Утвърждавам:

**Д-Р ОРЛИН ДИМИТРОВ**

*Директор на Регионална здравна инспекция-Враца*

**ИНСТРУКЦИЯ ЗА ЗАЩИТА**

**НА ЛИЧНИТЕ ДАННИ В РЗИ-ВРАЦА**

1. ОБЩИ ПОЛОЖЕНИЯ.
   1. Настоящата Инструкция се издава във връзка с приложението на Регламент (ЕС) 2016/679, Закона за защита на личните данни (ЗЗЛД) и националното законодателство на Република България в областта на защитата на личните данни. Същата влиза в сила на 17.06.2021 г., след като бе отменена старата с оглед влезлите в сила промени в националното законодателство (ЗЗЛД). Утвърдена е със заповед на Директора. Инструкцията допълва приложимата от администратора Политиката за поверителност, която е публикувана на електронния сайт на РЗИ-ВРАЦА.
   2. Инструкцията урежда организацията на обработване и защитата на лични данни, съобразно чл. 59 ЗЗЛД, във връзка с изпълнението на чл. 25и от същия закон, събирани от администратора, условията и реда за водене на регистри, съгласно чл. 62 и чл.6З ЗЗЛД, както и организацията и реда за упражняване на контрол при обработването на лични данни, по чл. 66 ал.1 ЗЗЛД от РЗИ-ВРАЦА, със седалище и адрес на управление: гр. Враца, ул. „Черни Дрин“№2, наричано за краткост „администратора“
   3. Инструкцията регламентира:
      1. Процедури и механизми за гарантиране на неприкосновеността на личността и личния живот, чрез осигуряване на защита на физическите лица, при неправомерно обработване на свързаните с тях лични данни, в процеса на свободно движение на данните;
      2. Видовете регистри, които се водят в дружеството във връзка с изпълнението на разпоредбите в чл. 62 от ЗЗЛД;
      3. Оценката на въздействието и нивото на защита за всеки от водените регистри с лични данни по чл. 64 ЗЗЛД;
      4. Необходимите технически и организационни мерки за защита на личните данни от случайно и/или незаконно унищожаване, и/или от случайна загуба, неправомерен достьп, изменение и/или разпространение, както и от други незаконни форми на обработване по чл. 66, 67, 68, 71 ЗЗЛД. Мерките имат за цел да гарантират поверителност, цялостност и наличност на личните данни;
      5. Правата и задълженията на лицата, обработващи лични данни и лицата, които имат достъп до лични данни, както и тяхната отговорност при изпълнението на тези задължения, съгласно чл. 53, по-специално ал. 5, чл. 54, по-специално ал. З, както и чл. 55, 56, 37а, 25а ЗЗЛД;
      6. Процедурите по докладване, управление и реагиране при инциденти, уредени в чл. 67, 68 ЗЗЛД;
      7. Правила за предоставяне на лични данни на трети лица, посочени в чл. 67, 68, 79 и 80 ЗЗЛД;
      8. Сроковете за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им, съгласно чл. 59 ЗЗЛД;
      9. Срокове за съхранение на личните данни и реда за тяхното унищожаване след изтичането им.
   4. Инструкцията се утвърждава, допълва, изменя и отменя от Директора.
   5. Инструкцията се прилага за личните данни по смисъла на Регламент (ЕС) 2016/679 и Закона за личните данни. Лични данни означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни”); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице, по смисъла на чл. 4, параграф 1 от Регламент 2016/679;

П. ПРИНЦИПИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ.

2.1. Инструкцията е съставена при спазване на следните принципи за защитата на лични данни:

* + 1. Законосъобразност, добросъвестност и прозрачност - обработване при наличие на законово основание, при полагане на дължимата грижа и при информиране на субекта на данни;
    2. Ограничение на целите — събиране на данни за конкретни, изрично указани и легитимни цели и забрана за по-нататъшно обработване по начин, несъвместим с тези цели;
    3. Свеждане на данните до минимум — данните да са подходящи, свързани със и ограничени до необходимото във връзка с целите на обработването;
    4. Точност — поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;
    5. Ограничение на съхранението — данните да се обработват за период с минимална продължителност съгласно целите. Съхраняване за по-дълги срокове е допустимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или статистически цели, но при условие, че са приложени подходящи технически и организационни мерки (чл. 25н ЗЗЛД);
    6. Цялостност и поверителност - обработване по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки;
    7. Отчетност - администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Ш. ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

3.1. Инструкцията е изготвена в изпълнение на следната политика за защита на личните данни:

* + 1. Установяване на ясни правила при събиране, организиране, съхраняване и разгласяване на лични данни от водените от дружеството регистри (чл.62, 63 ЗЗЛД), за да се гарантира неприкосновеността на личността и личния живот, като се защитят физическите лица при неправомерно обработване на свързаните с тях лични данни и се регламентира правото на достъп до сьбираните и обработвани такива данни (чл.55 ЗЗЛД).
    2. Създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица при неправомерно обработване на свързаните с тях лични данни, по реда на чл. 376, 37в, 38 и 39 ЗЗЛД;
    3. Задълженията на лицата, обработващи лични данни и/или лицата, които имат достьп до лични данни и работят в структурата на администратора, както и тяхната отговорност, съобразно чл. 70 ал. З ЗЗЛД;
    4. Предприемане на действия за защита на личните данни, предоставяни на Обработващи лични данни, съгласно чл. 70 ал. 2 ЗЗЛД.
    5. Необходимите технически и организационни мерки за защита на личните данни.

