

УТВЪРДИЛ:

ОБЛАСТЕН УПРАВИТЕЛ:

ЧАВДАР БОЖУРСКИ

ВЪТРЕШНИ ПРАВИЛА ЗА СЪБИРАНЕ, ОБРАБОТВАНЕ, СЪХРАНЯВАНЕ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ОБЛАСТНА АДМИНИСТРАЦИЯ СЛИВЕН

I. ПРЕДМЕТ

Чл. 1 (1) Вътрешните правила за събиране, обработване, съхраняване и защита на личните данни на Областна администрация Сливен („Правилата“) определят организацията и реда, по които Областна администрация Сливен, събира, записва, организира, структурира, съхранява, адаптира или променя, извлича, консултира, използва, разкрива чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подрежда или комбинира, ограничава, изтрива, унищожава или обработва по друг начин лични данни за целите на своята дейност.

(2) В зависимост от конкретната ситуация, Областна администрация Сливен може да обработва данни в качеството на администратор или обработващ.

(3) Правилата са изготвени в съответствие с изискванията на Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета на Европейския съюз 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), Закона за защита на личните данни и подзаконовите актове по прилагането му, ръководствата и насоките на Комисията за защита на личните данни и Работната група по чл. 29 (след 25.05.2018 г. – на Европейския комитет по защита на данните).

Чл. 2. Настоящите Правила уреждат:

- (1) Целите и принципите за обработка на личните данни;
- (2) Категориите лични данни, субектите на данни и техните права;
- (3) Процедурите за администриране на лични данни;
- (4) Лицата, които обработват лични данни и техните задължения;
- (5) Мерките, които Областна администрация Сливен е предприела за защити на личните данни на субектите;
- (6) Правилата за предаване на лични данни на трети лица в България и чужбина;
- (7) Оценката на въздействието върху защитата на лични данни;
- (8) Начинът на унищожаване на предоставените лични данни на хартиен и електронен носител;
- (9) Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността.

II. ЦЕЛИ И ПРИНЦИПИ

Чл. 3 Лични данни е всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

Чл. 4. Целта на настоящите правила е гарантиране на неприкосновеността на личността и личния живот чрез осигуряване защита на личните данни на физическите лица при неправомерно обработване в процеса на свободното движение на данните.

Чл. 5. Целите на обработването на лични данни са:

(1) свързани с дейността на Областна администрация Сливен като държавна институция, съгласно поверените ѝ права и задължения от нормативните актове в страната и приложимото законодателство;

(2) във връзка с подаваните от гражданите заявления, жалби, предложения, сигнали и други, които Областна администрация е оправомощена да извършва в рамките на своите компетенции;

(3) управление на човешките ресурси, изплащане на трудовите възнаграждения и изпълнение на свързаните с това задължения на работодателя, както и на други права и задължения на Областна администрация Сливен в качеството ѝ на работодател;

(4) администриране на отношенията с потребители на Областна администрация Сливен за предоставяне на услуги;

(5) сключване и изпълнение на договори с доставчици за предоставяне на услуги на Областна администрация Сливен.

Чл. 6. Принципите за защита на личните данни са:

(1) **Законосъобразност, добросъвестност и прозрачност** - обработвани при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;

(2) **Ограничение на целите** - събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;

(3) **Свеждане на данните до минимум** - данните са подходящи, свързани със целите на обработването и ограничени до необходимото във връзка с целите на обработването;

(4) **Точност** - поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;

(5) **Ограничение на съхранението** - данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки;

(6) **Цялостност и поверителност** - обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;

(7) **Отчетност** - администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Чл. 7. Обработването на лични данни се извършва, само ако и доколкото е приложимо поне едно от следните условия:

(1) Субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

(2) Обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

(3) Обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

(4) Обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или за друго физическо лице;

(5) Обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

(6) Обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по – специално когато субектът на данните е дете

Тази алинея не се прилага за обработването, което се извършва от публични органи при изпълнението на техните задачи.

