МИНИСТЕРСТВО НА ЗЕМЕДЕЛИЕТО, ХРАНИТЕ И ГОРИТЕ
ИЗПЪЛНИТЕЛНА АГЕНЦИЯ ПО ГОРИТЕ
РЕГИОНАЛНА ДИРЕКЦИЯ ПО ГОРИТЕ – БЛАГОЕВГРАД
Благоевград, ул. "Васил Коритаров" № 2, п.код 2700, тел. централа 88 50 09, факс 88 50 04

УТВЪРДИЛ:
Директор на РДГ
инж.Иван Гергов

Инструкция за техническите и организационни мерки за защита на личните данни, събирани, обработвани и съхранявани в регистрите и базите данни, поддържани от Регионална дирекция по горите Благоевград

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 Регионална дирекция по горите - Благоевград (РДГ)и реда за достъп до тях;
2. задълженията на длъжностните лица в РДГ, които работят с лични данни или имат достъп до такива;
3. необходимите технически и организационни мерки за защита на личните данни в РДГ 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) РДГ обработва само законно събрани лични данни, необходими за конкретни, точно определени и законни цели. Личните данни, които РДГ 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 РДГ се извършва когато:

1. това е необходимо за изпълнение на нормативно установено 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 РДГ, 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 лова и опазване на дивеча и подзаконовите актове по прилагането им, 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 РДГ 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 РДГ, предоставяне и удостоверяване на информация, когато такава се изисква 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 РДГ се събират и обработват автоматизирано и неавтоматизирано /хартиен носител/.

Раздел II
ОПИСАНИЕ НА ПОДДЪРЖАНИТЕ РЕГИСТРИ И БАЗИТЕ ДАННИ, ТЕХНОЛОГИЯ НА ОБРАБОТВАНЕ И СРОК ЗА СЪХРАНЕНИЕ

Чл. 7. Регионална дирекция по горите Благоевград поддържа следните регистри и бази данни:

1. База данни „Управление на човешките ресурси в РДГ“;
2. Регистър „Ведомости и заплати“;
3. Регистър „Деловодство“.
4. Регистър на производствените горски марки;
5. Електронен регистър актова преписка;
6. Електронен регистър на служебните карти;

Чл. 8 (1). В **база данни „Управление на човешките ресурси в РДГ”**, 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. семейно 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 експерт „Човешки ресурси“ във връзка с възникване, изменение и прекратяване на трудовите и служебни правоотношения на служителите в Регионална дирекция по горите Благоевград. Данните са на хартиен носител, като се въвеждат и в електронен вид в базата данни.

(4)Данните в регистъра се събират, обработват и съхраняват при експерт „Човешки ресурси”, дирекция „Административно-правно и финансово-ресурсна дейност“.

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

(6). Личните данни по ал.1, които са на сървърите на РДГ са защитени физически и посредством защита на автоматизираната информационна система.

(7). Достъп до информация от досиетата се предоставя на служители от РДГ в нормативно установените случаи след подадена писмена заявка, писмено разрешение от директора на РДГ 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 местоживеене, месечен доход.

(2) Личните данни се обработват и съхраняват във връзка с:

1.назначаване, изменение и прекратяване на служебното/трудовото правоотношение, като информацията се подава от експерт „Човешки ресурси“, дирекция АПФРД;

2.сключване на граждански договор – след извеждането на договора в деловодството, същият се предоставя на Главния счетоводител;

3. при издаване на УП 2 и 3 /за пенсиониране и трудов стаж/ от физическите лица.

(3) Личните данни се обработват и съхраняват от Главен специалист – касиер-домакин, дирекция АПФРД на електронен и 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 се осигурява в нормативно установените случаи и при спазване на Закона за защита на личните данни, след писмено разрешение от директор на РДГ.

(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 електронна база данни, формирана чрез действащ деловоден софтуер /МИКСИ 2009/, съдържаща две или три имена на физическите лица.

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

(3) Физическата защита на личните данни в деловодството е организирана, като данните се обработват и съхраняват на сървърите в РДГ, а на хартиен носител досиетата са в заключващи се шкафове и помещения със строг контрол на достъпа до тях. Данните се обработват от Главен специалист – адм.секретар-деловодител, дирекция АПФРД, в съответствие с длъжностна му характеристика.

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

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

Чл. 11. (1) В **Регистъра на производствените марки** се съхраняват следните видове лични данни – три имена, ЕГН, адрес, телефон.

