



РЕПУБЛИКА БЪЛГАРИЯ

МИНИСТЕРСТВО НА ЗЕМЕДЕЛИЕТО, ХРАНИТЕ И ГОРИТЕ

ОБЛАСТНА ДИРЕКЦИЯ “ЗЕМЕДЕЛИЕ” БЛАГОЕВГРАД

УТВЪРДИЛ: (П)

КИРИЛ УКЕВ

Директор на Областна дирекция „Земеделие“

ИНСТРУКЦИЯ

**ЗА ТЕХНИЧЕСКИТЕ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА
ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В
РЕГИСТРИТЕ, ПОДДЪРЖАНИ ОТ ОБЛАСТНА ДИРЕКЦИЯ
„ЗЕМЕДЕЛИЕ“ БЛАГОЕВГРАД ПРИ ТЯХНОТО ОБРАБОТВАНЕ
(СЪБИРАНЕ, ИЗПОЛЗВАНЕ, ОБМЕН, СЪХРАНЯВАНЕ И
УНИЩОЖАВАНЕ)**

Утвърдена със Заповед № РД-08-104/ 08.05.2018 г. на Директора на Областна дирекция
“Земеделие” Благоевград

ГР. БЛАГОЕВГРАД

2018 г.

Глава първа

ОБЩИ ПОЛОЖЕНИЯ

Чл.1. (1) С настоящата Инструкция за техническите и организационни мерки за осигуряване на защита на личните данни в регистрите, поддържани от Областна дирекция „Земеделие“ Благоевград при тяхното обработване (събиране, използване, обмен, съхраняване и унищожаване), наричана по-долу „Инструкцията“, се определят необходимите технически и организационни мерки за защита на личните данни, обработвани от Областна дирекция „Земеделие“ Благоевград, в качеството и на администратор на лични данни, наричана по-долу „Администратора“.

(2) Инструкцията е разработена в съответствие с разпоредбата на глава IV, раздел 1, член 24 от Регламент (ЕС) 2016/ 679 на Европейския парламент и на Съвета от 27 април 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 (Общ регламент относно защитата на данните), наричан по-долу “Регламента”, глава IV, чл.23, ал.4 от Закона за защита на личните данни, наричан по-долу “Закона” и глава V, чл.19, т.2 от Наредба №1/ 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, наричана по-долу “Наредбата”.

Чл.2. (1) Инструкцията има за цел защита на личните данни от случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване чрез определяне на необходимите технически и организационни мерки за това, гарантиращи поверителност, цялостност и наличност на личните данни.

(2) За изпълнение на целта по ал.1, Администраторът структурира Регистър на дейностите свързани с обработването на лични данни, съдържащ информация за:

1. поддържаните регистри, основанията за поддържането им и целите на обработването на личните данни в тях;
2. категориите субекти и категории лични данни, технологията на обработване и сроковете за съхраняване на личните данни;
3. обработващите и получателите на лични данни;
4. нивата на въздействие, нивата на защита, техническите и организационни мерки за защита на личните данни.

Чл.3. За определяне на нивата на защита и необходимите технически и организационни мерки за защита на личните данни, Администраторът използва като инструмент оценка на въздействието върху личните данни.

Чл.4. Администраторът определя длъжностно лице по защита на личните данни, което консултира Администратора по всички въпроси свързани със задълженията му по прилагане на Регламента или други нормативни задължения относно защитата на личните данни.

Чл.5. Администраторът спазва принципа на отчетност пред надзорния орган по прилагането на Регламента или други нормативни задължения относно защитата на личните данни.

Глава втора

РЕГИСТЪР НА ДЕЙНОСТИТЕ СВЪРЗАНИ С ОБРАБОТВАНЕТО НА ЛИЧНИТЕ ДАННИ

Чл.6. Администраторът поддържа на хартиен и електронен носител Регистър на дейностите свързани с обработването на лични данни, неразделна част от настоящата Инструкция.

Раздел първи

РЕГИСТРИ И ОСНОВАНИЯ ЗА ПОДДЪРЖАНЕТО ИМ.

ЦЕЛИ НА ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Чл.7. (1) Администраторът обработва лични данни, като за целта структурира регистри.