1. АДМИНИСТРАТОР, ОБРАБОТВАЩ ЛИЧНИ ДАННИ И РЕГИСТРИ С ЛИЧНИ ДАННИ.
   1. РЗИ-ВРАЦА е администратор на лични данни по смисъла на чл. 4, ал. 7 от Регламент (ЕС) 2016/679.
   2. Обработващ личните данни е всяко физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора. Определените от администратора лица, обработващи лични данни, имат оторизиран достьп само до регистрите, необходими за изпълняване на техните задължения.
   3. Отношенията между администратора и обработващия лични данни се уреждат с нормативен акт или писмен договор, който регламентира предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни и задълженията и правата на администратора, съобразно чл. 61 ал. З ЗЗЛД.
   4. Администраторът може да определи едно или повече лица, които да отговарят за координиране и прилагане на мерките за защита, съгласно чл. 61 ал. 1 ЗЗЛД.
   5. Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно въложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае” и след запознаване с нормативната уредба в областта на защитата на личните данни, политиката и ръководствата за защита на личните данни и опасностите за личните данни, обработвани от администратора, като за целта лицата подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.
   6. Всички лица отговарят за спазването на ограниченията за достъп до личните данни и са персонално отговорни пред Директора за нарушаването на принципите за поверителност, цялостност и наличност на личните данни, освен в случаите на форсмажорни обстоятелства. Контрол върху обработването на личните данни се осъществява от Директора.
   7. Всяко физическо лице, чиито лични данни ще се обработват от администратора, следва да бъде уведомено за:
      1. данните, които идентифицират администратора - наименование и начин за контакт;
      2. категориите лични данни, относящи се до съответното физическо лице;
      3. основанието и целите на обработването на личните данни;
      4. получателите или категориите получатели, на които могат да бъдат разкрити данните, както и дали данните се трансферират в трети страни извън ЕС;
      5. срока на съхранение на данните;
      6. информация за правата на субектите на данни (право на достъп, право на коригиране или изтриване на събраните данни, ограничаване на обработването, възражение срещу обработването, преносимост на данните) и реда за упражняването им;
      7. правото на субектите на данни да подадат жалба до КЗЛД (чл. 38 ЗЗЛД) или до съда (чл. 39 ЗЗЛД);
      8. дали предоставянето на лични данни е задължително по закон или договорно изискване, както и евентуалните последствия, ако тези данни не бъдат предоставени;
   8. Разпоредбата на т. 4.7. не се прилага, когато физическото лице, за което се отнасят данните, вече разполага с информацията по т. 4.7.
   9. Информацията по т. 4.7. се предоставя на субекта на данните към момента на получаване на личните данни чрез предоставяне на информационен лист, чрез предоставяне на настоящата инструкция, чрез e-mail, чрез препращане към Политиката/Декларацията за поверителност, поставени на видно място на седалището на управление на администратора и чрез всякакви други информационни канали, а за субекти, чиито лични данни са събрани преди приемане на настоящата инструкция и продължават да се обработват и съхраняват от администратора, информацията по т. 4.7. се предоставя в едномесечен срок от приемането й по описаните по-горе начини.
   10. ”Регистър с лични данни” е всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип. В РЗИ-ВРАЦА се обработват лични данни в следните регистри:
       1. Регистър „Контрагенти”;
       2. Регистър „Персонал”;
       3. Регистър „Видеонаблюдение”.
2. РЕГИСТЪР ”КОНТРАГЕНТИ”

Описание на поддържания регистър:

* 1. В регистьр „Контрагенти” се обработват лични данни на физически лица — контрагенти на РЗИ-ВРАЦА и/или представители на контрагентите юридически лица (клиенти, доставчици, партньори, и др.). Личните данни в Регистър „Контрагенти” се обработват за основните и допълнителни цели на осъществяваната от администратора дейност.

Категории лични данни в регистьра:

* 1. В регистьра се обработват следните категории лични данни:

5.2.1. За физическа идентичност: имена, ЕГН, адреси, телефон, ел. поща и др.

5.2.2. За икономическа идентичност — обща банкова информация, информация за номер на банкова сметка.

