РЕПУБЛИКА БЪЛГАРИЯ
Областна администрация
Смолян

Смолян, бул. "България"№14, тел.0301/ 60192,факс 0301/ 62333, e-mail: governor@region-smolyan.org; http://www.sm.government.bg

УТВЪРДИЛ:

НЕДЯЛКО СЛАВОВ
ОБЛАСТЕН УПРАВИТЕЛ
НА ОБЛАСТ СМОЛЯН

ОБЛАСТ * ОБЛАСТЕН УПРАВИТЕЛ * СМОЛЯН

ВЪТРЕШНИ ПРАВИЛА ЗА ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ И ДОПУСТИМИЯ ВИД НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ОБЛАСТНА АДМИНИСТРАЦИЯ – СМОЛЯН

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящите вътрешни правила за технически и организационни мерки и допустимия вид на защита на личните данни, наричани за краткост „Правилата", уреждат организацията на обработване на лични данни и тяхната защита на служители, граждани, кандидати за работа, потребители и доставчици на услуги в Областна администрация - Смолян.

(2) В зависимост от конкретната ситуация, Областна администрация – Смолян 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 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).

Чл. 2. (1) Обработването на лични данни е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхранение, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване или предаване, разпространяване, актуализиране или комбиниране, блокиране, заличаване или унищожаване на данните.

(2) Обработването на лични данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.

Чл. 3 (1) Лични данни са 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.

(2) Принципите за защита на лични данни са:

- Принцип на ограниченото събиране – събирането на лични данни трябва да бъде в рамките на необходимото. Информацията се събира по законен и обективен начин;
- Принцип на ограниченото използване, разкриване и съхранение – личните данни не трябва да се използват за цели, различни от тези, за които са били събирани, освен със съгласието на лицето или в случаите, изрично предвидени в закона. Личните данни трябва да се съхраняват само толкова време, колкото е необходимо за изпълнението на тези цели;
- Принцип на прецизност – личните данни трябва да са прецизни, точни, пълни и актуални, доколкото това е необходимо за целите, за които се използват;
- Принцип на сигурността и опазването – личните данни трябва да са защитени с мерки за сигурност, съответстващи на чувствителността на информацията.

Чл. 4. (1) Личните данни се събират за конкретни, точно определени от закона цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

(2) При обработване на личните данни от Областна администрация - Смолян служителите подписват декларация за съгласие – Приложение № 1, а гражданите, кандидатите за работа, потребителите и доставчици на услуги – Приложение № 2.

Чл. 5. Настоящите Правила уреждат:

(1) Принципите, процедурите и механизмите за обработка на личните данни;

(2) Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността;

(3) Процедурите за администриране на искания за достъп до данни, коригиране на обработваните данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат по закон;

(4) Лицата, които обработват лични данни и техните задължения;

(5) Правилата за предаване на лични данни на трети лица в страната и чужбина;

(6) Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване и в случай на инциденти, като случайно или незаконно унищожаване, загуба, неправомерен достъп, изменение или разпространение;

(7) Технически ресурси, прилагани при обработката на лични данни.

II. ПОНЯТИЯ И ДЕФИНИЦИИ

Чл.6. За целите на настоящите Правила, използваните понятия имат следното значение:

- ЗЗЛД - Закон за защита на личните данни.
- КЗЛД - Комисия за защита на личните данни.
- ОРЗД /GDPR/- 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).
- Длъжностно лице по защита на данните /DPO/ - физическо лице или организация, определени съгласно изискванията на чл. 37 и сл. от ОРЗД.
- Администратор на лични данни - физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни. В настоящите Правила „администратор“ обозначава Областна администрация - Смолян.
- Обработващ лични данни - лице или организация, което въз основа на договор/заповед обработва лични данни, предоставени от Областна администрация - Смолян, за уговорените цели.
- Известия по защита на данните - отделни известия, съдържащи информация, предоставяна на субектите на данни в момента, в който Областна администрация – Смолян събира информация за тях. Тези известия могат да бъдат както общи (напр. адресирани към работници и служители или известия на уебсайта на организацията), така и отнасящи се до обработване със специфична цел.
- Обработване на данни - всяка дейност, която е свързана с използването на лични данни. Това включва: получаване, записване, съхранение, извършване на операция или серия от операции с данните като напр. организиране, редактиране, възстановяване, използване, предоставяне, изтриване или унищожаване. Обработването също включва и трансфер на лични данни до трети лица.
- Псевдоминизиране - заместването на информация, която директно или индиректно идентифицира физическо лице, с един или повече идентификатори („псевдоними”), така че лицето да не може да бъде идентифицирано без достъп до допълнителната информация, която следва да се съхранява отделно и да е поверителна.
- Съгласие - всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данни, посредством изявление или ясно потвърждаващо действие, което изразява съгласие за обработка на лични данни, свързани с него.

III. СУБЕКТИ НА ДАННИ И КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 7. (1) Областна администрация - Смолян 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 - Смолян, са групирани в регистри на дейностите по обработване, съдържащи правила и политики за обработване на лични данни, отнасящи се до:

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

(2) Относно гражданите Областна администрация - Смолян, събира: три имена, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, имейл, данни по лична карта или паспортни данни и др. данни, необходими за осъществяване функциите на администрация, съгласно закона.

(3) Относно лицата, заети по служебни, трудови или граждански правоотношения в Областна администрация – Смолян, и на кандидатите за работа, се води регистър „Персонал" и се събират следните лични данни, съгласно приложимата нормативна уредба (ЗДСл, КТ, КСО, КДА, Наредба за провеждане на конкурсите за държавни служители, Наредба за документите за заемане на държавна служба, Наредба за служебното положение на държавните служители, Наредба за условията е реда за оценяване изпълнението на служителите в държавната администрация, Наредба №4 за документите, които са необходими за сключване на трудов договор съгласно чл. 62, ал.2 КТ и др.):

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

б) Образование и професионална квалификация; данни, свързани с образование, трудов опит, професионална и лична квалификация и умения;

в) Здравни данни: здравословно състояние, ТЕЛК решения, медицински свидетелства, болнични листове и всяка прилежаща към тях документация, необходими съгласно приложимия Закон- ЗДСЛ, КТ, КСО, ЗЗ;

г) Други данни: свидетелство за съдимост, когато се изисква представянето му съгласно нормативен акт, както и други данни, чието обработване е необходимо за изпълнение на правата и задълженията на Областна администрация - Смолян като работодател.

(4) Относно физически лица, потребители на услугите на Областна администрация – Смолян, се събират лични данни, които са необходими за изпълнението на законовите задължения на администрацията, като доставчик на услуги, както следва:

• име, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни.

(5) Относно физически лица, доставчици на услуги на Областна администрация - Смолян, се съхраняват лични данни, необходими за сключването и изпълнението на договори за предоставяне на услуги на администрацията от външни доставчици, както следва:

• име, ЕГН (дата на раждане), постоянен и/или настоящ адрес, телефон, данни по лична карта или паспортни данни; електронна поща.

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

IV. ЦЕЛИ И ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 8. Целите на обработването на лични данни са:

(1) свързани с дейността на Областна администрация - Смолян 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, молби, 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 за удържане и плащане на здравни и социални осигуровки на служителите, на данъци, както и на други права и задължения на Областна администрация - Смолян в качеството ѝ на работодател;

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

(3) сключване и изпълнение на договори с доставчици за предоставяне на услуги на Областна администрация – Смолян

Чл. 9. Личните данни се обработват законосъобразно, добросъвестно и прозрачно при спазване на следните принципи:

(1) Областна администрация – Смолян обработва лични данни на граждани, когато трябва да се спазят и изпълнят законови задължения; когато това е необходимо за нуждите на администрацията (или на трета страна) легитимен интерес, освен когато основни интереси или основни права и свободи на гражданите имат преимущество пред такива интереси; когато е необходимо да защитим жизненоважни интереси на граждани; и/или когато това е необходимо в обществен интерес или за упражняването на официални правомощия.

(2) Субектът на данните се информира предварително за обработването на неговите лични данни;

(3) Личните данни се събират за конкретни, точно определени законни цели и не се обработват допълнително по начин, несъвместим с тези цели;

(4) Личните данни съответстват на целите, за които се събират;

(5) Личните данни трябва да са точни и при необходимост да се актуализират;

(6) Личните данни се заличават или коригират, когато се установи, че са неточни или не съответстват на целите, за които се обработват;

(7) Гражданите могат да искат потвърждение относно обработването на личните им данни от администрацията, копие от личните им данни и/или да поискат да ги коригират.

(8) При определени обстоятелства гражданите имат правото да изискат от администрацията да изтрие личните им данни или въз основа на правото на преносимост да поискат Областна администрация – Смолян да им предаде някои от личните данни на тях или на други лица.

(9) Гражданите имат право да възразят срещу обработването на личните им данни.

(10) Когато Областна администрация – Смолян е поискала съгласието за обработване на личните данни на граждани, те имат право да оттеглят това съгласие, без неблагоприятни последици.

(11) Гражданите имат право да възразят и когато администрацията обработва личните им данни на основание легитимен интерес.

(12) Гражданите имат право, при определени обстоятелства, да ограничат обработването на личните им данни. Правата на гражданите в тази връзка, могат да бъдат ограничени в определени случаи, съгласно приложимото законодателство.

(13) Личните данни се поддържат във вид, който позволява идентифициране на съответните физически лица за период, не по-дълъг от необходимото, за целите, за които тези данни се обработват.

Чл. 10. За да е законосъобразно обработването на данните е необходимо:

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

б) 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;

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

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

е) 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. Буква е) не се прилага за обработването, което се извършва от публични органи при изпълнението на техните задачи.

V. СЪГЛАСИЕ

Чл. 11. (1) Областна администрация – Смолян 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. Съгласно ОРЗД и когато обработването се базира на правно основание, различно от съгласие или договор. Съгласието не следва да бъде упражнявано по отношение на администратори, обработващи данни в изпълнение на обществените си задължения. Ето защо това право не следва да се прилага, когато обработването на личните данни е необходимо за спазване на правно задължение, на което е подчинен администраторът, или за изпълнение на задача от обществен интерес, или при упражняване на официално правомощие, предоставено на администратора.

(2) Когато личните данни биха могли да се обработват законно, тъй като 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 следва все пак да 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.

VI. ПРОЦЕДУРИ ПО ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Процедура за обработване на личните Данни, отнасящи се до лицата, заети по служебни, трудови или граждански правоотношения в администрацията, както и на кандидатите за работа

Чл. 12. (1) Личните данни, отнасящи се до лицата, заемащи служебни, трудови или граждански правоотношения в Областна администрация - Смолян, 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, обезопасено и недостъпно за външни лица място.

(2) Личните досиета и данните на кандидатите за работа на хартиен носител се подреждат в специален метален шкаф, намиращ се в кабинета на главен експерт „Човешки ресурси". Достъпът до кабинета се предоставя само на длъжностното лице/обработващ на лични данни и отговарящ за човешките ресурси в администрацията.

(3) Лицата, обработващи лични данни, предприемат всички организационно технически мерки за съхраняването и опазването на личните досиета и класьорите 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 администрацията, освен ако закон или друг нормативен акт изисква това.

(5) Процедурата за обработване на личните данни е подробно разписана във Вътрешни правила за възникване, изменение и прекратяване на служебните и трудови правоотношения на Областна администрация - Смолян.

Процедура за обработване на лични данни, отнасящи се до потребители/граждани и доставчици на услуги

Чл. 13. (1) Личните данни, отнасящи се до потребители на услуги/граждани, се събират при подаване на заявление за предоставяне на услуга, при подаване на молба,
жалба, искане за издаване на удостоверение, предложение, сигнал, или сключване на договор с потребители на услуги на Областна администрация - Смолян.

(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 следните вътрешни нормативни документа: Вътрешни правила относно, документооборота, Номенклатурата на делата със срокове за съхранение, Вътрешните правила за организация на работа, опазване, съхранение и използване на архивен фонд на отдел „Устройство на територията и държавна собственост" в Областна администрация - Смолян, Вътрешни правила за дейността на учрежденския архив в Областна администрация-Смолян, Вътрешни правила за провеждане на инвентаризация на дълготрайните и краткотрайни активи в Областна администрация - Смолян, Вътрешни правила за поддържане на интернет страницата на Областна администрация - Смолян, Вътрешни правила за определянето нивото на класификация на информацията и за неговата промяна или премахване, Вътрешни правила за предоставяне на достъп обществена информация, Инструкция за организиране на пропускателния режим и вътрешния ред в сградата на Областна администрация - Смолян, Инструкция за информационното обслужване в Областна администрация - Смолян, Процес на физическа и информационна сигурност, Етичен кодекс за поведение на служителите в Областна администрация - Смолян.

(3) 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.

(4) 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.