(2) Данните се обработват локално на компютър, разположен в работното помещение. Достъпът до операционната система се осъществява с индивидуална парола.

(3) Личните данни в базата данни по ал.1 се събират при подаване на документи за регистрация на обекти по чл. 206 от Закона за горите.

(4) Събирането, обработването и съхранението на лични данни в базата данни се извършва от определен със заповед служител. Данните са на хартиен носител, като се въвеждат и в електронен вид в базата данни.

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

Чл.12 (1) **Електронен регистър актова преписка** – представлява електронна база дани, съдържаща три имена, ЕГН, адрес, номер на лична карта, във връзка с изпълнението на вменените със Закона за горите.

(2) Базата данни е разположена на сървърите на РДГ. Информационната система е с контролиран достъп, въведена е за работа само от юрисконсултите от дирекция АПФРД и чрез нея се предоставят справки.

(3) Личните данни в базата данни се въвеждат и обработват през персонални защитени компютри от същите служители .

(4) Преписките на хартиен носител, със съдържащите се в тях лични данни се съхраняват на хартиен носител от Старши юрисконсулт

Чл.13 (1) **Електронен регистър на служебните карти** се води от служител системен администратор.

(2) В регистъра се въвеждат трите имена, адрес, ЕГН.

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. 14. Директорът на РДГ със заповед определя лице по защита на личните данни и лица, които отговарят за въвеждането и поддържането на личните данни в регистрите и базите данни по чл. 7.

Чл. 15. 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. 16 (1.) Събирането, обработването и съхранението на личните данни в регистрите и бази данни, поддържани в РДГ се осъществява по следния начин:

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 носител- файлове, съответно по видове - текстови, програмно-генерирани, тип "електронна таблица".

3. Чрез глобалната мрежа (Интернет).

Раздел V
Технически и организационни мерки за защита на личните данни

Чл. 17. 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. 18. 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 придружава 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. сървърното и комуникационното оборудване се разполага в отделно помещение с ограничен контролиран достъп; достъпът до сървърното помещение е разрешен единствено на системен администратор;

7. осъществяване на контрол по достъпа, предоставен до регистрите по чл. 3, се извършва по ред, определен с друг нормативен акт;

8. 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 РДГ.

9. организарана е охрана на работните помещения чрез постоянно видеонаблюдение;

10. в работните помещения се осигурява климатична и пожароизвестителна система; в РДГ за помещението със сървърно и комуникационно оборудване задължително се разполагат пожарогасителни средства и се осигуряват отделно климатична система, пожароизвестителна система;

11. в РДГ контролът на достъпа през общите входове към работните помещения и помещението със сървърното и комуникационното оборудване се извършва с ключ, достъп до който има само директора и двама служители;

12. всички физически информационни носители, използвани за запис на лични данни (за технологични или други цели), се съхраняват в помещението със сървърно и комуникационно оборудване; контролът по използването и съхранението на носителите се извършва от Системен администратор.

13. всички действия по актуализация на личните данни от служителите в РДГ 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. 19. 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 РДГ, 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 директора на РДГ, 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 РДГ.

Чл. 20. За персоналната защита на личните данни се предприемат следните мерки:

1. попълване на декларация от всеки служител в РДГ 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 РДГ;

4. забранява се споделянето на критична информация, като пароли за достъп, идентификатори и други между служителите; удостоверението за квалифициран електронен подпис 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 РДГ;

Чл. 21. За защита на информационната система и мрежи се предприемат следните мерки:

1. по отношение на регистрите и базите данни по чл. 7:

а) сървърното оборудване е със система за откриване и корекции на грешки в оперативната памет;

б) подсистемите за съхранение на данни са със защита срещу отпадане на някое от изграждащите ги устройства – постоянна памет;

в) непрекъсваемите токозахранващи устройства (UPS) са за цялото оборудване, необходимо за правилната работа на регистрите (компютърни конфигурации, сървъри и комуникационни средства);

2. мрежовите интерфейси за хардуерна настройка на сървърното и комуникационното оборудване се обособяват в отделен мрежови сегмент;

3. сървърите, предназначени да предоставят услуги на потребители през интернет, се обособяват в отделен мрежови сегмент;

4. сървърът за електронна поща сканира всички писма с антивирусен софтуер, за който е активирано автоматично обновяване на антивирусните дефиниции;

5. връзките между мрежовите сегменти помежду им и с интернет се контролират със специализиран софтуер – защитна стена;

