съхранението на лични данни в базата данни се извършва от служител, съвместяващ длъжността „Човешки ресурси“ във връзка с възникване, изменение и прекратяване на трудовите и служебни правоотношения на служителите. Данните са на хартиен носител.

(4) Физическата защита на личните данни от регистъра е организирана, като данните се обработват и съхраняват в заключващи се помещения и има строг контрол на достъпа до тях.

(5). Достъп до информация от досиетата се предоставя на служители от ДПП «Шуменско плато» в нормативно установените случаи след подадена писмена заявка, писмено разрешение от директора на ДПП и при спазване на Закона за защита на личните данни.

(8). Срокът за съхранение на неполучените от работника/ служителя трудови книжки, дневниците и екземпляр от издадените удостоверения е 50 години.

Чл. 9. (1) В регистър „Ведомости и заплати“, на основание Закона за счетоводството, се съхраняват следните видове лични данни – трите имена, ЕГН, номер на лична карта, адрес, банкова сметка, данъчна служба по местоживееще, месечен доход.

(2)Личните данни се обработват и съхраняват във връзка с:
1. назначаване, изменение и прекратяване на служебното/трудовото правоотношение.
2. сключване на гражданска
3. при издаване на УП 2 и 3 /за пенсиониране и трудов стаж/ от физическите лица.

(3) Личните данни се обработват и съхраняват от старши счетоводителя на хартиен носител.

(4) Данните се обработват локално на компютър, разположен в работното помещение. Достъпът до операционната система се осъществява с индивидуална парола. Съхранението на данните е локално на твърдият диск на компютър. Използват се софтуерни продукти по обработка на данните относно възнагражденията на персонала, в това число основни и допълнителни възнаграждения, данъчни и други

задължения, трудов стаж, присъствени и неприсъствени дни и други подобни.

(5) Достъпът до личните данни в отдел „Счетоводство“ се осигурява в нормативно установените случаи и при спазване на Закона за защита на личните данни, след писмено разрешение от директора на ДГП.

(6) Лични данни от регистъра се предоставят електронно на Национална агенция по приходите и Националния осигурителен институт в съответствие с приложимата нормативна уредба.

(7) Срокът за съхранение на ведомостите за заплатите е 50 години;

Чл.10. (1) Регистър „Деловодство“ представлява хартиена база данни, формирана оформена в регистри.

(2) В деловодството на ДГП се съхраняват на хартиен носител всички изходящи писма, заповеди, договори и други, заедно с придружавашата ги документация, съдържащи лични данни.

(3) Физическата защита на личните данни в деловодството е организирана, като данните на хартиен носител са в заключващи се шкафове и помещения със строг контрол на достъпа до тях. Данните се обработват от служител, съвместяващ длъжността.

(2) Данните в преписките на хартиен носител се предоставят в нормативно установените случаи и при спазване на Закона за защита на личните данни.

(4). Срокът за съхранение на документите е 20 години.

Раздел III

Определяне на длъжностите, свързани с обработване и защита на лични данни, правата и задълженията им (лица, отговорни за защитата на личните данни)

Чл. 11. Директора на ДГП «Шуменско плато», със заповед определя лице по защита на личните данни и лица, което отговарят за въвеждането и поддържането на личните данни в регистрите и базите данни по чл. 7.

Чл. 12. Ръководството, организацията и контролът по прилагането на техническите и организационни мерки за защита на личните данни се осъществява от лицето по защита на личните данни.

Раздел IV

Форма на събиране, обработване и съхранение

Чл. 13 (1.) Събирането, обработването и съхранението на личните данни в регистрите и бази данни, поддържани в ДГП «Шуменско плато» се осъществява по следните начини:

1.На хартиен носител - съхраняват се в метална каса или механична картотека, в предвидените от нормативните актове за съответните видове документи срокове.

2.На технически носител- личните данни се въвеждат на твърд диск, на компютри и сървъри, със и без свързаност в локална мрежа и Интернет, но със защитен достъп до личните данни, който е непосредствен само от страна на операторите на лични данни, на лицата, действащи под тяхно или на администратора ръководство при обработване на лични данни. Персоналните компютри се намират в работни помещения на операторите лични данни. Паролата за достъп е индивидуална и може да се ползва само от операторът на лични данни, който я определя и периодично я сменя. Техническите носители се съхраняват в предвидените от нормативните актове, за съответните видове документи, срокове и в съответствие със сроковете за техническа годност. Техническите ресурси, прилагани за обработка на личните данни, включват персонални компютри, периферии устройства и мрежови ресурси. На електронен тип носител- файлове, съответно по видове - текстови, програмно-генериирани,

"електронна таблица".

3. Чрез глобалната мрежа (Интернет).

Раздел V

Технически и организационни мерки за защита на личните данни

Чл. 14. За гарантиране на поверителност, цялостност и наличност на личните данни в регистрите по чл. 7 при тяхното обработване се предприемат физическа, документална, персонална, криптографска защита и защита на информационната система и мрежи.

Чл. 15. Физическата защита на личните данни включва следните мерки.