III. СУБЕКТИ НА ДАННИ И КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 8. (1) Областна администрация Сливен събира и обработва лични данни, необходими за осъществяване на своите права и задължения като държавна администрация, работодател, доставчик на услуги и контрагент при съблюдаване изискванията на приложимото законодателство. Личните данни, обработвани от Областна администрация Сливен, се отнасят до:

- граждани;
- кандидати за работа, работници и служители и изпълнители по граждански договори;
- потребители на услуги;
- доставчици на услуги.

(2) Относно лицата, заети по служебни, трудови или граждански правоотношения в Областна администрация Сливен, и на кандидатите за работа, се събират следните лични данни, съгласно приложимата нормативна уредба:

1. Идентификация: три имена, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, номер на лична карта или паспортни данни и други данни;

2. Образование и професионална квалификация: данни, свързани с образование, трудов опит, професионална и лична квалификация и умения;

3. Здравни данни: здравословно състояние, ТЕЛК решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация, необходими съгласно приложимия Закон;

4. Други данни чието обработване е необходимо за изпълнение на правата и задълженията на Областна администрация Сливен като работодател.

(3) Относно физически лица, потребители на услуги, се събират лични данни, които са необходими за изпълнението на законовите задължения на Областна администрация Сливен, като доставчик на услуги, както следва: име, постоянен и/или настоящ адрес, телефон, електронна поща.

Юридическите лица потребители на услуги е необходимо да предоставят данни относно: името на представляващия, адрес за кореспонденция, телефон, седалището и адреса на управление, БУЛСТАТ/ЕИК, e-mail адрес.

(4) Относно физически лица, доставчици на услуги се обработват лични данни, необходими за сключването и изпълнението на договори за предоставяне на услуги на администрацията от външни доставчици: име, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни, електронна поща.

(5) Областна администрация Сливен обработва чувствителни данни, само до колкото това е необходимо за изпълнение на специфичните ѝ права и задължения в областта на трудовото и осигурително законодателство.

Чл. 9. Права на субектите на данни:

(1) Всяко лице има право да иска достъп до своите лични данни, включително и да се иска потвърждение дали данните, отнасящи се до него, се обработват, да се информира за целите на това обработване, категориите данни и за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него.

(2) Правото на достъп се осъществява чрез заявление на засегнатото физическо лице, получено на адреса на Областна администрация Сливен или по електронен път. При подаване на заявлението по електронен път следва същото да е подписано с усъвършенстван електронен подпис, основан на квалифицирано удостоверение за електронни подписи, или квалифициран електронен подпис, съгласно изискванията на Регламент (ЕС) № 910/2014 на европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ, L 257/73 от 28 август 2014 г.) и на Закона за електронния документ и електронните удостоверителни услуги.

(3) Отговор на заявлението следва да се получи в срок от един месец от датата на входиране. При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на заявленията.

(4) Всяко физическо лице има право да поиска заличаването, коригирането или блокирането на негови лични данни, обработването, на които не отговаря на изискванията на закона.

(5) Всяко лице има право да възрази срещу обработването на и/или предоставянето на трети лица на неговите лични данни без необходимото законово основание.

(6) Субектите на данни имат право да:

1. възразят срещу употреба на личните им данни;
2. бъдат уведомени за нарушение на защита на данните, което е вероятно да доведе до висок риск за техните права и свободи;
3. подават жалби до регулаторния орган – КЗЛД;
4. в някои случаи да получат или да поискат техните лични данни да бъдат трансферирани до трета страна в структуриран, общо използван формат, подходящ за машинно четене (право на преносимост).