5.2.3. В случай, че страна по склочения с администратора договор е юридическо лице се обработват личните данни на представляващия дружеството, а именно имена, ЕГН, адреси, телефон, ел. поща и др.

Технологично описание на регистъра:

* 1. Данните в регистъра се обработват на хартиен или технически носител. На хартия в шкафове със заключване в изолирано помещение се съхраняват обработените на хартиен носител лични данни. Помещението се охранява със сигнално-охранителна техника. На сървър с парола за достъп се съхраняват личните данни на технически носител - твърд диск на един компютьр.

Технология на обработване:

* 1. Личните данни от регистъра се събират от физическите лица, за които се отнасят, и от публичните регистри.

Срок за съхранение:

* 1. Данните в регистъра се съхраняват за срок от 5 (пет) години, освен ако в нормативен акт, съдебен акт, договор не се изисква друго.

Ддъжности, свързани с обработването и защитата на лични данни от регистъра и описание на техните џрава и задължения

* 1. Данните в регистъра се обработват от изрично оправомощени служители на дружеството при спазване на принципа „Необходимост да се знае”.
  2. Право на достьп до регистъра имат само оправомощени по длъжност или с изрична заповед лица.
  3. Лица, обработващи лични данни, нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Оценка на въздействието и определяне съответното ниво на защита на регистъра по чл. 64 ал. 2 ЗЗЛД:

* 1. Оценка на нивото на въздействие на регистър „Контрагенти”:

НИВО НА ВЪЗДЕЙСТВИЕ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование на регистъра | Повери-телност | Цялост-ност | Налич-ност | Общо |
| „Контрагенти“ | ниско | ниско | ниско | ниско |

Методика за определяне на адекватното ниво на техническите и организационните мерки:

* 1. За определяне на адекватното ниво на техническите и организационните мерки и допустимия вид защита администраторът извършва оценка на въздействието върху обработваните лични данни, съгласно чл. 64 ЗЗЛД. При определяне нивата на въздействие върху конкретно физическо лице или група физически лица се взема предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва по критериите „поверителност”, „цялостност” и „наличност”. Оценката на въздействието се извършва при промяна на характера на обработваните лични данни и броя на засегнатите физически лица. В зависимост от определеното ниско ниво на вьздействие нивото на защита на регистьр „Контрагенти” е ниско.

Технически и организационни мерки за защита:

* 1. Физическа защита:
     1. Личните данни от регистъра се обработват в изолирано работно помещение, в което се намират основните работни места на оправомощените лица и които са с ограничен достъп — само за тях. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в метални заключващи се шкафове.
     2. Помещенията, в които се обработват лични данни от регистьра са изолирани и защитени с пожарогасителни средства и сигнално охранителна техника.
     3. Достъп се предоставя само на служителите, чиито служебни задължения включват обработване на лични данни от регистьра.
     4. Външни лица нямат достьп до лични данни от регистъра.
     5. Личните данни не се изнасят извън обекта на администратора. Никое длъжностно или трето лице няма право на достъп до личните данни, освен ако те не са изисквани по надлежен законен път от органи на съдебната власт (съд, прокуратура, следствени органи) съобразно чл. 49 ЗЗЛД. В подобни случаи и ако в писменото искане на съдебния орган не се съдържа изрична забрана за разгласяване, администраторът на лични данни е длъжен да информира лицето, но не и да препятства работата на органите на съдебна власт.

5.12. Персонална защита:

* + 1. Лицата, обработващи лични данни се запознават с нормативните актове в областта на защитата на личните данни и настоящата Инструкция.
    2. Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения.

Декларацията се съхранява в досието на всеки служител.

* + 1. Администраторът провежда обучение на лицата, които обработват лични данни в регистрите с цел запознаване с нормативната уредба в областта на защитата на личните данни и опасностите, които могат да възникнат при обработването и трансфера, както и необходимата реакция при събития, застрашаващи сигурността на данните.

5.13. Документална защита:

* + 1. Личните данни в Регистьр „Контрагенти” се поддържат на хартиен и/или технически носител. Обработването се извършва само по време на редовното работно време. Достъп до регистьра имат лицата, посочени по-горе в настоящата Инструкция. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора и в изпълнение на сключените договори. Достъпът до регистъра е ограничен само за оправомощените лица в съответствие с принципа „Необходимост да се знае”.
    2. Личните данни могат да бъдат размножавани и разпространявани от оправомощените служители само, ако е необходимо за изпълнение на служебните им задължения или, ако са изискани по надлежния ред от упълномощени лица.
    3. Временните документи от регистьра, които са на хартиен носител и съдържат лични данни, се унищожават. След изтичане на сроковете за съхранение (посочени в настоящата инструкция), тези документи се унищожават чрез нарязване, за което се съставя протокол от назначен със заповед на Директора служител. Унищожаването се извършва след изрично писмено разрешение от Директора.