1. лични данни могат да се обработват във всички работни помещения от служителя, който има достъп до тях съгласно длъжностна характеристика или заповед, както и от служител с контролиран достъп, който има разрешен достъп от обработващия данните или от Администратора, в случаите на отсъствие на титуляра;

2. за работните помещения се установява регламентиран достъп, когато не се използват от служители, работните помещения се заключват;

3. достъп на външни лица до работните помещения се разрешава само за изпълнение на служебни задачи; за времето на престой външното лице се придрожава от служител;

4. достъпът на външни лица до компютърните конфигурации е забранен и следва да бъде възпрепятстван;

5. компютърна техника се предоставя за ремонт без устройствата, на които се съхраняват данни;

6. осъществяване на контрол по отношение на обработващия данни във връзка със спазването на технологията за обработка на личните данни и технологията за изграждане на архивни копия се извършва от служителя по защита на личните данни в ДПП «Шуменско плато».

7. всички действия по актуализация на личните данни от служителите в ДПП «Шуменско плато» се извършват посредством работните компютърни конфигурации чрез приложен софтуер; работният процес на всяка работна компютърна конфигурация стартира след идентификация с потребителско име и парола.

Чл. 16. За документалната защита се предприемат следните мерки:

1.Достъп до личните данни в регистрите и базите данни, които се поддържа на хартиен носител имат само лицата, които ги обработват съгласно длъжностна характеристика или заповед.

2. Служители на ДПП «Шуменско плато», различни от посочените в т.1 могат да получат достъп до лични данни от регистрите за изпълнение на служебните си задължения след подадено писмено искане /Приложение № 1/, с посочване на информацията и целта за която се иска достъп и разрешение от директор на дирекцията, която отговаря за поддържането на съответния регистър или база данни.

3.Контрол на достъпа до регистъра се осъществява от непосредствения ръководител на лицето, което поддържа регистъра.

4.Сроковете за съхранение на регистрите са в съответствие с приложимата нормативна уредба и са посочени по-горе в инструкцията за всеки регистър и база данни по отделно.

5.Личните данни могат да бъдат размножавани и разпространявани от упълномощените служители само ако е необходимо за изпълнение на служебните им задължения или ако са изискани по надлежния ред от упълномощени лица.

6.Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер). След изтичане на срока за съхранение, тези документи се унищожават чрез нарязване, за което се съставя протокол от назначена със заповед на председателя комисия. Унищожаването се извършва след изрично писмено разрешение от директора на ДПП «Шуменско плато».

Чл.17. За персоналната защита на личните данни се предприемат следните мерки:

1. попълване на декларация от всеки служител в ДПП «Шуменско плато» за неразпространение на лични данни, станали известни при и по повод изпълнение на служебни задължения;
2. запознаване на служителите, които обработват лични данни с нормативната уредба в областта на защитата на личните данни и настоящата инструкция;
3. одобрен е план за реакция при възникване на събития, застрашаващи сигурността на данните, който се съхранява при служителя отговарящ за защита на личните данни в ДПП «Шуменско плато»;
4. забранява се споделянето на критична информация, като пароли за достъп, идентификатори и други между служителите; удостоверението за квалифициран електронен подпись не се преотстъпва или предава за ползване от други лица;
5. при възникване и установяване на инцидент веднага се докладва на лицето по защита на личните данни на ДПП «Шуменско плато»;

Чл. 18. За защита на информационната система и мрежи се предприемат следните мерки:

1. по отношение на регистрите и базите данни по чл. 7:
 - а) подсистемите за съхранение на данни са със защита срещу отпадане на някое от изграждащите ги устройства – постоянна памет;
 - б) непрекъсваемите токозахранващи устройства (UPS) са за цялото оборудване, необходимо за правилната работа на регистрите (компютърни конфигурации, сървъри и комуникационни средства);
2. сървърът за електронна поща сканира всички писма с антивирусен софтуер, за който е активирано автоматично обновяване на антивирусните дефиниции;
3. за всички сървърни и работни компютърни конфигурации се използват операционни системи и приложен софтуер, за който е осигурена поддръжка от производителя с обновления по отношение на сигурността;
4. на всяка работна компютърна конфигурация се осигурява антивирусен софтуер с включено автоматично обновяване и постоянно сканиране;
5. забранено е включването на неслужебни компютърни и комуникационни устройства в компютърните мрежи;
6. забранено е използването на лични носители на данни в ДПП «Шуменско плато»;
7. работните компютърни конфигурации, както и цялата инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели;
8. всеки достъп до регистрите по чл. 7 се регистрира в съответния журнал; в журнала за всеки достъп като минимум се регистрира информация относно: потребителя, време (дата и час) на достъпа и информация, която позволява да се идентифицират данните, до които е осъществен достъп;
9. информацията по т. 8 се съхранява най-малко две години;
10. данните в регистрите по чл. 7 се архивират съгласно Инструкцията за документооборота в ДПП «Шуменско плато»;

Чл. 19. За предотвратяване от неправомерно обработване на личните данни, което би довело до възникване на значителни вреди или кражба на самоличност, на всеки две години се извършва оценка на въздействие и се определя съответното ниво на защита за поддържаните регистри и бази данни от служителя по защита на личните данни.