6. за всички сървърни и работни компютърни конфигурации се използват операционни системи и приложен софтуер, за които е осигурена поддръжка от производителя с обновления по отношение на сигурността;

7. на всяка работна компютърна конфигурация се осигурява антивирусен софтуер с включено автоматично обновяване и постоянно сканиране;

8. всяка работна компютърна конфигурация включва по възможност предпоследна или последна Desktop операционна система Windows или Linux;

9. забранено е включването на неслужебни компютърни и комуникационни устройства в компютърните мрежи;

10. включването на мобилни компютри в компютърните мрежи се извършва след

разрешение от системен администратор;

11. забранено е използването на лични носители на данни в РДГ;

12. за пренос на данни във връзка с изпълнението на конкретни дейности се използват оптични носители;

13. използваните оптични носители се унищожават в специализирани машини за унищожаване на документи;

14. работните компютърни конфигурации, както и цялата инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели;

15. в РДГ се провежда редовна профилактика на компютърните и комуникационните устройства от Системен администратор;

16. използването на работните компютърни конфигурации се извършва след идентификация с потребителско име и парола, изисквани от съответната операционна система;

17. паролите за идентификация и достъп до регистрите по чл. 7 се създават, променят и предоставят от Системния администратор;

18. паролата за достъп е персонална, като в случай на компрометиране на парола тя се подменя с нова. Забранява се друго предоставяне и записване на парола;

19. поддържането в актуално състояние на личните данни се осъществява чрез пакетна и директна актуализация;

20. всеки достъп до регистрите по чл. 7 се регистрира автоматизирано в журнал за съответния регистър; 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;

21. информацията по т. 20 се съхранява най-малко две години;

22. правата и ролите на потребителите се определят съобразно преките им задължения и/или съобразно условията на достъпа, регламентирани със споразумение или по ред в друг нормативен акт;

23. предоставянето на данни във вид на списъци във връзка с изпълнението на служебни задължения на служителите на РДГ се извършва след попълнена и одобрена писмена заявка съгласно приложение № 1;

24. непосредствен достъп до личните данни в регистрите по чл. 3 чрез системни програмни средства е разрешен на системния администратор и операторът на лични данни;

26. данните в регистрите по чл. 7 се архивират съгласно Инструкцията за деловодната дейност и документооборота в Регионална дирекция по горите;

27. данните върху оптичните носители се записват в криптиран вид чрез специализиран софтуер;

28. при възникване на нарушения от РДГ се сформира екип за действие според ситуацията.

Чл. 22. Мерките по криптографската защита включват система за разпределение и управление на криптогрфски ключове в рамките на КЕП.

Чл. 23. (1) Архивни копия на регистрите по чл. 7 се съхраняват на минимум две различни физически места.

(2) Създаването на архивни копия и времевите интервали за тяхното формиране се определя със заповед на изпълнителния директор на РДГ.

(3) След изтичане на времевите интервали за изграждане на архивни копия носителите се използват отново за създаване на нови архивни копия.

Чл. 24. 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 от РДГ 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. 25. Служителят по защита на личните данни в РДГ организира действията за защита на личните данни при аварии, произшествия и бедствия.

Чл. 26. (1) В случаите, когато при аварии, произшествия или бедствия са засегнати данните в поддържаните регистри по чл. 7, същите се възстановяват от архивни копия .

(2) Служителят по защита на личните данни и Системния администратор правят преглед на последствията от възникналото събитие и обема на засегнатите данни.

(3) В зависимост от засегнатите данни се възстановяват техните най-скорошни архивни копия, възстановяват се промените и трансакциите, извършени след снемане на архивните копия, посредством журнала на трансакциите им (transaction log).

(4) Служителят по защита на личните данни и системния администратор информират директора на РДГ относно последствията от възникналото събитие и предлагат действия за възстановяване на данните.

(5) Данните се възстановяват самостоятелно от Системния администратор или съвместно с оператора на лични данни.

(6) Провеждат се тестове за работоспособността на регистрите, поддържани в електронен вид, и се извършва проверка дали възстановените данни са актуални.

(7) В случай на непредвидени обстоятелства, възпрепятстващи успешното възстановяване на данните, системния администратор информира директора до края на следващия работен ден.

Раздел VII
Предоставяне на достъп до лични данни и обмен

Чл. 27. 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. 28. (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. 29. 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. 30. 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 РДГ и целите за които се изисква.