Чл. 10. (1) Категориите лични данни, които се отнасят до субектите могат да бъдат:

1. физическа идентичност – име, ЕГН/ЛНЧ, данни за лична карта/паспорт, адрес, месторождение, телефон за връзка, един или повече специфични признаци и други;
2. семейна идентичност – семейно положение (наличие на брак, развод, брой членове на семейството, в т.ч. деца до 18 години), родствени връзки и др.;
3. образование – вид на образованието, място, номер и дата на издаване на дипломата, допълнителна квалификация. Предоставят се от лицата на основание нормативно задължение във всички случаи, когато е необходимо;
4. допълнителна квалификация – данните се предоставят от лицата на основание нормативно задължение във всички случаи, когато е необходимо;
5. трудова дейност – професионална биография – данните се предоставят от лицата на основание нормативно задължение във всички случаи, когато е необходимо;

6. медицински данни – физиологично, психическо и психологично състояние на лицата. Данните са от значение при заемане на длъжности и изпълнение на функции, изискващи особено висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, в това число от рискови групи;

7. икономическа идентичност – имотно състояние, финансово състояние, участие и/или притежаване на дялове или ценни книжа в дружества и др.;

8. други – лични данни относно гражданско-правния статус на лицата, необходими за длъжностите, свързани с материална отговорност. Предоставят се на основание нормативно задължение.

(2) Специални категории лични данни:

1. Лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за сексуалния живот или сексуалната ориентация на физическото лице.

2. Забранява се обработването на лични данни от специалните категории, освен ако не е налице едно от следните условия:

- Субектът на данни е дал своето изрично съгласие за обработването на тези лични данни за една или повече конкретни цели, освен когато в правото на ЕС или в правото на държава членка се предвижда, че посочената забрана не може да бъде отменена от субекта на данни;

- Обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила, дотолкова, доколкото това е разрешено от правото на ЕС или правото на държава членка, или съгласно колективна договореност в съответствие с правото на държава членка, в което се предвиждат подходящи гаранции за основните права и интересите на субекта на данните;

- Обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

- Обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;

- Обработването е необходимо с цел установяване, упражняване или защита на правни претенции;

- Обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните;

- Обработването е необходимо за оценка на трудоспособността на служителя. Тези лични данни се обработват от или под ръководството на професионален работник, обвързан от задължението за професионална тайна по силата на правото на Съюза или правото на държава членка или правилата, установени от националните компетентни органи или от друго лице, също обвързано от задължение за тайна по силата на правото на Съюза или

правото на държава членка или правилата, установени от националните компетентни органи.

IV. ПРОЦЕДУРИ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 11. (1) Личните данни отнасящи се до лицата, заемащи служебни, трудови или граждански правоотношения в ОА Сливен, както и на кандидатите за работа, се събират при и по повод набирането на служители, персонал. Данните на всеки работник и служител на администрацията се съхраняват в лични досиета, като някои данни могат да се съхраняват или обработват и на технически носител. Данните от проведени конкурси и интервюта се съхраняват на технически и/или хартиен носител, в зависимост от нуждата, на сигурно, безопасно и недостъпно за външни лица място.

(2) Личните досиета се подреждат в специални картотечни шкафове.

(3) Лицата, обработващи лични данни, предприемат всички организационно технически мерки за съхраняването и опазването на лични досиета и класъорите с информация, в това число ограничаване на достъпа до тях на външни лица и неоторизирани служители.

(4) Досиетата на работниците и служителите, както и данните на кандидатите за работа, не се изнасят извън сградата на Областна администрация Сливен, освен ако закон или друг нормативен акт изисква това.

Чл. 12. (1) Личните данни, отнасящи се до потребители на услуги/граждани, се събират при подаване на заявление за предоставяне на услуга, при подаване на жалба, искане за издаване на удостоверение, предложение, сигнал, или сключване на договор с потребители на услуги на Областна администрация Сливен.

(2) Личните данни на гражданите се събират, обработват, съхраняват, предоставят на трети лица, унищожават/заличават, изтриват, съгласно утвърдените и влезли в сила със Заповед на областния управител вътрешни правила.