Раздел VI

Действия за защита на личните данни при аварии, произшествия и бедствия

Чл. 20. Служителят по защита на личните данни в ДПП «Шуменско плато» организира действията за защита на личните данни при аварии, произшествия и

бедствия.

(4) Служителят по защита на личните данни информира директора на ДПП относно последствията от възникналото събитие и предлага действия за възстановяване на данните.

Раздел VII

Предоставяне на достъп до лични данни и обмен

Чл. 21. Предоставянето на достъп до лични данни или обмен се извършва при спазване на условията за допустимост на обработването на лични данни в чл. 4 от Закона за защита на личните данни и/или по ред, определен в друг нормативен акт.

Чл. 22. (1) Физическите лица имат право на достъп до личните им данни, в свободно избрана от тях форма, съгласно Закона за защита на личните данни, за който подават писмено заявление до администратора на лични данни. Заявлението се подава лично или чрез упълномощено лице с нотариално заверено пълномощно.

(2) При упражняване на правото си на достъп до личните си данни лицето има право по всяко време да поиска от администратора информация дали личните му данни се обработват, за какви цели, категориите данни и получателите, на които тези данни се разкриват.

(3) Лицата, за които се отнасят личните данни имат право да искат от администратора на лични данни да заличи, коригира или блокира неговите лични данни, както и да уведоми трети лица на които са разкрити личните му данни за извършеното заличаване, коригиране или блокиране на личните му данни.

(4) При подаване на искане по ал. 3, администраторът на лични данни се произнася в 14-дневен срок по искането като го уважава или отказва мотивирано извършването им. Решението се изпраща до заявителя по реда на АПК.

Чл. 23. Освен оператора на лични данни достъп до личните данни имат и служителите, пряко ангажирани с оформянето и проверката на законосъобразността на документите, свързани с регистрите по чл. 7.

Чл. 24. Достъп до личните данни се разрешава в нормативно установените случаи след представено писмено заявление, в което е посочено нормативното основание на което се изисква достъпът и предоставянето на личните данни, които се съхраняват в ДПП и целите за които се изисква.

Чл. 25. Обмен на лични данни с други администратори на лични данни се извършва в законоустановените случаи в съответствие със Закона за защита на личните данни.

Раздел VII

Задължения на служителите, работещи с лични данни

Чл. 26. Операторът на лични данни събира, обработва и съхранява в съответните регистри и бази данни, данните при спазване изискванията на Закона за защита на личните данни и другите законови и подзаконовите нормативни актове, свързани с тях.

Чл. 27. Лицата, чиито лични данни се събират се уведомяват относно целите, за които се събират, обработват и съхраняват, на кого се предоставят или разкриват извън организацията и колко време се съхраняват тези лични данни в ДПП. Уведомяването се извършва устно или писмено, което се удостоверява с подпись и дата на лицето, чийто данни се обработват.

Чл. 28. При възникнал инцидент, операторът на лични данни задължително регистрира времето на установяването му, причините за възникването и незабавно уведомява администратора.

Чл. 29. При аварии, произшествия и форсмажорни причини (пожари, наводнения и др.) операторът на лични данни и оторизираните от него или администратора лица, полагат всички възможни усилия за защита на техническите и информационни ресурси

от унищожаване, повреди или незаконен достъп, включително и изнасянето на хартиените носители на безопасно място.

Чл.30. Унищожаването на хартиените и технически носители се извършва след преценка от комисия, назначена със заповед от изпълнителния директор на ДПП.

Чл.31. След постигане целта на обработване на личните данни администраторът ги съхранява само в предвидените в закон случаи.

Чл.32. Временните хартиени носители (чернови), както и създадените временни електронни файлове се унищожават веднага, след като се изпълнят целите, за които са били създадени.

Чл. 33. В случаите, когато прехвърлянето на лични данни е предвидено в закон и е налице идентичност на целите на обработване, администраторът прехвърля данните на друг администратор, като предварително уведомява за това Комисията за защита на личните данни.

Чл. 47. Администраторът на лични данни осъществява периодичен контрол на всеки шест месеца за спазване изискванията на Закона за защита на личните данни и тази Инструкция по дейността за събиране, обработване, съхраняване и защита на лични данни в съответните регистри и бази данни в ДПП.

ЗАКЛЮЧИТЕЛНА РАЗПОРЕДБА

§ 1. Инструкцията се издава на основание чл. 23, ал. 4 от Закона за защита на личните данни и чл. 19, т. 2 от Наредба № 1 от 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни (ДВ, бр. 14 от 2013 г.).

§ 2. Контрол по изпълнение на инструкцията се осъществява от директора на ДПП «Шуменско плато»

ШУМЕН
04.05.2018г

До
Директора на
ДПП «Шуменско плато»

Заявка за информация

Описание на данните, които се изискват:
.....
.....

За какво се изискват:
.....

Подпись:

Заявката е подадена

от:

Дата:

Одобрявам:

(Директор)

Дата:

Резултат от заявката:

.....
.....
.....

Извършил заявката:

Дата:

Проверил заявката:

Дата: