ЗАПОВЕД
№ РД-21-7711-9
21.10. **2021г**

МАРИО СМЪРКОВ – областен управител на област с административен център град Варна

У С Т А Н О В И Х:

Със заповед № РД-18-7711-6/28.05.2018г на областния управител на област Варна са одобрени „Вътрешни правила за обработване и защита на личните данни на физически лица в Областна администрация Варна" (за краткост ще бъдат наричани само Вътрешни правила нататък в заповедта), свързани с прилагането на Общ регламент за защита на личните данни 2016/679 на Европейския съюз.

Защитата на правата на физическите лица във връзка с обработването на лични данни изисква приемане на подходящи технически и организационни мерки, за да се гарантира изпълнението на изискванията на посочения регламент. Същият предоставя възможност на различните засегнати от разпоредбите му органи да приложат изискванията чрез адаптиране към спецификите в тяхната дейност и функции. За да може да докаже съответствието с настоящия регламент, администраторът следва да приеме вътрешни правила и да приложи мерки, които отговарят на принципите за защита на личните данни, заложени в европейското и националното законодателство.

Съгласно нормативните изисквания публичните органи, в качеството си на администратори на лични данни, следва да определят длъжностно лице по защита на данните. С цел оптимизиране на взаимодействието между звената в Областна администрация Варна при събиране, използване, съхранение и защита на лични данни на физически лица, както и предвид преобладаващия електронен характер на посочените процеси, Вътрешните правила следва да бъдат актуализирани.

С оглед на гореизложеното и на основание чл. 32, ал. 1 от ЗА

Н А Р Е Ж Д А М:

Изменям действащите „Вътрешни правила за обработване и защита на личните данни на физически лица в Областна администрация Варна" по следния начин:

1. ***Чл. 33*** от действащите Вътрешни правила се изменя и се чете:

(1) Длъжностното лице по защита на личните данни е служител в Областна администрация Варна, определен със заповед на областния управител, на когото не е изрично възложено да предоставя информация, с цел предотвратяване конфликт на интереси. В качеството си на лице по защита на личните данни, служителят се отчита директно пред областния управител, на когото при необходимост дава препоръки или съобщава за рискове, свързани с администрирането на лични данни.

(2) Задълженията на служителя в областта на защитата на лични данни се вписват в длъжностната му характеристика.

2. ***Чл. 35*** от действащите Вътрешни правила се отменя изцяло.

3. ***Чл. 37*** от действащите Вътрешни правила се изменя и се чете:

(1) При определяне на длъжностното лице по защита на личните данни се отчитат следните критерии и изисквания, изведени от контекста на Регламент (ЕС) 2016/679 и

съобразени със спецификите на ведомството като публичен орган и мащаба на обработване на лични данни на физически лица:

- опит в административното обслужване, работа с електронни масиви и електронна кореспонденция;
- познаване на нормативната уредба, свързана със защитата на лични данни на физически лица;
- разрешение / удостоверение за работа с класифицирана информация;
- предишна практика, свързана с управление на лични данни, работа с документи и информационна сигурност;
- служителят да познава операциите по обработване и начините за бързо филтриране на лични данни от административно-информационните ресурси на ведомството;
- служителят да няма наложено дисциплинарно наказание, свързано с нарушаване на конфиденциалността на служебна информация.

(2) Длъжностното лице по сигурност на личните данни следва да документира действията и съветите си към областния управител върху електронен и хартиен носител, както и да изготвя годишен отчет за дейността си.

Настоящата заповед е неразделна част от заповед № РД-18-7711-6/28.05.2018г на областния управител на област Варна, с която са одобрени „Вътрешни правила за обработване и защита на личните данни на физически лица в Областна администрация Варна".

Настоящата заповед се изготви в два еднообразни екземпляра – по един за преписката по издаване на заповедта и деловодството на Областна администрация Варна за сведение и изпълнение.

Копия от заповедта да се връчат на главния секретар, директорите на дирекции и експертът по информационно осигуряване и технологии в Областна администрация Варна.

Заповедта, ведно с утвърдените с нея изменения на Вътрешните правила, да се публикуват на интернет страницата на Областна администрация Варна от експертът по информационно осигуряване.

Директорите на дирекции да запознаят всички свои подчинени служители, работещи с лични данни на физически лица, с горепосочените изменения на Вътрешните правила.

Контрол по изпълнение на заповедта възлагам на главния секретар на Областна администрация Варна.

ОБЛАСТ ВАРНА ОБЛАСТЕН УПРАВИТЕЛ

МАРИО СМЪРКОВ
Областен управител на област с
административен център гр. Варна

ЗАПОВЕД
№ РД-18-7711-6
28.05. **2018г**

СТОЯН ПАСЕВ – областен управител на област с административен център град Варна

У С Т А Н О В И Х:

От 25 май 2018г публичните органи следва да прилагат Общ регламент за защита на личните данни 2016/679 на Европейския съюз. Областна администрация Варна следва да осъществява своята дейност при спазване на принципите, заложени в него, относно защитата на физически лица при обработването на лични данни и свободното движение на такива.

Защитата на правата на физическите лица във връзка с обработването на лични данни изисква приемане на подходящи технически и организационни мерки, за да се гарантира изпълнението на изискванията на посочения регламент. Същият предоставя възможност на различните засегнати от разпоредбите му органи да приложат изискванията чрез адаптиране към спецификите в тяхната дейност и функции. За да може да докаже съответствието с настоящия регламент, администраторът следва да приеме вътрешни правила и да приложи мерки, които отговарят на принципите за защита на личните данни.

С чл. 47 от Регламент 2016/679 на Европейския съюз се урежда създаването на задължителни фирмени правила за прилагане на изискванията му.

Предвид изложеното е необходимо да бъдат приети систематизирани вътрешни правила, които да регулират взаимодействието на звената в Областна администрация Варна при събиране, използване, съхранение и защита на лични данни на физически лица.

С оглед на гореизложеното и на основание чл. 32, ал. 1 от ЗА

Н А Р Е Ж Д А М:

Утвърждавам „Вътрешни правила за обработване и защита на личните данни на физически лица в Областна администрация Варна", ведно с два образеца на декларации към тях, регистър за информираност на служителите и информационен бюлетин за публикуване на интернет страницата на ведомството.

Настоящата заповед се изготви в два еднообразни екземпляра – по един за преписката по издаване на заповедта и деловодството на Областна администрация Варна за сведение и изпълнение.

Копия от заповедта да се връчат на главния секретар, директорите на дирекции и старши експерт в дирекция „АПОФУС", дейност „ИОТ".

Заповедта, ведно с утвърдените с нея Вътрешни правила, декларация – Приложение № 1 към правилата и информационния бюлетин, да се публикуват на интернет страницата на Областна администрация Варна от старши експерт в дирекция „АПОФУС", дейност „ИОТ".

Всички служители в Областна администрация Варна, работещи с лични данни на физически лица, да се запознаят с горепосочените Вътрешни правила и да подпишат Декларация – Приложение № 2 и Регистър - Приложение № 3, които да се съхраняват при експерт „Човешки ресурси".