(5) Обработването на лични данни е предназначено да служи на гражданите. Правото на защита на личните данни не е абсолютно право, а трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа на пропорционалност.

VII. ДОКУМЕНТИРАНЕ НА ОБРАБОТКАТА НА ЛИЧНИ ДАННИ

Чл. 14. (1) Областна администрация - Смолян документира дейностите по обработване на лични данни при спазване на принципите заложени във вътрешната нормативна уредба.

(2) Документацията трябва да е достатъчна, за да докаже спазването на принципите за законосъобразно обработване на личните данни.

(3) Обработването на данни, свързано с предаване на данни на обработващи, установени в страната или чужбина; съхранение на данни на сървъри, собственост на трети лица; архивиране или изтриване на данни; въвеждане на псевдонимизация, както и всяка друга обработка, чиито параметри са различни от описаните в тези правила, се документира чрез създаване на протоколи, които съдържат следната информация:

(а) целите на обработването;

(б) категориите лични данни и категориите субекти на данни;

(в) категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави;

(г) предаването на лични данни на трета държава;

(д) когато е възможно, предвидените срокове за изтриване на различните категории данни;

(е) общо описание на техническите и организационни мерки за сигурност.

VIII. МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Областна администрация - Смолян, разполага с разработени, утвърдени и работещи Вътрешни правила с посочени в тях правила относно защитата на личните данни в Областна администрация - Смолян,

Технически мерки

Чл. 15. (1) Всички помещения, в които се съхраняват и обработват лични данни, са с контрол на достъпа.

(2) Сградата на Областна администрация – Смолян е надеждно обезопасена посредством противопожарни мерки и пожароизвестителна система съгласно българското законодателство.

(3) В сградата на Областна администрация – Смолян се извършва непрекъсната 24 часова охрана, задължени лица по пропускателния режим и охраната са информаторът- пропускар и постовият от охраната, отговорни лица относно организацията и спазването на пропускателния режим и вътрешния ред в сградата на администрацията са: главният експерт по отбранително-мобилизационна подготовка и отговорник за пожарната и аварийна безопасност и физическата сигурност в сградата.

(4) Областна администрация – Смолян сключва договор за охрана със СОТ срещу заплащане, съгласно чл.5, ал.1, т.2 от Закона за частната охранителна дейност за защита от престъпни посегателства на имуществото на администрацията, намиращо се в охранявания обект, при която чрез монтиране, поддържане и използване на сигнално-охранителни известителни системи се осъществява наблюдение на обекта.

Мерки за документална защита

Чл.16. (1) Областна администрация – Смолян установява процедури по обработване на лични данни, регламентиране на достъпа до данните, процедури по унищожаване и срокове за съхранение, подробно разписани във Вътрешни правила за документооборота.

(2) Размножаването и разпространението на документи или файлове, съдържащи лични данни, се извършва само и единствено от упълномощени служители 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 нормалното дейност на Областна администрация - Смолян, сключване на договори, изпълнение на договори, упражняване на предвидени в закона права и установени от закона задължения;

(4) Личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения е/или нормалната бизнес дейност на администрацията, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;

(5) Достъпът до документите с лични данни е ограничен и се предоставя само на упълномощени служители, в съответствие с принципа на „Необходимост да се знае“;

(6) Личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок;

(7) 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 машина, електронно изтриване и други подходящи за целта методи, съобразени с физическия носител на данните).

(8) Личните данни, оценени с по- висока степен на риск, освен мерките по-горе се прилагат и следните допълнителни мерки:

1. Контрол на достъпа до документите, ограничаващ достъп на персонала или в ограничени случаи на други специално упълномощени лица, в съответствие с принципа „Необходимост да знае“, за да изпълняват техните задължения;

2. Правила за размножаване и разпространение, които разрешават копиране и разпространяване на лични данни единствено в случаите, когато това е необходимо за юридически нужди, възниква по изискване на закон и/или държавен орган, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на дисциплинарни санкции и други мерки, ако представлява и друг вид нарушение, освен нарушение на трудовата дисциплина.