5.14. Защита на автоматизирани информационни системи и мрежи:

* + 1. При работа с данните от регистьра се използва специализиран софтуерен продукт за обработване. Относно издадените Фактури във връзка със сключените между физическото лице или юридическо лице и дружеството договори (доставка, комисионен, наем и други) се използва счетоводна програма. Данните се въвеждат в база данни. Компютрите са със защитен достъп до личните данни. Системата за достъп поставя ограничения при опити за получаване на неоторизиран достъп до файловете с лични данни. Цялата счетоводна информация се събира и съхранява на сървъра на министерство на здравеопазването. С цел възстановяване на загубена, унищожена, заличена или изтрита информация, същата се съхранява на облак създаден от разпространителите на счетоводната програма. Всеки оправомомощен служител има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.
    2. За защита на данните е инсталирана антивирусна програма. Използва се и механизъм за криптиране на данни.
    3. В помещението, в което са разположени компютърни и комуникационни средства, е изолирано;
    4. При пренос на данни на преносим електронен носител, данните могат да се разпространяват само от и на оторизирани лица. Администраторът гарантира, че данните не могат да се четат или променят при пренасянето им.
    5. При пренос на данни чрез ел. поща, ел. поща следва да е защитена със сертификат за сигурност: SSL или друг подобен и надежден.

5.15. Организационни мерки за гарантиране нивото на сигурност:

* + 1. Работните компютърни конфигурации, както и цялата IТ инфраструктура, включително и достъпът до интернет, се използват единствено от служебни лица или от служители на дружеството, което извършва счетоводно обслужване на администратора;
    2. При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без предоставяне на достъп до личните данни;
    3. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.
    4. Сроковете за съхранение на данни от регистъра са описани в т. 5.5. от настоящата Инструкция.

5.16. Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.):

5.16.1. При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

5.17. Предоставяне на лични данни на трети лица:

5.17.1. Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение по чл. 42 ЗЗЛД.

5.17.2. Във връзка с използването на куриерски услуги - приемане, пренасяне и доставка и адресиране на пратките до физически лица дружеството посочва следните данни: три имена, адрес, област, пощенски код и наименование на населеното място.

Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им:

5.18. Оправомощените служители следва да извършват ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостга от тяхното обработване и съответно ако е отпаднало задължението - за заличаването им.

Ш. РЕГИСТЪР „ПЕРСОНАЛ“

Описание на поддържания регистър:

6.1. В регистър ”Персонал” се обработват лични данни на физически лица, работещи в дружеството по граждански и трудови правоотношения, както и на кандидати за работа. Личните данни в Регистър ”Персонал” се обработват за целите на управление на човешките ресурси, в т.ч. за:

* + 1. индивидуализиране на правоотношения по Закона за държавния служител, Закона за задълженията и договорите и трудовите правоотношение по Кодекса на труда;
    2. изпълнение на нормативните изисквания на Закона за задълженията и договорите, специалните закони и Кодекса на труда;
    3. използване на събраните данни за съответните лица за служебни цели:

6.1.4. всички дейности, свързани със съществуване, изменение и прекратяване на служебните, трудовите и гражданските правоотношения;

6.1.5. изготвяне на всякакви документи на лицата в тази връзка (договори, заповеди, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и др. подобни);

6.1.6. установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по служебни, трудови или граждански договори;

* + 1. водене на счетоводна отчетност относно възнагражденията на посочените по-горе лица по служебни, трудови или граждански правоотношения и начисляване на данъци;
    2. нуждите на пенсионното, здравното и социалното осигуряване.

Категории лични данни в регистъра:

6.2. В регистъра се обработват следните категории лични данни:

* + 1. За физическа идентичност: имена, ЕГН, паспортни данни, месторождение, адрес, телефон за връзка и др.;
    2. За социална идентичност — данни относно образование и допълнителна квалификация, трудова дейност и професионална биография;
    3. За икономическа идентичност — информация за номер на банкова сметка,

6.2.4. Лични данни относно съдебното минало на лицето (свидетелство за съдимост в зависимост от длъжностга);

6.2.5. Данни за здравословно състояние — медицинско свидетелство, данни, съдържащи се в болнични листове, представяни от самите служители като субекти на данните, решения на ТЕЛК/НЕЛК и др.

Технологично описание на регистъра:

* 1. Данните в регистьра се обработват на хартиен и/или технически носител.
  2. Автоматизираната обработка на данните се осъществява посредством специализиран софтуер или счетоводна програма.

Технология на обработване:

* 1. Данните в регистъра се предоставят от физическите лица при назначаването им. Данните се въвеждат директно от служител, който извършва счетоводно обслужване на администратора в граждански или трудови договори, други договори, допълнителни споразумения, документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др. Администраторът има склочено споразумение със счетоводна фирма с конкретно формулирани цели за събиране и обработване на точно определена категория лични данни и за разпределяне на задълженията и отговорностите между страните в изпълнение на Регламента. Обработващият лични данни има същите задължения за защита на данните, както задълженията, предвидени в европейското и националното законодателство за Администратора на лични данни. При работа с данните обработващият използва софтуерни продукти по обработка на данните относно възнагражденията на персонала. Софтуерните продукти са адаптирани към специфичните нужди на администратора на лични данни.