Контрол по изпълнение на заповедта възлагам на главния секретар на Областна администрация Варна.

СТОЯН ПАСЕВ
Областен управител на област с административен център гр. Варна

РЕПУБЛИКА БЪЛГАРИЯ

ОБЛАСТЕН УПРАВИТЕЛ НА ОБЛАСТ ВАРНА

УТВЪРЖДАВАМ:

ОБЛАСТЕН УПРАВИТЕЛ:

/СТОЯН ПАСЕВ/

ВЪТРЕШНИ ПРАВИЛА

ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ФИЗИЧЕСКИ ЛИЦА В ОБЛАСТНА АДМИНИСТРАЦИЯ ВАРНА

2018г

ВЪТРЕШНИ ПРАВИЛА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ФИЗИЧЕСКИ ЛИЦА В ОБЛАСТНА АДМИНИСТРАЦИЯ ВАРНА

ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Настоящите правила за обработване и защита на личните данни в Областна администрация Варна служат за регулиране взаимодействието на звената при събиране, използване, съхранение и защита на лични данни на физически лица.

Чл.2. (1) Администрацията осъществява своята дейност при спазване на принципите, заложени в Общ регламент за защита на личните данни 2016/679 на Европейския съюз относно защитата на физическите лица във връзка с обработването на лични данни и свободното движение на такива.

(2) При организиране на управлението на лични данни Областна администрация Варна се ръководи от нормите за законност, откритост, достъпност, отговорност, отчетност, ефективност, координация, предвидимост, обективност и безпристрастност.

Чл.3. (1) Администрацията е длъжна да гарантира целесъобразно използване на личните данни на физическите лица в техен интерес и в рамките на услугата, за която са дали съгласие да бъдат употребени.

(2) Когато е налице законово основание за администратора за използва конкретни лични данни на физическото лице, това се осъществява при максимална икономия: събира се най-малкото количество данни за субекта, позволяващи неговата недвусмислена идентификация в административното производство или съответната сфера на служебна комуникация.

Чл.4. Администрацията осъществява своята дейност в интерес на обществото и в съответствие с Конституцията и другите нормативни актове. При използването на лични данни се съобразяват националните и международни норми, които са относими или задължителни за прилагане в публичната дейност на органа.

Чл.5. Администрацията планира и изпълнява дейността си по начин, който води до постигане на висок обществен резултат при възможно най-икономично използване на ресурсите.

Чл.6. (1) Всяко обработване на лични данни следва да бъде законосъобразно и добросъвестно. За физическите лица следва да е прозрачно по какъв начин отнасящи се до тях лични данни се събират, използват, обработват или съхраняват, както и в какъв обхват се извършва или ще се извършва обработването на данните.

(2) Принципът на прозрачност изисква всяка информация и комуникация във връзка с обработването на тези лични данни да бъде лесно достъпна и разбираема и да се използват ясни и недвусмислени формулировки.

(3) Физическите лица следва да бъдат информирани за рисковете, правилата, гаранциите и правата, свързани с обработването на лични данни, и за начините, по които да упражняват правата си по отношение на обработването.

(4) Потребителите на административни услуги следва да разполагат с ясна информация кои лични данни са необходими на административния орган по нормативни изисквания, за които данни не е необходимо изрично съгласие от носителя им при предоставяне на административния орган.

Чл.7. (1) Личните данни следва да са адекватни, релевантни и ограничени до необходимото за целите, за които се обработват. Това налага срокът, за който личните данни се съхраняват, да е ограничен до минимум, съобразно отделни Вътрешни правила за

съхраняването и използването на документите в учрежденския архив на Областна администрация Варна, утвърдени от областния управител и началникът на отдел „Държавен архив" Варна.

(2) Относно сроковете за съхраняване и унищожаването на данни на хартиен носител се отчитат и становищата на постоянно действаща експертна комисия по организиране на архивния фонд към Областна администрация Варна.

(3) С цел да се гарантира, че срокът на съхранение на личните данни не е по-дълъг от необходимия, администраторът установява срокове, приложени към Вътрешни правила за използване и съхранение на документи в архива на Областна администрация Варна, за унищожаване на преписки на хартиен носител и изтриване на сканираните им копия от електронната деловодна система на ведомството. При фиксирането на тези срокове се отчита становището на представител на „Държавен архив" дали определени документи не следва да бъдат предадени за съхранение в Националния архивен фонд.

Чл.8. (1) Администраторът следва да осигури на субектите възможност да коригират или заличават неточните лични данни.

(2) Личните данни следва да се използват и съхраняват по начин, гарантиращ подходяща степен на сигурност и поверителност, включително за предотвратяване на непозволен достъп до тях и до оборудване за обработването им.

(3) Администраторът не следва да запазва лични данни с единствената цел да може да реагира на евентуални искания.

Чл.9. (1) Настоящите правила се прилагат за обработването на лични данни на физически лица изцяло или частично с автоматични средства, както и за обработването с други средства на такива данни, които са или предназначени да бъдат част от регистър с персонални данни.

(2) Правилата не обхващат обработването на лични данни, които засягат юридически лица.

(3) Правилата не се отнасят за лични данни на починали лица, към които се прилагат общите правила за документооборот в Областна администрация Варна.

Чл.10. Общият регламент за защита на личните данни 2016/679 на Европейския съюз въвежда легални дефиниции, с които публичният администратор на лични данни следва да съобразява дейността си. Предвди това за нуждите на документооборота в Областна администрация Варна и защитата на съдържащите се в него лични данни на физически лица, в работните стандарти на ведомството се интегрират следните понятия:

а) „лични данни" представляват всяка информация, свързана с идентифицирано физическо лице или такова, чиято легитимация може да бъде установена въз основа на тези данни - субект на данни;

б) „обработване" означава всяка операция или съвкупност от операции, извършвана с лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

в) „ограничаване на обработването" означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

г) „псевдонимизация" означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирания им субект;

д) „регистър с лични данни" означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии;

е) „администратор" означава 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;

ж) „обработващ лични данни" означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

з) „получател" означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват лични данни, независимо дали е участник в служебна кореспонденция по повод стратирало административно производство или трета страна;

и) „съгласие на субекта на данните" означава всяко свободно изразено, конкретно, информирано и недвусмислено волеизявление на субекта на данните, което разкрива съгласието му свързаните с него лични данни да бъдат обработени;

й) „нарушение на сигурността на лични данни" означава положение, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

к) „генетични данни" са лични данни, свързани с наследени или придобити генетични белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето му и които са получени от анализ на биологична проба от въпросното лице;

л) „биометрични данни" са лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават идентификацията му - лицеви изображения или дактилоскопични данни;

м) „данни за здравословното състояние" означава лични данни, свързани с физическото или психическо здраве на физическо лице, които дават информация за здравословното му състояние;

н) „профилиране" означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице - за анализиране или прогнозиране на аспекти, отнасящи се до негови лични предпочитания, интереси, поведение.