Персонални мерки на защита

Чл. 17. (1) Преди заемане на съответната длъжност лицата, които осъществяват защита и обработване на личните данни:

(а) поемат задължение за неразпространение на личните данни, до които имат достъп (попълват Декларация за поверителност);

(б) се запознават с нормативната база, вътрешните правила и политики на Областна администрация - Смолян относно защитата на личните данни, документооборота в администрацията, Номенклатурата на делата, Вътрешни правила за организацията на работа, опазване, съхранение и използване на архивен фонд на отдел „Устройство на територията и държавна собственост“ в Областна администрация - Смолян и др.;

(в) преминават обучение за реакция при събития, застрашаващи сигурността на данните;

(г) са инструктирани за опасностите за личните данни, които се обработват от Областна администрация - Смолян;

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

(2) При постъпване на работа всички служители преминават обучение за реакция при събития, застрашаващи сигурността на данните, и обучение относно задълженията на администрацията, свързани с обработката на лични данни, и мерките за защита на данните, които следва да предприемат в процеса на работа. Последващи обучения и тренировки на персонала се провеждат периодично, за да се гарантира познаване на нормативната уредба, потенциалните рискове за сигурността на данните и мерките за намаляването им.

Мерки за защита на автоматизирани информационни системи и криптографска защита

Чл.18. (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, включван:

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 и да се въведе достъп, съобразен с принципа „Необходимост да знае“;

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, поддържка и обработка;

3. Управление на външни 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 на Областна администрация -Смолян. Като външни мрежи се разглеждат всички мрежи, вкл. и безжични мрежи, интернет, интернет връзки, мрежови връзки с трети страни, мрежови сегменти на хостинг системи на трети страни, които не са под административния контрол на Областна администрация – Смолян..

• 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 и е съобразен с принципа „Необходимо да знае“. Минималното 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 администрация 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 минимализиране 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 - Смолян лица. Забранено е инсталирането на софтуерни продукти без изричното одобрение на ИТ специалиста на администрацията след разрешение от областния управител..

• използване на вградената функционалност на операционната система и/или хардуера, които се настройват единствено от оторизирани от ръководството на Областна администрация - Смолян 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 от ръководството на 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 изолиран 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 Областна администрация – Смолян.

• Начина на архивиране: информацията следва да бъде архивирана по подходящ способ и на носител, извън конкретния физически компютър, и да позволява пълното възстановяване на данните, в случай на погиване на техния основен носител.

• Отговорност за архивиране има лицето, обработващо личните данни.

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

• Съхраняването на архива следва да бъде в друго физическо помещение. Всички архиви, съдържащи поверителна и/или служебна информация, трябва да 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, памети ленти и други носители на информация, еднократно записваеми носители.

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

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

9. Данните, които вече не са необходими за целите на Областна администрация – Смолян и чийто срок за съхранение е изтекъл, се унищожават чрез приложим способ (напр. чрез нарязване, изгаряне или постоянно заличаване от електронните средства).

(3) За лични данни, оценени с по-висока степен на риск, освен мерките по ал. 2 се прилагат и допълнителни мерки, свързани с:

1. Организация на телекомуникационните връзки и отдалечения достъп до вътрешните мрежи на администрацията:

• Отдалечен достъп до вътрешни мрежи на Областна администрация – Смолян не е предвиден. По изключение, и след изричната оторизация от ръководството на администрацията, може да се

разреши подобен достъп от оторизираните лица, като за целта се използват адекватни и приложими съвременни методи за защита на връзката и обменяните данни.

• На служителите от Областна администрация - Смолян може да бъде предоставен Интернет достъп (отдалечен достъп) за изпълнение на служебните им задължения до електронните регистри с лични данни. Обхватът на достъпа и типа достъпни ресурси (вкл. сайтове, файлове, услуги и др.) се определя по преценка и предложение на преките ръководители, съгласувано и одобрено с оторизираните от ръководството на администрацията лица за степента на осъществимост, в пряка връзка с изпълняваните задължения и свързаните с този достъп рискове и след становище на длъжностното лице по регистрация. Отдалечен достъп чрез Интернет до определени ресурси, вкл. и вътрешните такива, може да бъде прекратен по всяко време по преценка на ръководството на администрацията, както и в случаите на заплаха за сигурността на данните.

• Публикуването на служебна информация в Интернет, независимо от формата на документите, се извършва единствено след писмена оторизация от ръководството на администрацията.

2. Мерките, свързани с текущото поддържане и експлоатация на информационните системи и ресурси на Областна администрация - Смолян, 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 способи 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 служителите на Областна администрация - Смолян, 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. За неоторизирано използване на подобни инструменти служителят се наказва дисциплинарно, а ако нарушението представлява престъпление – по предвидения за санкциониране на това нарушение/престъпление ред.