(2) Администраторът обработва лични данни в поддържаните регистри при наличието на поне едно от следните основания:

1. обработването, произтича от нормативно задължение за Администратора;
2. субектът на лични данни е дал своето съгласие за обработване за една или повече конкретни цели;
3. обработването е необходимо за изпълнение на задължения по договор, по който субектът на лични данни е страна или за предхождащи сключването на договор действия предприети по негово искане;
4. обработването е необходимо, за да се защитят живота и здравето на субекта на лични данни или на други субекти;
5. обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес или при упражняването на официални правомощия, които са предоставени на Администратора или на трети страни.

(3) Администраторът се задължава да спазва забраната за обработване на следните категории лични данни:

1. разкриващи расов или етнически произход;
2. политически възгледи, религиозни или философски убеждения, или членство в политически и синдикални организации;
3. генетични данни, данни за сексуалния живот или сексуалната ориентация.

Раздел втори

КАТЕГОРИИ СУБЕКТИ И КАТЕГОРИИ ЛИЧНИ ДАННИ.

ТЕХНОЛОГИЯ НА ОБРАБОТВАНЕТО И СРОКОВЕ ЗА СЪХРАНЯВАНЕ ЛИЧНИТЕ ДАННИ

Чл.8. Администраторът обработва лични данни на следните категории субекти:

1. физически лица, потребители на административни услуги;
2. физически лица в договорни отношения с Администратора;
3. физически лица в служебни или трудови правоотношения с Администратора.

Чл.9. (1) Администраторът обработва следните категории лични данни:

1. физическа идентичност – име, ЕГН, паспортни данни, постоянен и настоящ адрес, телефон, e-mail;
2. икономическа идентичност – имотно състояние, финансово състояние, участие и/ или притежаване на дялове или ценни книжа в дружества, банкови сметки;
3. социална идентичност – образование, трудова дейност;
4. гражданскоправната идентичност – семейно положение, родствени връзки.

(2) За целите на трудовото и социално законодателство, превантивната и трудова медицина, сигурността и вътрешния ред, Администраторът обработва следните специални категории лични данни:

1. физиологична идентичност – здравословно състояние,
2. психическа идентичност – психическо здраве;
3. психологическа идентичност – психологическо състояние;
4. други идентифициращи субектите лични данни – биометрични данни.

Чл.10. Администраторът обработва лични данни със задължението за спазване на следните права на субектите на лични данни:

1. право на прозрачна информация, комуникация и условия за упражняване на правата им;
2. право на съгласие и оттегляне на съгласието;
3. право на информация за обработваните лични данни и достъп до тях;
4. право на коригиране, изтриване (право „да бъдеш забравен“) и ограничаване на обработването;
5. право на уведомяване при коригиране, изтриване и ограничаване на обработването;
6. право на преносимост;
7. право на възражение;
8. право да не бъде обект на автоматизирано вземане на индивидуални решения, включително профилиране;
9. право на съобщаване за нарушение на сигурността на личните данни;
10. право на подаване на жалба до надзорния орган;
11. право на ефективна съдебна защита срещу администратор или обработващ лични данни;
12. право на обезщетение и отговорност за причинени вреди.

Чл.11. Администраторът обработва лични данни неавтоматизирано на хартиен носител и автоматизирано на електронен носител.

Чл.12. Администраторът обработва лични данни за период не по-дълъг от необходимия за целите, за които те се обработват, съгласно сроковете произтичащи от нормативни задължения или съгласно сроковете разписани в Индивидуалната номенклатура на делата със срокове за тяхното съхраняване, образувани от административните дейности в Областна дирекция „Земеделие“ Благоевград.

Раздел трети

ОБРАБОТВАЩИ ЛИЧНИ ДАННИ. ПОЛУЧАТЕЛИ НА ЛИЧНИ ДАННИ

Чл.13. Администраторът обработва лични данни при спазване на следните принципи:

1. законосъобразност, добросъвестност и прозрачност;
2. ограничение на целите;
3. свеждане на данните до минимум;
4. точност;
5. ограничение на съхраняването;
6. цялостност и поверителност;
7. отчетност.