Срок за съхранение:

* 1. Данните в регистьра, касаещи работници и служители по трудов договор, се съхраняват за срок от 50 (петдесет) години във връзка с нормативно установени срокове. Данните в регистъра, касаещи лица по граждански договори, се съхраняват за срок от 5 (пет) години във връзка с нормативно установени срокове. В случай, че друг нормативен акт изисква съхранението им за по-дълъг срок, то администраторът ще се съобрази с него. Данните в регистъра, касаещи неодобрените кандидати за работа, се съхраняват за срок от 5 (пет) месеца, като след изтичане на този срок администраторът изтрива/унищожава съхраняваните документи с лични данни, освен ако специален закон предвижда друго. Когато неодобреният кандидат за работа е предоставил на администратора оригинали или нотариално заверени копия на документи, които удостоверяват физическа и психическа годност на кандидата, необходимата квалификационна степен и стаж за заеманата длъжност, администраторът връща тези документи на субекта на данни, в 5 (пет) месечен срок от окончателното приключване на процедурата по подбор. В определени случаи при подбор на персонал администраторът използва услугите на jobs.bg. Във връзка с предоставяните услуги jobs.bg обработва лични данни съгласно Политиката за защита на личните данни („Политика“) и спазва изискванията на Общия регламент за защита на личните данни.

Длъжности, свързани с обработването и защитата на лични данни от регистьра и описание на техните права и задължения:

* 1. Данните от регистъра се обработват от Директора и/или от оправомощени лица, изпълняващи функции на счетоводство и ТРЗ и при спазване на принципа „Необходимост да се знае”. 
  2. Право на достъп до регистъра имат само оправомощени по длъжност или с изрична заповед лица.
  3. Лица, обработващи лични данни, нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

Оценка на въздействието и определяне съответното ниво на защита на регистъра по чл. 64 ЗЗЛД:

6.10.0ценка на нивото на въздействие на регистьр „Персонал”:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование на регистъра | Повери-телност | Цялост-ност | Налич-ност | Общо |
| „Персонал“ | ниско | ниско | ниско | ниско |

Методика за определяне на адекватното ниво на техническите и организационните мерки:

6.11. За определяне на адекватното ниво на техническите и организационните мерки и допустимия вид защита администраторът извършва оценка на въздействието върху обработваните лични данни съгласно чл. 64 ал. 2 ЗЗЛД. При определяне нивата на въздействие върху конкретно физическо лице или група физически лица се взема предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва по критериите „поверителност”, „цялостност” и „наличност”. Оценката на въздействието се извършва при промяна на характера на обработваните лични данни и броя на засегнатите физически лица. В зависимост от определеното ниско ниво на въздействие нивото на защита на регистър „Персонал“е ниско.

Технически и организационни мерки за защита

6.12. Физическа защита:

6.12.1. Личните данни от регистъра се обработват в работни помещения на оправомощените лица (дружество, което е ангажирано със счетоводното обслужване на администратора или седалището на администратора), които са с контролиран достъп. Всички документи на хартиен носител, съдържащи лични данни, се съхраняват в заключващ се шкаф в същите помещения.

6.12.2. Помещенията, в които се обработват лични данни от регистъра са защитени чрез пожарогасителни средства и са под постоянно видеонаблюдение.

6.12.3. Достъп се предоставя само на служителите на обработващия лични данни, чиито служебни задължения включват обработване на лични данни от регистьра.

6.12.4. Външни лица нямат достъп до лични данни от регистъра.

6.13. Персонална защита:

6.13.1. Лицата, обработващи лични данни се запознават с нормативните актове в областта на защитата на личните данни и настоящата Инструкция.

6.13.2. Лицата, обработващи лични данни, задължително преминават обучение за събиране, обработка и съхранение на чувствителна информация, провеждат тренировка за реакция при събития, застрашаващи сигурността на данните, и подписват декларация, с която поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения. Декларацията се съхранява в досието на всеки служител на администратора и на обработващия лични данни. 6.12.3. Споделяне на критична информация между служителите (като идентификатори, пароли за достъп и т.н.) е забранено от политиките за информационна сигурност.

6.13. Документална защита:

6.13.1. Личните данни в Регистър „Персонал“ се поддържат на хартиен носител и съхраняват от обработващия лични данни (досиета, чието съдържание съответства на нормативните уредби на Република България, както и на вътрешните нужди за периодична оценка на служителите). Обработването се извършва само по време на редовното работно време. Достъп до регистьра имат лицата, посочени по-горе от настоящата Инструкция. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Достъпът до регистъра е ограничен само за оправомощени лица на счетоводната фирма в съответствие с принципа „Необходимост да се знае“.