Чл. 13. Личните данни, отнасящи се до доставчици на услуги, се събират при сключване на договор с доставчик на услуги, като обичайно личните данни се съдържат в текста на самите договори.

Чл. 14. Личните данни се съхраняват на електронен и/или хартиен носител (подписани копия на сключените договори), които се класират в отделни досиета. Електронните данни се съхраняват в бази данни.

Чл. 15. (1) Областна администрация Сливен работи и функционира на базата на Закона и подзаконовите нормативни актове в страната и извършва дейност в рамките на предоставените ѝ от Закона компетенции, в тази връзка не е необходимо администрацията да търси/иска съгласие от гражданите за обработване на лични данни, както и да предоставя на гражданите декларации за съгласие за обработване на личните им данни. Съгласието не следва да бъде упражнявано по отношение на администратори, обработващи данни в изпълнение на обществените си задължения.

(2) Когато личните данни се обработват съгласно закона и обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официално правомощие, предоставено на администратора, или по съображения, свързани със законните интереси на администратора или на трета страна, всеки субект на данни има право на възражение срещу обработването на лични данни, свързани с неговото конкретно положение. Администраторът следва да докаже, че неговите неоспорими законни интереси имат преимущество пред интересите или основните права и свободи на субекта на данни.

V. ЛИЦА, ОТГОВАРЯЩИ ЗА СЪБИРАНЕТО, ОБРАБОТКАТА И СЪХРАНЕНИЕТО НА ЛИЧНИТЕ ДАННИ И ДОСТЪП ДО ЛИЧНИ ДАННИ

Чл. 16. Длъжностното лице по защита на личните данни, и лицата, обработващи личните данни от името на Областна администрация Сливен, са физически лица, притежаващи необходимата компетентност и назначени и/или упълномощени със съответен писмен акт.

Чл. 17. Длъжностното лице по защита на личните данни:

(1) подпомага администрацията и лицата, обработващи личните данни при изпълняване на задълженията им по защита на личните данни, като осигурява прилагането и поддържа необходимите технически и организационни мерки и средства за осъществяване на защитата на данните;

(2) осигурява нормалното функциониране на системите за защита;

(3) осъществява контрол през целия процес на събиране и обработване на данните;

(4) изпълнява всички задължения по докладване и управление на нарушения на сигурността на данните;

(5) периодично изисква информация от лицата, обработващи лични данни, във връзка със събирането, достъпа и обработването им;

(6) уведомява ръководството на администрацията своевременно за всички нередности, установени във връзка с изпълнение на задълженията му.

Чл. 18. (1) Събирането, обработката, съхранението и защитата на личните данни се извършва от лица, на които това е изрично указано и чиито служебни задължения или конкретно възложена задача налагат това.

(2) При възлагане на дейности, налагащи обработката на лични данни от регистрите на администрацията, гражданите, доставчиците на услуги следва да спазват приложимите нормативни изисквания относно обработката на личните данни.

(3) Достъп до личните данни могат да имат и съответните държавни органи – съд, следствие, прокуратура, ревизиращи органи и др. Същите могат да изискат данните по надлежен ред във връзка с изпълнението на техните правомощия.

(4) Ограничения в обхвата на задълженията и правата на гражданите във връзка със защитата на личните данни са на лице в случаите със значение за:

1. националната сигурност;

2. отбраната;

3. обществената сигурност;

4. предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност;

5. предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регламентираните професии;

6. защитата на субекта на данните или на правата и свободите на други лица;

7. изпълнението по гражданскоправни искове.

VI. МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 19. Технически мерки

(1) Всички помещения, в които се съхраняват и обработват лични данни, са с контрол на достъпа (ключалки).

(2) Сградата на Областна администрация Сливен е надеждно обезопасена посредством противопожарни мерки съгласно българското законодателство.

(3) В сградата на Областна администрация Сливен се извършва непрекъсната 24 часова охрана: назначени са лица по пропускателния режим и охрана, те са отговорни за организацията и спазването на пропускателния режим и вътрешния ред в сградата на администрацията, както и главният експерт по отбранително - мобилизационна подготовка и отговорник за пожарната и аварийна безопасност и физическата сигурност в сградата.