Чл.11. Областна администрация Варна използва автоматизирана деловодна информационна система, в която се съхраняват лични данни на потребителите на административни услуги и заинтересованите страни в административното производство.

Чл.12. (1) Принципите за защита на данните се прилагат по отношение на всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано. Личните данни, подложени на псевдонимизация, които могат да бъдат свързани с дадено физическо лице чрез използването на допълнителна информация, следва да се считат за информация, отнасяща се до физическо лице, което може да бъде идентифицирано.

(2) За да се установи дали има достатъчна вероятност дадени средства да бъдат използвани за идентифициране на физическото лице, следва да се вземат предвид всички обективни фактори, като разходите и количеството време, необходими за идентифицирането, и се отчитат наличните към момента на обработване на данните технологии.

(3) Принципите на защита на данните не следва да се прилагат по отношение на анонимна информация, т.е. информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или по отношение на лични данни, които са анонимизирани по такъв начин, че субектът на данните вече не може да бъде идентифициран.

ПРИНЦИПИ ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Чл.13. (1) Личните данни се обработват законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните.

(2) Данните се събират за конкретни, изрично указани, легитимни и ясно дефинирани цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(3) Събират се подходящи данни, ограничени до необходимото и свързани с целите, за които се обработват.

(4) Следва да се събират актуални данни и да се предприемат разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.

(5) Личните данни се съхраняват във форма, която да позволява идентифицирането на субекта им за период, не по-дълъг от необходимото за целите, за които се обработват; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, както и в съответствие с предвидените в нормите за Националния архивен фонд срокове; следва да бъдат приложени подходящите технически и организационни мерки с цел да бъдат гарантирани правата и свободите на субекта на данните.

(6) Данните се обработват по начин, гарантиращ подходящо ниво на сигурност и поверителност, включително защита срещу неразрешено или незаконосъобразно обработване и случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически и организационни мерки.

Чл.14. (1) Личните данни са обикновени и специални.

а) обикновените се делят на:

- свързани с физическата идентичност на лицата – три имена, постоянен и настоящ адрес, ЕГН, номер на личната карта, орган и дата на издаването й, електронен адрес, телефон;
- свързани с икономическата идентичност – имотно и финансово състояние, участие и/или притежание на дялове, ценни книжа в дружества, наличие на публични задължения, данни, необходими за идентифициране за целите на данъчното законодателство, данъчен идентификационен номер;
- свързани със социалната идентичност – образование, трудова дейност, гражданство;
- свързани със семейната идентичност - семейно положение, родствени връзки.

б) специалните лични данни се наричат още „чувствителни" и разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, генетични данни, биометрични данни, данни за здравословното състояние, данни за сексуалния живот или сексуалната ориентация на физическото лице.

(2) Обработването на специални лични данни се забранява, освен ако:

а) субектът на данни е дал своето изрично съгласие за обработването им за една или повече конкретни цели, освен когато в националното или европейско право се предвижда, че забраната не може да бъде отменена от субекта на данни;

б) обработването е необходимо за изпълнение на задълженията или упражняването на специални правомощия на администратора или за осъществяване на права на субекта на данните по силата на действаща нормативна хипотеза;

в) 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;

г) обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;

д) обработването е необходимо с цел установяване, упражняване или защита на правни претенции или е по искане на съдилищата в качеството им на правораздаващи органи;

е) обработването е необходимо по причини от важен обществен интерес на основание европейското или национално право, извършва се пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интереси на субекта на данните;

ж) обработването е необходимо за целите на превантивната или трудова медицина, за оценка на трудоспособността на служителя, или ако по надлежния ред за него се установи медицинска диагноза, която с правна норма е призната за пречка за заемането на определена длъжност, като се спазват подходящи условия и гаранции за защита на събраните лични данни;

з) обработването е необходимо в контекста на съображения от обществен интерес в областта на колективното здраве, като защитата срещу сериозни трансгранични заплахи за здравето или осигуряването на високи стандарти за качество и безопасност на здравните грижи и лекарствените продукти;

и) обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели при зачитане правото на защита на данните.

Чл.15. За да е налице законосъобразност при обработването на лични данни, събирането им следва да е резултат от следните алтернативни правни основания:

а) съгласие на субекта на данни;

б) сключване или изпълнение на договор;

в) законово задължение на администратора;

г) защита на жизненоважни интереси на субекта на данните или друго физическо лице;

д) изпълнение на задача от обществен интерес или упражняване на официални правомощия, предоставени на администратора.

Чл.16. (1) Информацията, предназначена да осведоми субектите на лични данни за техните права, необходимостта от предоставяне на такива данни на администратора и действията, които се извършват с тях, следва да е прозрачна и лесно достъпна. Същата се публикува на интернет страницата на Областна администрация Варна за достъп от широк кръг потребители. Администраторът може да използва и брошури или информационно табло, разположени в или близо до помещението на звеното за административно обслужване, за да предостави сведения в тази насока на заявителите.

(2) В изпълнение на ал. 1 на сайта на Областна администрация Варна се обособява раздел с информация за субектите на данни, който включва:

а) функционално идентифициране на ведомството, начин за контакт, включително с длъжностно лице по защита на данните;

б) категориите лични данни, които се събират и за какви цели се обработват;

в) категориите получатели на лични данни извън административния орган, както и информация дали данните ще се трансферират в други държави, включително извън Европейския съюз;

г) срок за съхранение на данните

д) описание на конкретни права на субектите на данни (право на достъп, коригиране или изтриване на лични данни, ограничаване на обработването, възражение срещу обработването, преносимост на данните) и реда за упражняването им;

е) правото на субектите на данни да подадат жалба до съда или КЗЛД

ж) информация дали предоставянето на конкретни категории лични данни е задължително по закон или договорно изискване и евентуалните последици, ако тези данни не бъдат предоставени;

(3) Администраторът публикува информация, че не прилага автоматизирано вземане на решения, включително профилиране на потребителите на административни услуги или договорните контрагенти на ведомството.

(4) Администраторът запознава всичките си служители с основните изисквания на Регламент за защита на личните данни 2016/679, което се удостоверява с подписа им в Регистър за информираност на служителите относно правилата за работа с лични данни на физически лица (Приложение № 3), който се съхранява при експерт „Човешки ресурси".

(5) Лични данни на физически лица се съхраняват в преписките на хартиен носител, в електронната деловодна система на ведомството и в лично създадените файлове от всеки служител. Служителят взема необходимите мерки да спазва правилата за правомерно обработване на лични данни на физически лица, съобразно целите на обработката. Непотребни документи, съдържащи лични данни, се изхвърлят от ведомството след механично унищожаване на носителя им.