6.13.2.Личните данни могат да бъдат размножавани и разпространявани от оправомощените лица на администратора или на обработващия лични данни само ако е необходимо за изпълнение на служебните им задължения или ако са изискани по надлежния ред от упълномощени лица.

6.13.3. Временните документи от регистъра, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер). След изтичане на сроковете за съхранение (посочени в настоящата инструкция), тези документи се унищожават чрез нарязване, за което се съставя протокол от назначен със заповед на Директора служител или от обработващия лични данни. Унищожаването се извършва след изрично писмено разрешение от Директора.

6.14. Защита на автоматизирани информационни системи и мрежи: 6.14.1. При работа с данните от регистъра се използва софтуерен продукт за обработване. Данните се въвеждат в база данни и се съхраняват на облак посредством използваната счетоводна програма. Чувствителната информация може да се криптира. Всеки оправомощен служител на обработващия лични данни има личен профил (потребителско име и парола), с определени съобразно задълженията му права и нива на достъп. С чувствителна информация работи изрично оправомощен служител, който единствено обработва криптираните файлове. Дефинирани са и уникални потребителски имена и пароли за стартиране на операционната система на всеки един компютър.

6.14.2. За защита на данните е инсталирана антивирусна програма. За защита на криптираната информация е инсталирана криптираща програма.

6.14.3. В помещенията, в които са разположени компютърни и комуникационни средства, е осигурено заключване на помещенията.

6.14.4. При пренос на данни на преносим електронен носител, данните могат да се разпространяват само от и на оторизирани лица. Администраторът гарантира, че данните не могат да се четат или променят при пренасянето им.

6.14.5. При пренос на данни чрез ел. поща, ел. поща следва да е защитена със сертификат за сигурност: SSL или друг подобен и надежден.

6.15. Организационни мерки за гарантиране нивото на сигурност:

6.15.1. Работните компютърни конфигурации, както и цялата IТ инфраструктура, включително и достъпът до интернет, се използват единствено от служебни лица.

6.15.2. При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

6.15.3. Не се разрешава осъществяването на отдалечен достъп до данни от регистъра.

6.15.4. Сроковете за съхранение на данни от регистъра са описани в т. 6.6. от настоящата Инструкция. След изтичане на сроковете за съхранение данните се заличават/изтриват от носителя.

6.16. Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.):

6.16.1. При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

6.17. Предоставяне на лични данни на трети лица:

6.17.1. Данни от регистъра могат да бъдат предоставяни на дьржавни институции с оглед изпълнение на нормативно задьлжение (НОИ, НАП, МВР и т.н.).

6.17.2. В качеството си на работодател, РЗИ-Враца, предоставя лични данни и на определени кредитни институции (банки) във връзка с изплащането на дължимите възнаграждения на служители, както и по молба от работещите във връзка с отпускането на кредити на служителите. Личните данни, които се предоставят са три имена и единен граждански номер и се предоставят с цел идентификация на лицето, в чиято полза се извършва плащането, както и размер на възнаграждението на лицето за определен период от време, в полза на което се извършва кредитирането. Това се налага, с оглед изискванията на кредитните институции във връзка с извършваните от тях банкови операции.

6.17.3. Във връзка с използването на куриерски услуги - приемане, пренасяне и доставка и адресиране на пратките до физически лица дружеството посочва следните данни: три имена, адрес, област, пощенски код и наименование на населеното място.

Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им:

6.18. Оправомощените служители на администратора и на обработващия лични данни следва да извършват ежегодни проверки на личните данни от регистъра с оглед преценка на необходимостта от тяхното обработване и съответно ако е отпаднало задължението - за заличаването им.

VII. ”ВИДЕОНАБЛЮДЕНИЕ”

Описание:

7.1. Администраторът извършва видеонаблюдението в сградата и около сградата на РЗИ-ВРАЦА. За целта се използват собствени камери за видеонаблюдение.

Администраторът обработва данни чрез автоматично денонощно видеонаблюдение (видеообраз) за движението на работници, служители и посетители, в т.ч. клиенти. Личните данни се обработват за следните цели: правилно съхранение на биопродукти, радиоактивни изотопи, контрол върху издаването на зелен сертификат за Ковид 19, законно и професионално изпълнение на служебните задължения, спазване на трудовата дисциплина, охрана на имуществото на администратора, защита на живота и здравето на работници, служители и посетители в т.ч. клиенти. Основание за обработването на тези данни е защита на здравето на гражданите, превенция на престъпления, защита на живота и здравето на работници, служители и посетители.

Категории лични данни:

7.2. Обработват се следните категории лични данни:

7.2.1. За физическа идентичност: видеообраз.

Технологично описание:

7.3. Данните се обработват като ежедневно се проследяват записите от Директора.