Чл. 20. Мерки за документална защита

(1) Областна администрация Сливен има установени процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение на документи.

(2) Размножаването и разпространението на документи или файлове, съдържащи лични данни, се извършва при възникнала необходимост.

(3) На хартиен носител се съхраняват всички лични данни, които изискват попълването им върху определени бланкови документи и/или формуляри, свързани с изпълнение на изискванията на действащото законодателство или пряко свързани с осъществяването на нормалната дейност на Областна администрация Сливен, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения.

(4) Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на администрацията или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (напр. изгаряне, нарязване - шредер, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

Чл. 21. Преди заемане на съответната длъжност лицата, които обработват лични данни:

1. поемат задължение за неразпространение на личните данни, до които имат достъп;

2. се запознават с нормативната база, вътрешните правила и политики на Областна администрация Сливен относно защитата на личните данни, документооборота в администрацията, Вътрешни правила на администрацията и др.;

3. се задължават да не споделят критична информация помежду си и с външни лица, освен по установения с тези Правила ред.

Чл. 22. Мерки за защита на автоматизирани информационни системи

(1) Защитата на автоматизираните информационни системи и/или мрежи в администрацията включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват данни.

(2) Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, включват:

1. Идентификация и автентификация чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на администрацията. Прилагането на тази мярка е с цел да се регламентират нива на достъп;

2. Управление на документите, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка;

3. Управление на връзки и/или свързване, включващо от своя страна:

- Дефиниране на обхвата на вътрешните мрежи: Като вътрешни мрежи се разглеждат всички локални жични мрежи и/или телекомуникационни връзки тип „точка – точка“, които се намират под контрола и администрацията на Областна администрация Сливен. Като външни мрежи се разглеждат всички мрежи, вкл. и безжични мрежи, интернет.

- Регламентиране на достъпа до вътрешната мрежа: Достъп до вътрешната мрежа имат единствено служителите и/или специално упълномощени от Областния управител лица. Достъпът до мрежата и обработваните лични данни се предоставя с оглед изпълнение на техните преки служебни задължения. Минимално изискваното ниво на сигурност за достъп до вътрешните мрежи изисква идентифициране с уникално потребителско име и парола.

- Администриране на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на достъпа, са възложени на лица с необходимата квалификация. В отговорностите са включени и дейности, свързани с одобряване на инсталирането на всички устройства, технологии и софтуер за достъп до мрежата, включително суичове, рутери, безжични точки за достъп, точки за достъп до мрежата, интернет връзки, връзки към външни мрежи и други устройства, технологии и софтуер, които могат да позволят достъп до вътрешните мрежи на Администратора.

- Контрол на достъпа до вътрешната мрежа: Отговорностите, свързани с осъществяване на контрола на достъпа са възложени на лица с необходимата квалификация. Те са задължени да предприемат адекватни мерки за минимизиране на риска от неоторизиран (физически и/или отдалечен) достъп до мрежите на администрацията, вкл. и чрез използване на защитни стени и други адекватни мерки и инструменти.

4. Защитата от зловреден софтуер включва:

- използването на стандартни конфигурации за всяка компютърна и/или мрежова платформа, като системният, а при възможност и приложният, софтуер се контролира, инсталира и поддържа от оторизирани от Ръководството на Областна администрация Сливен лица. Забранено е инсталирането на софтуерни продукти без изричното одобрение на ИТ специалиста на администрацията.

- използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от оторизирани от Ръководството лица. Всяка промяна и/или деактивация на системите за защита от неоторизирани лица е забранена.

- активиране на автоматична защита и сканиране за зловреден софтуер и обновяване на антивирусни дефиниции. Забранено е потребителите да отказват автоматични софтуерни процеси, които актуализират вирусните дефиниции.