Чл.14. Обработването на лични данни се извършва от:

1. длъжностни лица, действащи под ръководството и по указание на Администратора, с правомощия, произтичащи от нормативно задължение, разписани в длъжностната им характеристика или от заповед на Администратора. Длъжностните лица, обработващи лични данни се задължават да спазват изискването за поверителност (неразкриване) на лични данни;

2. обработващи лични данни от името и по указание на Администратора, с правомощия произтичащи от договор или нормативно задължение за обработващите спрямо Администратора, регламентиращи предмета и срока на действие на обработването, обхвата, естеството и целта на обработването, категориите субекти и категориите лични данни, както и правата и задълженията на обработващите. Обработващите лични данни се задължават да спазват изискването за поверителност (неразкриване) на лични данни.

Чл.15. Длъжностните лица, действащи под ръководството и по указание на Администратора извършват следните действия по обработване на лични данни:

1. събиране, записване, организиране, подреждане, структуриране;
2. адаптиране, промяна, извличане, консултиране, ползване, пренасяне, комбиниране, коригиране, ограничаване;
3. съхраняване, изтриване или унищожаване.

Чл.16. (1) За изпълнение или нарушение на разпоредбите на Регламента или други нормативни задължения относно защитата на личните данни, Администраторът и обработващият лични данни носят отговорност за вреди.

(2) При установено изпълнение или нарушение от страна на Администратора или обработващия лични данни, надзорният орган предприема необходимите мерки и в допълнение към тях или вместо тях налага административни наказания „глоба“ и „имуществена санкция“ при спазването на принципите на ефективност, пропорционалност и превантивност.

Чл.17. За изпълнение или нарушение на разпоредбите на Инструкцията длъжностните лица, обработващи лични данни под ръководството и по указание на Администратора носят отговорност по Закона за защита на личните данни, Закона за държавния служител и Кодекса на труда.

Чл.18. (1) Получател на лични данни е всяко физическо или юридическо лице, публичен орган или друга структура, който получава личните данни.

(2) Трета страна е всяко физическо или юридическо лице, публичен орган или друга структура, различна от субекта на лични данни, Администратора, обработващия лични данни и лицата, които под ръководство на администратора или на обработващия лични данни имат право да обработват личните данни.

Чл.19. (1) Публични органи с правомощия, произтичащи от нормативно задължение получават лични данни след отправяне на искане в писмена форма, което е обосновано и конкретно, не се отнася до целия регистър и не води до свързване на регистри, съдържащи лични данни.

(2) Публичните органи по ал.1 обработват получените лични данни в съответствие с Регламента или други нормативни задължения относно защитата на личните данни, като за целите на обработването не се изисква съгласие на субекта на лични данни.

Раздел четвърти

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО.

НИВА НА ВЪЗДЕЙСТВИЕ. НИВА НА ЗАЩИТА. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

Чл.20. (1) Оценка на въздействието е инструмент за определяне на нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от обработваните категории лични данни и броя на засегнатите физически лица, както и за определяне на необходимите технически и организационни мерки, гарантиращи поверителност, цялостност и наличност на личните данни.

(2) Дирекцията извършва оценка на въздействието:

1. периодично на всеки две години, при промяна в поддържаните регистри или структуриране на нов регистър;
2. форсмажорно при съществуваща вероятност за висок риск при обработването на личните данни и предвид естеството, обхвата и целта на обработването.

(3) Администраторът извършва предварителна консултация с надзорния орган за целите на ал.2, т.2.

Чл.21. (1) Нивата на въздействие се определят за всеки регистър, съдържащ лични данни по всеки от критериите поверителност, цялостност и наличност, като общото ниво на въздействие е най-високото определено.

(2) Администраторът определя следните нива на въздействие върху личните данни в поддържаните регистри:

1. високо;
2. средно.

Чл.22. (1) Администраторът определя следните технически и организационни мерки за защита на личните данни в поддържаните регистри:

1. физическа;
2. персонална;

3. документална;
4. защита на автоматизирани информационни системи и мрежи;
5. псевдонимизация и криптиране на личните данни.

(2) Администраторът определя следните нива на защита на личните данни в поддържаните регистри в съответствие с определените нива на въздействие:

1. високо;
2. средно.