Технология на обработване:

7.4. Записите с видеообрази не се копират на отделен персонален компютър или други технически устройства.

Срок за съхранение:

7.5. Данните се съхраняват за срок от 8 месеца или до запълване на паметта на записващото устройството, освен ако в нормативен акт или в практиката не изисква друго.

Длъжности, свързани с обработването и защитата на лични данни и описание на техните права и задължения:

7.6. Данните се обработват от Директора на инспекцията.

7.7. В определени случаи право на достъп до данните имат само оправомощени по длъжност или с изрична заповед лица.

7.8. Лица, обработващи лични данни, нямат право да разпространяват информация за личните данни, станали им известни при изпълнение на служебните им задължения.

7.9. Служителите на РЗИ-ВРАЦА дават съгласие за осъществяване на видеонаблюдение по време на изпълнение на трудовите им задължения.

Оценка на въздействието и определяне съответното ниво на защита:

7.10. Оценка на нивото на въздействие:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование на регистъра | Повери-телност | Цялост-ност | Налич-ност | Общо |
| „Контрагенти“ | ниско | ниско | ниско | ниско |

Методика за определяне на адекватното ниво на техническите и организационните мерки:

7.11. За определяне на адекватного ниво на техническите и организационните мерки и допустимия вид защита администраторът извършва оценка на въздействието вврху обработваните лични данни. При определяне нивата на въздействие върху конкретно физическо лице или група физически лица се взема предвид характера на обработваните лични данни и броя на засегнатите физически лица. Оценката на въздействието се извършва по критериите „поверителност”, „цялостност” и „наличност”. В зависимост от определеното ниско ниво на въздействие нивото на защита на тази категория данни е ниско.

Технически и организационни мерки за защита:

7.12. Физическа защита:

7.12.1. Личните данни се обработват т.е. записите се проследяват ежедневно основно от директора на инспекцията в изолирано помещение.

7.12.2. Помещенията, в които се обработват лични данни са защитени чрез заключване на вратите, пожарогасителни средства.

7.12.3. Достьп се предоставя само на служителите, чиито служебни задължения включват обработване на лични данни от регистъра.

7.12.4. Външни. лица нямат достъп до лични данни от регистъра.

7.12.5. Личните данни не се изнасят извън обекта на администратора. Никое длъжностно или трето лице няма право на достъп до личните данни, освен ако те не са изисквани по надлежен законен път от органи на съдебната власт (съд, прокуратура, следствени органи). В подобни случаи и ако в писменото искане на съдебния орган не се съдържа изрична забрана за разгласяване, администраторът на лични данни е длъжен да информира лицето, но не и да препятства работата на органите на съдебна власт.

7.13. Персонална защита:

7.13.1.Лицата, обработващи лични данни се запознават с нормативните актове в областта на защитата на личните данни и настоящата Инструкция.

7.13.2.Лицата, обработващи лични данни, задължително подписват декларация, с която поемат задължение за неразпространение на лични данни, станали им известни във връзка и по време на изпълнение на служебните им задължения.

7.13.3. Администраторът провежда обучение на лицата, които обработват лични данни в регистрите с цел запознаване с нормативната уредба в областта на защитата на личните данни и опасностите, които могат да възникнат при обработването и трансфера, както и необходимата реакция при събития, застрашаващи сигурността на данните. 

* 1. Документална защита:

7.14.1.Личните данни не се поддържат на технически носител. Обработването се извършва денонощно. Достьп до данните имат лицата, посочени по-горе в настоящата Инструкция. Личните данни се събират само с конкретна цел, в съответствие с нормативните изисквания към администратора. Достьпът до регистъра е ограничен само за оправомощените лица в съответствие с принципа „Необходимост да се знае”. 

7.14.2.Личните данни могат да бъдат размножавани и разпространявани от оправомощените лица само ако е необходимо за изпълнение на служебните им задължения или ако са изискани по надлежния ред от упълномощени лица.

7.14.3.След изтичане на сроковете за съхранение (посочени в настоящата инструкция, а именно до запълване на паметта на устройството), данните се изтриват/заличават автоматично от носителя.

* 1. Защита на автоматизирани информационни системи и мрежи:

7.15.1.При работа с данните не се използва специализиран софтуерен продукт за обработване, тъй като същите не се снемат, пренасят или записват на други устройства. Налице е системата за достъп, която поставя ограничения при опити за получаване на неоторизиран достъп до лични данни.

7.15.2.За защита на данните е инсталирана антивирусна програма.