- забрана за пренос на данни от заразени компютри. При съмнение или установяване на заразяване на компютърна система работещият с нея е задължен да уведоми оторизираните в администрацията лица и да преустанови всякакви действия за работа и/или изпращане на информация от заразения компютър (чрез външни носители, електронна поща и/или други способи за електронна обмяна на информация). До премахване на зловредния софтуер заразеният компютър следва да бъде незабавно изключен от вътрешните мрежи.

5. Политика по създаване и поддържане на резервни копия за възстановяване, която регламентира:

- Основната цел на архивирането е свързана с предотвратяване на загуба на информация, свързана с лични данни, която би затруднила нормалното функциониране на администрацията.

- Начина на архивиране: информацията се архивира по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на повреда на техния основен носител.

- Срокът на архивиране следва да е съобразен с действащото законодателство.

- Всички архиви, съдържащи конфиденциална и/или служебна информация, се съхраняват с физически контрол на достъпа

6. Основни електронни носители на информация са: вътрешни твърди дискове (част от компютърна и/или сторидж система), еднократно и/или многократно презаписваеми външни носители (външни твърди дискове, многократно презаписваеми карти и други носители на информация, еднократно записваеми носители и др.)

7. Персоналната защита на данните е част от цялостната охрана на Областна администрация Сливен.

8. Личните данни в електронен вид се съхраняват съгласно нормативно определените срокове и съобразно спецификата и нуждите.

(3) Мерките, свързани с текущото поддържане и експлоатация на информационните системи и ресурси на ОА Сливен, включват:

- Оценка на сигурността, включваща периодични тестове и оценки на уязвимостта на мрежите и системите на администрацията от външни и вътрешни атаки (Vulnerability test), включително оценка на въздействието, адекватността на използваните мерки и способности за защита, както и препоръки за нейното техническо и организационно подобряване. Оценката включва посочените аспекти и по отношение сигурността на събираните, обработвани и съхранявани лични данни.

- Забрана за притежание и ползване на хардуерни или софтуерни инструменти от персонала, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Към тази група се отнасят и инструменти, способстващи за нарушаване на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Забранено е използването и на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър.

(4) Мерките, свързани със създаване на физическа среда (обкръжение), включват физически контрол на достъпа (ключалки, метални решетки и други приложими способности), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност. Те са насочени към осигуряване на среда за нормално функциониране, за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

VII. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 23. (1) Областна администрация Сливен може при необходимост да предоставя лични данни на трети лица, действащи в качеството на администратор на лични данни, въз основа на законово основание и нужда от това.

(2) В случаите на предоставяне на данните на трети страни, Областна администрация Сливен:

1. изисква достатъчно гаранции от администратора/обработващия за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни, освен когато съответното трето лице е организация, която осъществява своята дейност по силата на закона и ѝ е вменено законово задължение или обработва лични данни на базата на обществен интерес;

2. ако е необходимо сключва писмено споразумение или друг правен акт с идентично действие, който урежда задълженията на обработващия и отговаря на изискванията на чл. 28 от Регламент (ЕС) 2016/679.

VIII. ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

Чл. 24. (1) Оценка на въздействието се извършва, когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни, извършвана от Областна администрация Сливен. Оценка на въздействието се извършва за високорискови дейности по обработване.

(2) Оценка на въздействието е необходимо при всяко въвеждане на ключова система или смяна на бизнес програма, която е свързана с обработване на лични данни, включително:

1. първоначалното въвеждане на нови технологии или прехода към нови технологии;
2. автоматизирано обработване, включително профилиране или автоматизирано вземане на решения (експертни системи);
3. обработване на чувствителни лични данни в голям мащаб;
4. мащабно, систематично наблюдение на публично обществена зона;

(3) За оценката се съставя протокол, който се предоставя при поискване от страна на КЗЛД.