3. Мерките, свързани със създаване на физическа среда (обкръжение), включват физически контрол на достъпа (сигнално-охранителна техника, ключалки, метални решетки и други приложими способи), създаване на подходяща работна среда, вкл. чрез поддържане на подходяща температура и нива на влажност, както и пожароизвестителна система. 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.

(4) По отношение на личните данни се прилагат и мерки, свързани с криптографска защита на данните чрез стандартните криптографски възможности на операционните системи, на системите за управление на бази данни и на комуникационното оборудване. Криптирането се използва и за защита на личните данни, които се предават от Областна администрация – Смолян по електронен път или на преносими носители.

Чл.19. (1) Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване, извършени умишлено от лице или в случай на технически неизправности, аварии, произшествия, бедствия, др., се осигурява посредством:

1. периодични проверки на целостта на базата данни и актуализиране на системната информация, поддържане на системата за достъп до данните;

2. архивиране на данните на технически носители, съгласно Политика за резервиране и архивиране на информацията, според нормативно определените срокове, поддържане на информацията на хартиен носител (архивни копия).

3. Лицето, отговорно за личните данни, докладва на ръководството на Областна администрация - Смолян за предприетите мерки за гарантиране нивото на сигурност при обработване на лични данни.

4. Областна администрация - Смолян е утвърдила „Политика за поверителност при ползване на уебсайта на Областна администрация - Смолян“.

IX. НАРУШЕНИЯ НА СИГУРНОСТТА

Чл.20. (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 – Смолян наличната информация за нарушение 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 - Смолян, длъжностното лице по защита на личните данни, предприема мерки за предотвратяване или намаляване последиците от пробива и възможностите за възстановяване на данните.

(5) При спешност, когато съгласуване с ръководството би забавило реакцията и би нанесло големи щети, длъжностното лице по защита на личните данни, може по своя преценка да предприеме мерки за предотвратяване или намаляване последиците от нарушението на сигурността. В този случай длъжностното лице по защита на личните данни, уведомява незабавно ръководството за предприетите мерки и съобразява последващи действия с получените инструкции.

Чл.21. (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 - Смолян, 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:

(а) 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;

(б) името и координатите за връзка на длъжностното лице по защита на личните данни;

(в) описание на евентуалните последици от нарушението на сигурността;

(г) 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.22. (1) Областна администрация – Смолян води регистър на нарушенията на сигурността, който съдържа следната информация:

(а) дата на установяване на нарушението;

(б) описание на нарушението — източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо);

(в) описание на извършените уведомявания: уведомяване на КЗЛД и засегнатите лица, ако е било извършено;

(г) предприети мерки за предотвратяване и ограничаване на негативни последици за субектите на данни и за Областна администрация - Смолян;

(д) 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.

X. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл.23. (1) Областна администрация – Смолян 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 - Смолян:

(а) 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;

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

(в) информира физическите лица, чиито данни ще бъдат предоставени на трети страни.

(3) Обработване на лични данни от обработващи извън ЕС/ЕИП е допустимо само когато:

(а) Европейската Комисия е приела решение, потвърждаващо, че страната, към която се извършва трансферът, осигурява адекватно ниво на защита на правата и свободите на субектите на данни;

(б) Налице са подходящи мерки за защита като например Обвързващи Корпоративни Правила (ОКП), стандартни договорни клаузи, одобрени от Европейската Комисия, одобрен кодекс за поведение (Етичен кодекс за поведение на служителите в Областна администрация - Смолян) или сертификационен механизъм;

(в) Субектът на данни е дал своето изрично съгласие за трансфера, след като е информиран за възможните рискове;

(г) Трансферът е необходим за една от целите, изброени в ОРЗД, включително изпълнението на договор със субекта, защита на обществения интерес, установяване и защита на правни спорове, защита на жизненоважните интереси на субекта на данни в случаите, когато той е физически или юридически неспособен да даде съгласие.

XI. 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 - Смолян. 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:

(а) първоначалното въвеждане на нови технологии или прехода към нови технологии;

(б) автоматизирано обработване, включително профилиране или автоматизиране вземане на решения;

(в) обработване на чувствителни лични данни в голям мащаб;

(г) мащабно, систематично наблюдение на публично обществена зона.