(6) Администраторът прилага политика на „чистото бюро", която всички служители, обработващи лични данни, прилагат. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни за неоторизирани лица и не бива да бъдат изваждани от помещенията на администратора без изрично разрешение или конкретна процесуална нужда, присъща за функциите на администрацията. Веднага щом хартиените документи вече не са необходими за текущата работа по обработване на лични данни, те следва да бъдат архивирани по съответния ред, а ако липсва основание за тяхното архивиране, следва да бъдат унищожени в съответствие със създадена за това процедура.

Чл.17. (1) В случай, че администраторът обработва лични данни на основание единствено съгласието на лицето, законосъобразността на действията му се потвърждава, когато администраторът докаже, че:

а) съгласието е свободно изразено и е не е дадено под натиск или заплаха от неблагоприятни последици;

б) съгласието е конкретно – за всяка определена цел, а когато е относимо - и за отделна категория лични данни;

в) съгласието е информирано – дадено въз основа на пълна, точна и лесно разбираема информация;

г) съгласието е недвусмислено – не се предполага, а е израз на пряко волеизявление или ясно потвърждаващо действие; мълчанието или липсата на волеизявление в тази насока не може да се приеме за съгласие.

(2) Съгласието по ал. 1 се документира в декларация, неразделна част от настоящите правила (Приложение 1).

(3) Ако физическото лицето откаже да подпише декларация за информирано съгласие, се съставя протокол, подписан от служителя „Административно обслужване" и длъжностното лице по защита на личните данни или юрисконсулт от ведомството, с който се удостоверява направения отказ, въпреки предоставената от администратора информация.

(4) На субекта на данните се предоставя възможност по всяко време да оттегли съгласието си с процедура аналогична на тази, с която го е дал.

Чл.18. (1) Съгласие следва да се дава чрез ясен утвърдителен акт – действие, което категорично показва, че субектът на данни е съгласен с предложеното обработване на неговите лични данни. Поради това мълчанието, предварително отметнати полета на хартиен или технически носител или липсата на действие не представляват съгласие.

(2) Съгласието следва да обхваща всички дейности по обработване, извършени за една и съща цел или цели. Когато обработването преследва повече цели, за всички тях следва да бъде дадено съгласие.

(3) Когато обработването се извършва въз основа на съгласието на субекта на данните, администраторът следва да може да докаже, че субектът на данните е дал съгласието си за операцията по обработване. Администраторът осигурява предварително съставена декларация за съгласие в разбираема и лесно достъпна форма, която не съдържа неравноправни клаузи.

(4) За да бъде съгласието информирано, субектът на данни следва да знае самоличността на администратора и целите на обработването, за които са предназначени личните данни.

Съгласието не следва да се разглежда като свободно дадено, ако субектът на данни няма истински и свободен избор и не е в състояние да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него.

Чл.19. (1) Когато е налице правно основание за обработване на лични данни, различно от съгласието – нормативно задължение, договор – администраторът не дублира това основание със съгласието на лицето.

(2) При всички положения субектът на данните следва да ги предостави с ясното съзнание за причината, поради която го прави, което се удостоверява с подписа му върху заявлението, с което е предоставил лични данни на администратора.

(3) При заявяване на административна услуга правното основание физическо лице – потребител да предостави лични данни е по подразбиране нормативно задължение – чл. 29, ал. 2 от АПК или специална правна хипотеза. В такъв случай лицето не е необходимо да попълва декларация за съгласие относно предоставените лични данни.

Чл.20. (1) Извън Областна администрация Варна лични данни на физически лица, предоставили ги на ведомството, могат при необходимост да се разкриват пред:

а) публични органи – НАП, НОИ, МВР, съдебни органи, контролни органи, органи на местното самоуправление, държавни агенции, компетентни структури на изпълнителната власт;

б) на обработващ лични данни – физическо или юридическо лице, което обработва личните данни от името на администратора и по негово възлагане – счетоводна къща, IT компания, поддържаща информационната система, подизпълнители по договор.

(2) Независимо от исканията на други органи или лица, администраторът следи за ограничаване разкриването на лични данни и свеждането му до необходимия минимум, като определя дали са налице нормативни предпоставки за предоставяне на данните на външен субект, дали е налице съгласие от титуляра на данните, ако няма правно изискване за предоставянето им, и какви рискове поражда трансферирането на личните данни в съответния случай.

(3) Службите по трудова медицина следва сами да събират предварителни данни от служителите чрез попълване на декларации за здравословното им състояние, без да делегират тези функции към работодателя, предвид обстоятелството, че медицинските данни са специални и административният орган не е оторизиран да събира или обработва такива, с изключение на болнични листове и документи за медицински преглед при първоначално постъпване на работа, както и ако трудовата дейност е прекратявана за повече от три календарни месеца.

(4) Отговорност за нарушение на принципите за защита на личните данни на физически лица носи администраторът, който ги е предоставил незаконосъобразно на трета страна, а не субектът, който ги е поискал.

ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

Чл.19. (1) Субектите имат гарантирани права по отношение на предоставените от тях лични данни:

а) право на достъп до личните данни, свързани с лицето, които се обработват от администратора;

б) право на коригиране или допълване на неточни или непълни лични данни;

в) право на изтриване на лични данни, които се обработват незаконосъобразно или с отпаднало правно основание (изтекъл срок на съхранение, оттеглено съгласие, изпълнена първоначална цел, за която са били събрани);

г) право на ограничаване на обработването – при наличие на правен спор между администратора и физическото лице до неговото решаване и/или за установяването, упражняването или защитата на правни претенции;

д) право на преносимост на данните – ако се обработват по автоматизиран начин на основание съгласие или договор; за целта данните се предават в структуриран, широко използван и пригоден за машинно четене формат; ако е технически осъществимо, прехвърлянето на данните може да стане пряко от един администратор към друг при спазване на процедурите, свързани с комплексното административно обслужване; правото на преносимост обхваща само данни, предоставени лично от субекта им, както и лични данни, генерирани и събрани от неговата дейност;

е) право на възражение, което може да се упражни по всяко време и на основания, свързани с конкретна претенция на лицето, при условие, че не съществуват убедителни законови основания за обработването, които да са с предимство пред интересите, правата и свободите на субекта на данните или го засягат в значителна степен;

ж) субектът на данни има право да не бъде обект на изцяло автоматизирано решение, включващо профилиране, което поражда правни последици за субекта на данните или го засяга в значителна степен.

(2) В случай, че администраторът разполага с лични данни на лице, което не му ги е предоставило само, при поискване следва да разкрие на лицето източника на личните данни и дали той е публично достъпен.

(3) Администраторът не е задължен да удовлетворява искания за изтриване на лични данни от физически лица, ако са налице нормативни предпоставки за съхранението или обработката им. Администраторът обаче е длъжен да документира подобно искане в определен за целта регистър, както и своя отговор по него.

(4) Когато лични данни са станали достояние на администратора нецеленасочено, като косвен резултат от изпълнението на негово законово правомощие или задължение (видеозапис на лице, преминало през зоната за охранително видеонаблюдение) администраторът не е длъжен да предостави достъп до тази информация на лицето повече от веднъж.