Чл. 31. 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 VIII
Задължения на служителите, работещи с лични данни

Чл. 32. 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. 33. 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 РДГ. Уведомяването се извършва посредством интернет страницата на РДГ за определени административни производства, устно или писмено за останалите случаи, което се удостоверява с подпис и дата на лицето, чийто данни се обработват.

Чл. 34. При възникнал инцидент, операторът на лични данни задължително регистрира времето на установяването му, причините за възникването и незабавно уведомява администратора.

Чл. 35. 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. 36. Унищожаването на хартиените и технически носители се извършва след преценка от комисия, назначена със заповед от директора на РДГ.

Чл. 37. След постигане целта на обработване на личните данни администраторът ги съхранява само в предвидените в закон случаи.

Чл. 38. Временните хартиени носители (чернови), както и създадените временни електронни файлове се унищожават веднага, след като се изпълнят целите, за които са били създадени.

Чл. 39. Операторите на лични данни извършват ежемесечни проверки на техническите и електронни носители и техните защити, с цел предотвратяване на тяхното унищожаване, повреждане или нерегламентиран достъп до личните данни.

Чл. 40. 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. 41. 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 РДГ.

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 зам.директора на РДГ.

Приложение № 1
към чл. 19, т. 2

До
Директора на
РДГБлагоевград

Заявка за информация

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

.....

.....

За какво се изискват: .....

Подпис: .....

Заявката е подадена

от: .....

Дата: .....

Одобрявам: .....

(Директор на РДГ .....)

Дата: .....

Резултат от заявката:

.....

.....

.....

Извършил заявката: Дата: .....

.....

Проверил заявката: Дата: .....

.....

МИНИСТЕРСТВО НА ЗЕМЕДЕЛИЕТО, ХРАНИТЕ И ГОРИТЕ

ИЗПЪЛНИТЕЛНА АГЕНЦИЯ ПО ГОРИТЕ

РЕГИОНАЛНА ДИРЕКЦИЯ ПО ГОРИТЕ – БЛАГОЕВГРАД

Благоевград, ул. "Васил Коритаров" № 2, п.код 2700, тел. централа 88 50 09, факс 88 50 04

УВАЖАЕМИ ДАМИ И ГОСПОДА,

На основание Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО в сила от 25.05.2018 г. и Закона за защита на личните данни Ви уведомяваме, че всички лични данни, съдържащи се в горскостопанските програми, входирани в РДГ – Благоевград ще бъдат използвани единствено и само за целите на разглеждане на горскостопанските програми и последващ контрол по отношение мероприятията, предвидени в горските територии.

Личните данни могат да бъдат предоставени на съд, прокуратура и органите на МВР.

ДИРЕКТОР РДГ :...../п./.....

/инж. И. Гергов/

ОДОБРИЛ:
ДИРЕКТОР РДГ:
ИНЖ. ИВАН ГЕРГОВ

Процедура за информираност на субектите на лични данни и прозрачност при обработването им в регистрите и бази данни в РДГ Благоевград

Настоящата процедура е разработена в съответствие с целите на Регламент (ЕС) 2016/679 на Европейския съвет.

1. Обработката на лични данни се извършва при спазване на правата на информираност на субектите на лични данни и прозрачност при обработването им в регистрите и бази данни.
2. Принципът на прозрачност изисква за всяко обработване на субектите на лични данни да се дава определена информация, която да гарантира тяхното право да се запознаят с процеса и да го оспорят при нужда.
3. На физическото лице, което е субект на данни, се предоставя информация за администратора на лични данни, както и за обработването на личните му данни. Тази информация включва:
   - данни, идентифициращи администратора, както и негови координати за връзка, вкл. координатите за връзка с длъжностното лице по защита на данните;
   - целите и правното основание за обработването;
   - получателите или категориите получатели на личните данни, ако има такива;
   - намерението на администратора да предаде личните данни на трета страна (когато е приложимо);
   - срока на съхранение на личните данни;
   - информация за всички права, които субектът на данни има;
   - правото на жалба до надзорния орган;
4. Информацията се предоставя от служителят определен за обработване на личните данни в съответния регистър или база данни.

5. Ако личните данни са получени от друг източник информацията се предоставя в рамките на срок от един месец след получаването на личните данни.
6. Субектът на лични данни устно декларира, че е съгласен да предостави личните си данни.
7. Администраторът информира субектите на лични данни през целия период на обработването – при начините, по които комуникират във връзка с техните права и в специфични случаи по време на обработването – например при нарушаване на сигурността на личните данни или в случаите на съществени промени при обработването.