IX. УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл. 25. (1) Унищожаване на личните данни се извършва от Областна администрация Сливен и/или от изрично упълномощено лице, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването, и при спазване на относимите нормативни разпоредби.

(2) Информацията се унищожава след постигане на целите на обработката и при отпаднала необходимост за съхранение.

(3) Унищожаването на данни на хартиен носител се извършва чрез нарязване с шредер машина или изгаряне. Електронните данни се изтриват от електронната база данни по начин, непозволяващ възстановяване на информацията.

X. НАРУШЕНИЯ НА СИГУРНОСТТА

Чл. 26. (1) Лицата, идентифицирали признаци на нарушение на сигурността на данните, са длъжни да докладват незабавно на Длъжностното лице по защита на личните данни, като му предоставят цялата налична информация.

(2) Длъжностното лице по защита на личните данни, извършва незабавно проверка по подадения сигнал, като се опитва да установи дали е осъществено нарушение на сигурността и кои данни са засегнати.

(3) Длъжностното лице по защита на личните данни, докладва незабавно на ръководството на Областна администрация Сливен - наличната информация за нарушението на сигурността, включително информация относно характера на инцидента,

времето на установяването му, вида на щетите, предприетите към момента мерки и мерките, които счита, че трябва да се предприемат.

(4) След съгласуване с ръководството на Областна администрация Сливен, Длъжностното лице по защита на личните данни, предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

Чл. 27. (1) В случай че нарушението на сигурността създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, и след одобрение от ръководството на Областна администрация Сливен, Длъжностното лице по защита на личните данни, организира уведомяването на КЗЛД.

(2) Уведомяването на КЗЛД следва да се извърши без ненужно забавяне и когато това е осъществимо не по-късно от 72 часа след първоначалното узнаване на нарушението.

(3) Уведомлението до КЗЛД съдържа следната информация:

1. описание на нарушението на сигурността, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

2. името и координатите за връзка на длъжностното лице по защита на личните данни;

3. описание на евентуалните последици от нарушението на сигурността;

4. описание на предприетите или предложените мерки за справяне с нарушението на сигурността, включително мерки за намаляване на евентуалните неблагоприятни последици.

(4) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Длъжностното лице по защита на личните данни, без ненужно забавяне и при спазване на приложимото законодателство уведомява засегнатите физически лица.

Чл. 28. (1) Областна администрация Сливен води регистър на нарушенията на сигурността, който съдържа следната информация:

1. дата на установяване на нарушението;

2. описание на нарушението - източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо);

3. описание на извършените уведомявания: уведомяване на КЗЛД и засегнатите лица, ако е било извършено;

4. предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни и за Областна администрация Сливен;

5. предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.

(2) Регистърът се води в електронен формат от Длъжностното лице по защита на личните данни.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Ръководителите и служителите в Областна администрация Сливен са длъжни да познават и спазват разпоредбите на настоящите правила.

§2. Контролът по спазване на разпоредбите във Вътрешните правила за събиране, обработване, съхраняване и защита на личните данни се осъществява от главния секретар на Областна администрация Сливен.

§3. Настоящите правила се утвърждават със Заповед № РД-11-06-002/2018 г. и на основание чл. 4, параграф 20 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година и във връзка със Закона за защита на личните данни

Регистър на нарушенията на сигурността

съгласно чл. 30 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г.

Администратор:

Областна администрация Сливен
гр. Сливен
ул. „Димитър Добровиц“ № 3
тел.: 044/66 32 02
факс: 044/61 66 99
<http://www.sliven.government.bg>

Длъжностно лице по защита на лични данни:

Антония Желева
Старши експерт
Дирекция „Административен контрол, регионално развитие и държавна собственост“
тел.: 044/61 66 73
e-mail: zheleva@regionsliven.com

№	Дата на установяване на нарушението	Описание на нарушението	Описание на извършените уведомявания	Предприети мерки за предотвратяване и ограничаване на последните	Предприети мерки за ограничаване на последващи нарушения