(5) Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или извършването на исканите действия, или да откаже да предприеме действия по искането. В тези случаи администраторът носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.

Чл.20. (1) Правото на субекта на данни да предава или получава отнасящи се до него лични данни не поражда задължение за администраторите да придобиват или поддържат технически съвместими системи за обработване. Когато в определен пакет от лични данни е засегнат повече от един субект на данни, правото личните данни да бъдат получавани следва да не засяга правата и свободите на други субекти на данни.

(2) Когато това е технически осъществимо, субектът на данни има право на пряко прехвърляне на личните данни от един администратор към друг.

Чл.21. Дори когато личните данни се обработват законно - обработването е необходимо за изпълнението на задача от обществен интерес, при упражняването на официално правомощие, предоставено на администратора, или по съображения, свързани със законните интереси на администратора или 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 на субекта на данни.

Чл.22. (1) Без да се засягат които и да било други административни или съдебни средства за правна защита, всеки субект на данни има право да подаде жалба до надзорния орган – Комисия за защита на личните данни (КЗЛД), ако счита, че обработването на лични данни, отнасящи се до него, нарушава относимите правни разпоредби. Надзорният орган, до

когото е подадена жалбата, информира жалбоподателя за напредъка в разглеждането на жалбата и резултата от нея, включително за възможността за съдебна защита.

(2) Всеки субект на лични данни има право на ефективна съдебна защита срещу администратор или обработващ лични данни, когато счита, че правата му по Регламент 2016/679 са били нарушени в резултат на неправомерно обработване на личните му данни. Производствата срещу областния управител на област Варна като администратор и обработващ лични данни се образуват с подаване на жалба чрез него пред Административен съд Варна.

Чл.23. Когато администраторът възнамерява да обработва личните данни по-нататък за цел, различна от тази, за която са събрани, той предоставя на субекта на данните преди това информация за естеството на целта и свързаните с нея специфики.

Чл.24. За съблюдаване правата на субектите на лични данни администраторът осигурява вътрешна процедура за приемане, разглеждане и отговаряне в едномесечен срок на искания от физически лица, свързани с предоставените от тях персонални данни.

Чл.25. Административният орган е длъжен да информира работниците и служителите във ведомството, в случай че извършва видеонаблюдение или следи предоставените от него средствата за електронна комуникация на работното място.

Чл.26. (1) За да гарантира правата на субектите на лични данни администраторът следва да изгради система за управление на риска по отношение на защитата на лични данни на физически лица.

(2) Извършването на оценка на риска обхваща:

- естеството, рамката, контекста и целите на обработването;
- възможните рискове за правата и свободите на физическите лица, тяхната вероятност и тежест, както и последиците за правата и свободите на физическите лица.

(3) Администраторът извършва оценка на въздействието върху защитата на личните данни при наличието на висок риск, например в резултат на мащабно обработване на спациални лични данни, систематично мащабно наблюдение на публично достъпна зона, използването на нови технологии.

(4) Администраторът извършва задължителна предварителна консултация с КЗЛД, ако оценката на въздействието върху защитата на данните показва, че обработването ще породи висок риск, ако не се предприемат ефективни мерки за ограничаването му.

(5) Администраторът избира подходящи технически и организационни мерки, за да може да гарантира и докаже спазването на Регламент 2016/679 на ЕС и националното законодателство в областта на защитата на лични данни. IT експертът на администрацията осъществява програма от мерки, които да обезпечат сигурността на информацията, обработвана в електронната деловодна система и регистри на Областна администрация Варна. Възможни подходящи мерки могат да бъдат:

- псевдонимизация на личните данни;
- криптиране на личните данни;
- осигуряване на непрекъсната поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;
- водене на записи на дейностите по обработване на лични данни в електронните системи на ведомството.

Чл.27. (1) Мерки за защита на данните следва да се осъществяват още в етапа на проектирането, както и по подразбиране.

(2) В етапа на проектиране, към момента на определяне на средствата за обработване и в процеса на самото обработване, следва да бъдат въведени подходящи технически средства и конфигурации, както и организационни мерки, разработени с оглед ефективното прилагане на принципите за защита на данните. Основна практика в тази връзка е свеждането на

данните до минимум и интегриране на необходимите гаранции в процеса на обработване чрез специализиран софтуер.

(3) Предприемат се на мерки по подразбиране, които да гарантират, че без намеса на физическото лице личните му данни няма да са достъпни за неограничен брой потребители. Въвеждат се подходящи технически мерки, за да се гарантира, че се обработват само лични данни, които са необходими с конкретна цел.

Чл.28. Прилагането на псевдонимизация на личните данни служи да намали рисковете за съответните субекти на данни и да помогне на администратора и обработващия лични данни да изпълняват своите задължения за защита на данните.

Чл.29. (1) Експерт „Човешки ресурси" от структурата на администратора, в сътрудничество с длъжностното лице по защита на личните данни, следва да приведе досиетата на служителите и работниците във ведомството в съответствие с изискванията на Регламент 2016/679 (ЕС). Медицински изследвания, освен медицинското свидетелство при постъпване на работа и решения от органите на медицинска експертиза (ТЕЛК), както и копия на лични карти не се изискват за досиетата на заетите в държавната администрация.

(2) Експерт „Човешки ресурси" от структурата на администратора следи автобиографиите на кандидати за работа да бъдат използвани еднократно в рамките на конкурса за длъжността, за която са подадени. Без съгласието на отпадналите кандидати документите им не следва да се използват за контакт с тях в последващ момент, при възникване на необходимост за администратора и показани добри резултати в конкурса.

(3) При постъпване на нови служители в Областна администрация Варна към първоначалния комплект с документи експерт „Човешки ресурси" връчва и декларация за поверителност (Приложение № 2), в която е изложено каква информация се събира за лицето и как се използва, както и каква отговорност носи служителят по отношение на работата си с лични данни на други лица.

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Чл.30. Публичните органи като администратори на лични данни определят длъжностно лице по защита на данните, което има за основна задача да информира и съветва администратора и неговите служители по всички въпроси, свързани с обработването и защитата на личните данни.

Чл.31. Длъжностното лице по защита на данните има ключова роля за осигуряване на законосъобразното обработване на лични данни в структурата на администратора. То следва да разполага с експертни познания в областта на относимото законодателство и/или информационните технологии.

Чл.32. Длъжностното лице по защита на данните не определя целите и средствата за обработване на данни и администраторът не може да му прехвърля своята отговорност за неспазване на нормативните изисквания в тази сфера.

Чл.33. Длъжностното лице по защита на данните не следва да е служител в учреждението на администратора, за да се избегне конфликт на интереси. То трябва да е външна фигура за йерархичната административна организация и да се отчита директно пред областния управител като ръководител на ведомството, на когото да дава препоръки, следейки за прилагането на законосъобразни практики в администрирането на лични данни.

Чл.34. Длъжностното лице следва да разполага с висока степен на независимост, за да изпълнява ефективно своите консултативно-превантивни функции. Администраторът няма право да дава указания или нареждания във връзка с изпълнението на задачите на длъжностното лице по защита на данните.