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

XII. УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл.25. (1) Унищожаване на личните данни се извършва от Областна администрация - Смолян 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 разпоредбите и на относимите нормативни актове в т.ч. Номенклатура на делата със срокове за съхранение на Областна администрация - Смолян.

(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. Електронните данни се изтриват от електронната база данни по начин, непозволяващ възстановяване на информацията.

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

Чл.26. Длъжностното лице по защита на личните данни, и лицата, обработващи личните данни от името на Областна администрация - Смолян, са физически лица, притежаващи необходимата компетентност и назначени и/или упълномощени със съответен писмен акт, включително и чрез настоящите Правила.

Чл.27. Длъжностното лице по защита на личните данни:

(а) подпомага Областна администрация – Смолян 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;

(б) осигурява нормалното функциониране на гореспоменатите системи за защита;

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

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

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

(е) уведомява ръководството на Областна администрация – Смолян своевременно за всички нередности, установени във връзка с изпълнение на задълженията му;

Чл.28. (1) Събирането, обработката, съхранението и защитата на личните данни се извършва само 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 Областна администрация - Смолян, 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 обхватът на задълженията и правата на гражданите във връзка със защитата на личните данни са на лице в случаите със значение за:

а) националната сигурност;

б) отбраната;

в) обществената сигурност;

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

д) други важни цели от широк обществен интерес за Съюза или за държава членка, и по-специално важен икономически или финансов интерес на Съюза или на държава членка, включително паричните, бюджетните и данъчните въпроси, общественото здраве и социалната сигурност;

е) защитата на независимостта на съдебната власт и съдебните производства;

ж) предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регламентираните професии;

з) функция по наблюдението, проверката или регламентирането, свързана, дори само понякога, с упражняването на официални правомощия в случаите, посочени в букви а)—д) и ж);

и) защитата на субекта на данните или на правата и свободите на други лица;

й) изпълнението по гражданскоправни искове.

XIV. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл.29. (1) Всяко лице има право да иска достъп до своите лични данни, включително и да 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 искане на засегнатото физическо лице, получено на адреса на Областна администрация – Смолян или официалната електронна поща.

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

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

(5) Областна администрация – Смолян е длъжна в двуседмичен срок от получаване на искане по предходните алинеи да уведоми заявителя дали са налице законовите основания за уважаване на искането. Ако Областна администрация - Смолян намери, че са налице законовите основания да уважи искането, уведомява лицето и за реда, по който може да упражни правото си.

(6) Субектите на данни имат също правото да:

(а) възразят срещу употреба на личните им данни;

(б) изискат информация за законовото основание, въз основа на което личните им данни са предоставени за обработване на обработващ извън ЕС/ЕИП;

(в) възразят срещу решение, взето изцяло на база на автоматизирано обработване, включително профилиране;

(г) бъдат уведомени за нарушение на защита на данните, което е вероятно да доведе до висок риск за техните права и свободи;

(д) подават жалби до регулаторния орган- КЗЛД;

(е) 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).

XV. ПРОМЕНИ НА ВЪТРЕШНИТЕ ПРАВИЛА

Чл.30. Областна администрация – Смолян може да променя тези Правила по всяко време при необходимост, като същите да бъдат незабавно сведени до знанието на длъжностните лица, които засягат тези промени.

Чл.31. Всички административни звена в рамките на Областна администрация – Смолян спазват правилата и политиките, които администрацията е внедрила във връзка със защитата на личните данни.

XVI. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

За целите на настоящите правила:

§ 1. „Администратор на лични данни“ е Областна администрация - Смолян, представлявана от областния управител.

§ 2. „Обработващите лични данни“ са длъжностни лица от администрацията, които обработват лични данни от името на администратора на лични данни;

§ 3. Контролът по изпълнението на настоящите вътрешни правила се възлага на директора на дирекция „АПОФУС”.

§ 4. Настоящите правила се издават на основание чл. 24, ал. 4 от Закона за защита на личните данни и Наредба № 1 от 07.02.2007 г. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни, издадена от Комисия за защита на личните данни.

§ 5. Копие от Правилата са на разположение на служителите, имащи достъп до личните данни на потребители и доставчици на услуги на Областна администрация – Смолян.

Настоящите Правила са приети и влизат в сила от деня на утвърждаването им.

Съгласувал:
Ваклин Топов
Директор
на дирекция „АПОФУС“

Изготвил:
Ема Миткова
Гл. експерт „ЧР“
Дирекция „АПОФУС“