Чл.23. Администраторът предприема необходимите действия за защита на личните данни при настъпването на форсмажорни обстоятелства като бедствия, аварии и пожари в съответствие с:

1. План за защита при бедствия в Областна дирекция „Земеделие“ Благоевград;
2. Противопожарна инструкция на Областна дирекция „Земеделие“ Благоевград.

Глава трета

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ЛИЧНИТЕ ДАНИ

Чл.24. (1) Администраторът определя длъжностно лице по защита на личните данни със следните задачи:

1. да информира и съветва Администратора и обработващите лични данни под негово ръководство и по негово указание;
2. да наблюдава спазването на Регламента и другите нормативни задължения относно защитата на личните данни, политиките на Администратора, възлагането на отговорности, повишаването на осведомеността, обучението на обработващите лични данни под негово ръководство и по негово указание, както и извършването на одити;
3. при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на личните данни и да наблюдава нейното извършване;
4. да съдейства на надзорния орган при изпълнение на задълженията му;
5. да действа като лице за контакт с надзорния орган по въпроси, свързани с обработването на лични данни, включително предварителната консултация преди обработването при съществуваща вероятност за висок риск, както и по целесъобразност да се консултира по всякакви други въпроси.

(2) Администраторът и обработващите лични данни по негово указание или от негово име подпомагат длъжностното лице по защита на личните данни в изпълнението на задачите по ал.1.

(3) Длъжностното лице по защита на личните данни:

1. не може да получава никакви указания във връзка с изпълнение на задълженията си.
 2. се задължава да спазва изискването за поверителност (неразкриване) на личните данни;
 3. може да изпълнява и други задачи, които не водят до конфликт на интереси;
- (4) Длъжностното лице по защита на личните данни спазва принципа на отчетност по отношение на Администратора.

Глава четвърта

ОТЧЕТНОСТ ПРЕД НАДЗОРНИЯ ОРГАН

Чл.25. (1) Администраторът спазва принципа на отчетност пред надзорния орган, като носи отговорност и е в състояние да докаже спазването на останалите принципи при извършването на дейности по обработване на лични данни.

(2) За изпълнението на задължението по т.1 Администраторът разработва:

1. План за прилагане на определените технически и организационни мерки за защита на личните данни;
2. Вътрешни правила и процедури за действие при нарушаване на сигурността на личните данни;
3. Етичен кодекс за поведение на Администратора.

Глава пета

СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ЛИЧНИ ДАННИ

Чл.26. (1) Администраторът извършва периодично всяка година преглед относно необходимостта от обработване на лични данни и съхраняването им, както и за тяхното унищожаване при отпадане на задължението за обработване.

(2) След изтичане на сроковете за съхранение на личните данни, съгласно чл.12 от Инструкцията, Администраторът определя чрез актове носителите на лични данни, начина и мястото за унищожаването им.

(3) Унищожаването се извършва посредством наличните към момента технически възможности на Администратора посредством нарязване с шредер и/ или изгаряне на хартиените носители при неавтоматизирана обработка на личните данни, както и посредством разрушаване на външни преносими носители или заличаване (форматиране) на твърди дискови устройства при автоматизирана обработка на лични данни.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

По смисъла на настоящата Инструкция:

§1. „лични данни“ са всяка информация, идентифицираща физическо лице („субект на данни“) пряко или непряко чрез идентификатор като име, идентификационен номер, местонахождение, онлайн идентификатор или по специфични признаци за физическата, физиологичната, психическата, психологическата, икономическата, социалната, гражданскоправната или друга идентичност.

§2. „регистър на лични данни“ е всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или друг принцип.

§3. „обработване“ е всяка дейност извършвана чрез автоматични или неавтоматични средства свързана със събиране, използване, обмен, съхраняване и унищожаване.

§4. „администратор на лични данни“ е Областна дирекция „Земеделие“ Благоевград.

§5. „надзорен орган“ е Комисията за защита на личните данни.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Указания по приложението и изпълнението на Инструкцията се дават от Главния секретар.

§2. Изменението и допълнението на Инструкцията се извършва по реда на приемането и.

§3. Инструкция се утвърждава със заповед на Директора на Областна дирекция „Земеделие“ Благоевград и влиза в сила от момента на утвърждаването и.