Чл.35. (1) Длъжностното лице по защита на данните - физическо или юридическо лице, профилирано в сферата на защита и обработка на личните данни, може да изпълнява функциите си въз основа на един от следните алтернативни способи:

- назначаване на служител в администрацията с конкретна длъжностна характеристика в областта на защитата на лични данни на физически лица;
- по граждански договор / договор за услуга.

(2) По изключение длъжностното лице за защита на данните може да е служител на администрацията по съвместяване с друга длъжност, която да не е ръководна или пряко свързана с обработването на лични данни, и да не е служител, заемащ длъжността „юрисконсулт" и производните й по ранг или занятие форми – основен ангажимент на юрисконсултите е процесуално представителство за защита правата на областния управител, което влиза в конфликт на интереси със задълженията на длъжностното лице по защита на данните, имащо за основен предмет на дейност да открива пропуски, слабости или отклонения при администрирането на лични данни.

Чл.36. (1) Длъжностното лице по защита на данните изпълнява най-малко следните задачи:

а) информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на Регламент 2016/679 на Европейския съюз и на други приложими правни разпоредби за защитата на данни;

б) наблюдава спазването на нормативните изисквания за защита на лични данни, включително възлагането на отговорности и повишаването на осведомеността на персонала, участващ в операциите по обработване;

в) при поискване предоставя съвети по отношение на оценката на въздействието върху защитата на данните и наблюдава извършването на тази оценка;

г) сътрудничи си с надзорния орган - КЗЛД;

д) действа като лице за контакт с надзорния орган по въпроси, свързани с обработването и по целесъобразност се консултира по всякакви други въпроси.

(2) При изпълнението на своите задачи длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.

Чл.37. (1) При определяне на длъжностното лице по защита на личните данни се отчитат следните критерии и изисквания, изведени от контекста на Регламент 2016/679:

- предишен опит, удостоверен с надлежен сертификат;
- предишна практика в работа с класификация на информация и управление на лични данни;
- да притежава IT квалификация или правно образование, но да е независим от титуляра, носещ риска от администрирането на лични данни;
- да не участва пряко в извършването на IT операции;
- да не е предпоставка за възникване на конфликт на интереси;
- да е пряко подчинен единствено на областния управител;

(2) Длъжностното лице по защита на данните не може да бъде освобождавано от длъжност, нито санкционирано от администратора или обработващия лични данни, за изпълнението на своите задачи. Длъжностното лице по защита на данните се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни.

(3) Длъжностното лице по сигурност на личните данни следва да документира действията и съветите си към ръководителя на структурата върху електронен и хартиен носител, както и да изготвя годишен отчет за дейността си.

ОТЧЕТНОСТ

Чл.38. Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с нормативните изисквания. Тези мерки при необходимост се актуализират.

Чл.39. Отчетността е задължение на администратора на лични данни и основен инструмент за доказване изпълнението на релевантните правни изисквания. Отчетност е способността във всеки един момент администраторът на лични данни да удостовери и докаже, че обработва личните данни добросъвестно, законосъобразно и прозрачно, за адекватни и пропорционални цели, с подходящо ниво на сигурност и защита.

Чл.40. Основните средства за спазване на принципа на отчетност са:

- поддържането на регистри на дейностите по обработване;
- определяне на длъжностно лице по защита на личните данни;
- извършване на оценка на въздействието при наличие на висок риск за правата и свободите на физическите лица;
- своевременно уведомяване на Комисията за защита на личните данни и субекта на данните при нарушения на сигурността;
- полагане на усилия за минимизиране на вредите за засегнатото лице при наличие на пробив в сигурността за съхраняваните лични данни.

Чл.41. (1) Всеки администратор или негов упълномощен представител поддържа регистър на дейностите по обработване, за които отговоря. Този регистър съдържа:

а) името и координатите за връзка на администратора, а когато е приложимо - на всички съвместни администратори, на представителя на администратора и на длъжностното лице по защита на данните;

б) целите на обработването;

в) описание на категориите субекти на данни и на категориите лични данни;

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

д) когато е приложимо, предаването на лични данни на трета държава или международна организация;

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

ж) общо описание на техническите и организационни мерки за сигурност.

(2) Регистрите се поддържат основно в електронен формат, осигуряващ възможност за обективиране на хартиен носител при нужда. При поискване администраторът или обработващият лични данни осигуряват достъп до регистъра на надзорния орган.

(3) Към регистрите не се прикачват лични данни.

Чл.42. (1) Публични органи, пред които се разкриват лични данни в съответствие с правно задължение за упражняване на официалната им функция, например данъчни и митнически органи, звена за финансово разследване или независими административни органи, не следва да се разглеждат като получатели, ако получават лични данни, които са необходими за провеждането на конкретно разследване от общ интерес, в съответствие с националното право или това на Европейския съюз.

(2) Исканията за разкриване на данни, изпратени от публичните органи, следва винаги да бъдат в писмена форма, да са обосновани и да засягат само отделни случаи, като не следва да се отнасят до целия регистър с лични данни или да водят до свързване на регистри на лични данни. Обработването на личните данни от посочените публични органи следва да е в

съответствие с приложимите правила за защита на данните съобразно целите на обработването.

Чл. 43. (1) С цел да се поддържа сигурността и да се предотврати обработване, което е в нарушение на принципите за работа с лични данни, администраторът или обработващият следва да извърши оценка на рисковете, свързани с обработването, и да предприеме мерки за ограничаване на тези рискове, например криптиране. Тези мерки следва да гарантират подходящо ниво на сигурност, включително поверителност, като се вземат предвид достиженията на техническия прогрес и разходите по изпълнението спрямо рисковете и естеството на личните данни, които трябва да бъдат защитени.

(2) При оценката на риска за сигурността на данните следва да се разгледат рисковете, произтичащи от обработването на лични данни, като случайно или неправомерно унищожаване, загуба, промяна, неправомерно разкриване, или достъп до предадени, съхранявани или обработвани по друг начин лични данни, което може по-конкретно да доведе до физически, материални или нематериални вреди.

Чл.44. (1) Оценката на въздействието е важен метод за отчетност, който се прилага в помощ на администраторите не само да спазват законодателните изисквания, но и да стане видно, че са взети подходящи мерки в изпълнение на тази цел.

(2) Оценката на въздействието е процес, предназначен да опише обработването на лични данни, да оцени необходимостта и пропорционалността на обработката и да спомогне за избора на най-подходящите технически и организационни мерки за защита.

(3) Извършването на оценка на въздействието върху защитата на лични данни не е задължително за всяка операция по обработването им. Тя се изисква само когато обработването на лични данни има вероятност да доведе до висок риск за правата на физическите лица. Управлението на риска включва анализ как ще се въздейства върху него и как той ще се отрази върху правата на лицето / лицата.

(4) Операции по обработване, които по правило въвеждат висок риск, са извършването на автоматично вземане на решения, включително профилиране; мащабно обработване на специални данни, включително информация за предишни осъждания на лицето; системно мащабно наблюдение на публично достъпна зона.

Чл.45. Оценката на въздействие може да бъде извършена от самия администратор, негов служител или от външно за организацията лице, но отговорността за извършването й остава на администратора. Той задължително следва да потърси съвет от длъжностното лице по защита на данните, когато такова е определено, а взетите решения следва да бъдат документирани.

Чл.46. Минималното съдържание на оценката на въздействие включва:

а) системен опис на предвидените операции по обработване и целите на обработването, ако е приложимо – преследвания от администратора законен интерес;

б) оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

в) оценка на рисковете за правата и свободите на субектите на данни;

г) предвидените мерки за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защита на личните данни на физическите лица;

д) предвидените мерки за доказване спазването на нормативните изисквания в областта на защитата на лични данни на физически лица.

Чл.47. Администраторът задължително провежда предварителна консултация с КЗЛД, ако оценката на въздействие върху защитата на данните покаже, че обработването ще породи висок риск, в случай че не се предприемат ефективни мерки за ограничаването му.

Чл.48. (1) В съответствие с принципа на отчетност администраторът е длъжен освен да приложи практически принципите за защита на личните данни по смисъла на Регламент 2016/679, още да докаже, че обработването на лични данни действително съответства на тези принципи.

(2) Документирането на дейностите по администриране на лични данни обхваща създаване и редовно актуализиране на вътрешни регистри на дейностите по обработване на лични данни, съдържащи следната информация:

- име и координати за връзка с администратора, както и на длъжностното лице по защита на данните;
- цели на обработването;
- описание на категориите субекти на данни и категориите лични данни;
- категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получатели в трети държави или международни организации;
- предвидените срокове за изтриване на различните категории данни;
- общо описание на техническите и организационни мерки за сигурност.

(3) Информацията по ал. 2 се публикува на интернет страницата на Областна администрация Варна в раздела, обособен за субектите на данни по чл. 16 от настоящите Правила.

Чл.49. (1) Надзорен орган по въпросите за защита на личните данни на физически лица е Комисия за защита на личните данни. Тя има следните основни функции и правомощия:

а) наблюдава и осигурява прилагането на нормативните изисквания;

б) дава становища, в съответствие с действащите правни норми, относно законодателните и административните мерки, свързани със защитата на правата и свободите на физическите лица по отношение на обработването;

в) насърчава информираността на администраторите и обработващите лични данни за задълженията им по силата на нормативната уредба;

г) при поискване предоставя информация на всеки субект на данни във връзка с упражняването на правата му по силата на правилата за работа с лични данни;

д) разглежда жалбите, подадени от субект на данни или от структура, организация или сдружение и разследва предмета на жалбата, доколкото това е целесъобразно;

е) дава становища по операциите за обработване на данни;

ж) разпорежда на администратора и на обработващия лични данни да предоставят всяка информация за изпълнението на своите задачи;

з) провежда разследвания под формата на одити във връзка със защитата на данните;

и) уведомява администратора или обработващия лични данни за предполагаемо нарушение на нормативните правила;

й) получава от администратора и обработващия лични данни достъп до всички лични данни и до цялата информация, от която се нуждае за изпълнението на своите задачи;

к) получава достъп до всички помещения на администратора и обработващия лични данни, включително до всяко оборудване и средство за обработване на данни;

л) отправя предупреждения до администратора или обработващия лични данни, когато има вероятност операции по обработване на данни, които те възнамеряват да извършат, да нарушат законовите разпоредби;

м) отправя официално предупреждение до администратора или обработващия лични данни, когато операции по обработване на данни са нарушили правните разпоредби;

н) разпорежда на администратора или обработващия лични данни да изпълнят исканията на субекта на данни да упражнява правата си съгласно действащите правни норми;

о) налага временно или окончателно ограничаване, в това число и забрана за обработването на данни;

п) разпорежда коригирането или изтриването на лични данни или ограничаването на обработването им;

р) налага административно наказание „глоба“ или „имуществена санкция“ в допълнение към другите санкции или вместо тях, в зависимост от особеностите на всеки отделен случай;

с) разпорежда преустановяването на потока на данни към получател в трета държава или към международна организация;

т) одобрява задължителните вътрешни правила на администраторите или обработващите данни.

(2) Надзорният орган има правомощието да дава разрешения и становища:

а) на администратора в съответствие с процедурата по предварителна консултация;

б) до Народното събрание, правителството или други институции и органи, както и до обществеността по всякакви въпроси, свързани със защитата на лични данни – по собствена инициатива или при поискване.

Чл.50. (1) Всяко физическо и юридическо лице има право на ефективна съдебна защита срещу отнасящо се до него решение със задължителен характер на надзорен орган.

(2) Всеки субект на данни има право на ефективна съдебна защита, когато компетентният надзорен орган не е разгледал жалбата или не е информирал субекта на данните в срок от три месеца за напредъка в разглеждането на жалбата или за резултата от нея. Производствата срещу КЗЛД се образуват пред Върховния административен съд на РБ.

(3) Когато се образува производство срещу решение на надзорен орган, което е било предхождано от становище или решение на Европейския комитет по защита на данните в съответствие с механизма за съгласуваност, надзорният орган предава това становище или решение на съда.

МРЕЖОВА СИГУРНОСТ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл.51. Администраторът въвежда в експлоатация или надгражда използваните електронни системи и оперативен софтуер така, че да бъдат активирани технически спецификации, ориентирани към спазване принципите на Регламент 2016/679. В електронните продукти следва да са ингерирани механизми за защита на личните данни.

Чл.52. Като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност.

Чл.53. (1) В случай на пробив в киберсигурноста на Областна администрация Варна, довел до изтичане на информация, свързана с лични данни на физически лица, областният управител в срок до 72 часа от узнаването следва да уведоми КЗЛД и субектите на станалите достъпни лични данни, както и да предприеме незабавни мерки за възстановяване електронната сигурност на базата данни и ограничаване на вредите, които биха претърпели физическите лица от неправомерна обработка на личните им данни.

(2) Уведомлението, посочено в ал. 1, съдържа най-малко следната информация:

а) описание на естеството на нарушението в сигурността на личните данни, включително, при възможност, категориите и приблизителният брой на засегнатите субекти и записи на лични данни;

б) посочване на името и координатите за връзка с длъжностното лице по защита на данните или друго лице за контакт, от което може да се получи повече информация;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни и мерки за намаляване на евентуалните неблагоприятни последици.

(3) Ако изтеклите данни са били криптирани или ако субектите на данни, които са станали уязвими, са много на брой, се публикува съобщение за инцидента на страницата на администратора.

(4) Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с това нарушение, последиците от него и предприетите действия за справяне с инцидента. Тази документация се предоставя на надзорния орган при извършване на проверка.

Чл.54. (1) Администраторът или обработващ личните данни следва да прилага псевдонимизация и криптиране на личните данни, както и да проявява устойчива способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване.

(2) Администраторът или обработващ личните данни осигурява своевременно възстановяване на наличността и достъпа до личните данни в случай на инцидент и осъществява преценка на ефективността на техническите и организационни мерки с оглед гарантиране сигурността на обработването.

Чл.55. Законен интерес на съответния администратор на данни представлява обработването на лични данни в степен строго необходима и пропорционална на целите за гарантиране на мрежовата и информационна сигурност - способността на дадена мрежа или информационна система да издържа, със съответно равнище на доверие, на случайни събития или неправомерни или злонамерени действия, които повлияват на наличността, автентичността, целостта и поверителността на съхраняваните или предавани лични данни, както и на сигурността на свързаните услуги, предлагани или достъпни посредством тези мрежи и системи от страна на публичния орган.

Чл.56. Администраторът следва да използва всички разумни мерки за проверка на самоличността на субекта на данни, който иска достъп, по-специално по отношение на онлайн услугите и онлайн идентификаторите.

Чл.57. В автоматизираните регистри на лични данни ограничаването на обработването следва да бъде осигурено с технически средства, така че личните данни да не подлежат на операции за по-нататъшно обработване и да не могат да се променят. Фактът, че обработването на лични данни е ограничено, следва да бъде ясно посочен в системата.

Чл.58. (1) Действията по осъществяване на киберсигурност, във връзка със защитата на лични данни, се прилагат от системния администратор на Областна администрация Варна в съответствие с Вътрешните правила за мрежова и информационна сигурност.

(2) При сключване на договор с доставчик на софтуерен продукт, относим или директно приложим в администрирането на лични данни, отговорностите на доставчика се уреждат с договор между него и администратора на лични данни в лицето на областния управител на област Варна.

(3) Доставчикът на продукта за администриране на лични данни на физически лица или водене на регистри, свързани с тази дейност, носи отговорност за съвместимостта на предложения продукт с изискванията на приложимото законодателство и адекватните мерки за защита на информацията.

(4) В случай на санкция, наложена на администратора на лични данни по вина на доставчика на специализирания софтуерен продукт, доставчикът следва да поеме имуществената отговорност по погасяване на задължението.

(5) В случай, че администраторът използва електронни регистри за дейностите по защита и обработка на личните данни, които запазват информацията на външен за ведомството сървър, потребителят администратор следва при прекратяване на абонамента да получи от доставчика цялата въведена информация в машинно четим формат.

САНКЦИИ

Чл.59. (1) Всяко лице, което е претърпяло материални или нематериални вреди в резултат на нарушение на нормативните разпоредби, има право да получи обезщетение от администратора или обработващия лични данни.

(2) Администраторът, участващ в обработването на лични данни, носи отговорност за вреди, произтичащи от извършеното обработване, което нарушава установените правила. Тази отговорност възниква само когато администраторът не е изпълнил свои задължения по Общ регламент за защита на личните данни 2016/679 или националното законодателство, конкретно насочени към обработващите лични данни, или когато е действал извън или в противоречие със законосъобразните указания на надзорния орган или длъжностното лице по защита на данните.

Чл.60. (1) Администраторът или обработващият лични данни се освобождава от отговорност, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата.

(2) Ако в една и съща операция по обработване участват повече от един администратор или обработващ лични данни или участват и администратор, и обработващ лични данни, когато те са отговорни за вреда, причинена от обработването, всеки администратор или обработващ лични данни носи отговорност за цялата вреда, за да се гарантира действително обезщетение на субекта на данни.

(3) Когато администратор или обработващ лични данни е изплатил пълното обезщетение за причинената вреда, той има право да поиска от другите администратори или обработващи лични данни, участвали в същата операция, да му възстановят част от платеното обезщетение, съответстваща на тяхната част от отговорността за причинената вреда, в съответствие с правилата на гражданското съдопроизводство.

Чл.61. (1) Комисията за защита на личните данни има право да налага административни наказания „глоба“ или „имуществена санкция“ за извършени нарушения на нормативните разпоредби като гарантира, че във всеки конкретен случай те са ефективни, пропорционални и възпиращи.

(2) В зависимост от обстоятелствата във всеки конкретен случай административните наказания „глоба“ или „имуществена санкция“ се налагат в допълнение към предупреждения, разпореждания, ограничения или вместо тях.

(3) Когато се взема решение дали да бъде наложено административно наказание „глоба“ или „имуществена санкция“ и се определя нейният размер, във всеки конкретен случай се разглеждат следните елементи:

а) естеството, тежестта и продължителността на нарушението, като се взема предвид видът, обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда;

б) дали нарушението е извършено умишлено или по небрежност;

в) действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни;

г) степента на отговорност на администратора или обработващия лични данни като се вземат предвид техническите и организационни мерки, въведени от тях;

д) евентуални свързани предишни нарушения, извършени от администратора или обработващия лични данни – преценка за наличие на рецидив;

е) степента на сътрудничество с надзорния орган с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него;

ж) категориите лични данни, засегнати от нарушението;

з) начина, по който нарушението е станало известно на надзорния орган, по-специално дали и до каква степен администраторът или обработващият лични данни е уведомил за нарушението;

и) ако на засегнатия администратор или обработващ лични данни преди са налагани мерки във връзка със същия предмет на обработването, дали посочените указания са спазени;

й) всякакви други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая, като пряко или косвено реализирани финансови ползи или избегнати загуби вследствие на нарушението.

(4) Ако администратор или обработващ лични данни умишлено или по небрежност наруши няколко разпоредби на настоящия регламент при една и съща операция по обработване или при свързани операции, общият размер на административната глоба или имуществената санкция не може да надвишава сумата, определена за най-тежкото нарушение.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§1. Настоящите Вътрешни правила за обработване и защита на личните данни на физически лица в Областна администрация Варна влизат в сила от датата на утвърждаването им със заповед на областния управител и отменят всички предходни инструкции със същия предмет във ведомството.

§2. В случаите, когато със специален закон или подзаконов нормативен акт е предвиден особен ред за работа с лични данни на физически лица, различен от установения по-горе, настоящите правила не се прилагат.

§3. Преди да бъдат утвърдени от областния управител, Вътрешните правила за обработване и защита на личните данни на физически лица се съгласуват от главния секретар на ведомството, на който се възлага и контрола по изпълнението им.

§4. Областният управител назначава или сключва договор с лице по защита на личните данни, което е подчинено единствено на него.

§5. Административният орган не е длъжен да изпълни неоснователно, незаконосъобразно или явно прекомерно искане на субект на данни, или такова, което съдържа очевидно противоречие с нормативно установено задължение на администратора.

§6. Неразделна част от настоящите Вътрешни правила за обработване и защита на личните данни на физически лица в Областна администрация Варна са три приложения: два образеца на декларации - една за информирано съгласие от физическо лице, когато не е налице правно основание или задължение за обработване на негови лични данни и една за поверителност; регистър за информираност на служителите относно правилата за работа с лични данни на физически лица.