* 1. Организационни мерки за гарантиране нивото на сигурност:

7.16.1. Достъпът до камерите е ограничен, като цялата IТ инфраструктура, включително и достъпът до интернет, се използват единствено от служебни лица;

7.16.2. При ремонт на камера за видеонаблюдение, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без предоставяне на достъп до личните данни;

* + 1. Не се разрешава осъществяването на отдалечен достъп до данни, поместени на записващите устройства.
    2. Сроковете за съхранение на данни от регистьра са описани в т. 7.5. от настоящата Инструкция.
  1. Действия за защита при аварии, произшествия и бедствия (пожар, наводнение и др.):

7.17.1. При възникване и установяване на инцидент, веднага се докладва на лицето, отговорно за защитата на личните данни. В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защитата на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

* 1. Предоставяне на лични данни на трети лица:

7.18.1.Данни от регистъра могат да бъдат предоставяни на държавни институции с оглед изпълнение на нормативно задължение.

VIII. ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ. ПРОЦЕДУРА ПРИ НАРУШАВАНЕ НА СИГУРНОСТТА НА ЛИЧНИ ДАННИ 

8.1. Администраторът не назначава длъжностно лице по защита на данните поради липса на законовите предпоставки за неговата необходимост съобразно чл. 69, чл. 70 ал. ЗЗЛД.

8.2.В случай, че администраторът установи нарушение на сигурността на личните данни, той изпраща до Комисия за защита на личните данни уведомление за нарушението не по-късно от 72 часа, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица.

8.3.Отговорно лице за координиране на процедурата при нарушаване на сигурностга на лични данни е Директорът на инспекцията.

8.4.Администраторът документира всяко нарушение на сигурностга на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него.

8.5.При установено изтичане на лични данни, администраторът извършва оценка относно степента на риска. В случай, че след извършване на оценка на въздействието върху защитата на данните, администраторът установи, че има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурностга на личните данни.

1. СЪДЕЙСТВИЕ ЗА УПРАЖНЯВАНЕ НА ПРАВАТА

НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ по чл. 53 ал. 2 ЗЗЛД.

9.1. Администраторът оказва необходимото съдействие в случаите, когато субектът на лични данни упражнява правата си, предоставени му съгласно Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на Европейския съюз и законодателството на Република България.

9.2. При подаване на молба/ възражение/ искане по предходната точка от субект на лични данни, Администраторът организира разглеждането и решаването й/му безплатно в едномесечен срок от постъпването й/му.

* 1. Подаването на заявление от субекта на данни е безплатно. Лицето може да подаде писмено заявление, в това число и по електронен път лично или чрез упълномощено лице.
  2. Заявлението съдържа име на лицето и други данни, които го идентифицират - ЕГН, длъжност, месторабота, описание на искането, предпочитана форма за предоставяне достъпа до лични данни, подпис, дата и адрес на кореспонденцията; пълномощно - когато заявлението се подава от упълномощено лице. Заявлението се завежда в общия входящ регистьр на администратора.

9.5. Достьп до данните на лицето се осигурява под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице или упълномощено от него такова;
4. предоставяне на копие от исканата информация.

9.6. При подаване на искане за осигуряване на достьп представляващият администратора разглежда заявлението за достъп или разпорежда на отговорника по обработване на лични данни да осигури искания от лицето достьп в предпочитаната от заявителя форма. Срокьт за разглеждане на заявлениего и произнасяне по него е 30-дневен от деня на подаване на искането. Решението се съобщава писмено на заявителя лично. Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достьп до тях с мотивирано решение. Отказът за предоставяне достьп може да се обжалва от лицето пред посочения в писмото орган и срок. 

* 1. Достьп до личните данни на лицата, съдържащи се на технически носител имат отговорника по обработване на лични данни, обработващият лични данни в лицето на счетоводна къща, служба за трудова медицина,директорът на инспекцията, а в тяхно отсъствие и когато тези данни се отнасят до възнагражденията на лицата, достъп до тях има временно упълномощено от отговорника по обработване на лични данни лице, комуто е известна паролата за достьп до файловете.
  2. Решението си за предоставяне или отказване достьп до лични данни за съответното лице администраторът съобщава на третите лица в 30-дневен срок от подаване на молбата, респ. искането.
  3. В отговора до субекта Администраторът излага мотивирано становище относно основателността на искането и описание на конкретно предприетите мерки (в случите на основателност на искането).
  4. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може или да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или предприемането на исканите действия, или да откаже да предприеме действия по искането.
  5. Адресът, на който се приемат молби за достъп и предоставяне на лични данни от Администратора на РЗИ-Враца е гр. Враца, ул. Черни Дрин №2, представлявано от Орлин Цветанов Димитров.

Х. АКТУАЛВАЦИЯ НА ЛИЧНИ ДАННИ. АРХИВИРАНЕ

10.1. Актуализация на лични данни представлява допълнение или изменение на съществуваща информация в инспекцията. Актуализация на лични данни се извършва:

- по искане на лицето; за което се отнасят личните данни, когато то е установило, че е налице грешка или непълнота в тях и удостовери това с документ;

- по инициатива на администратора или оправомощено от него лице при наличие на документ; даващ основание за актуализация;

- при установена грешка при обработване на личните данни от страна на РЗИ-ВРАЦА или от отговорника или оправомощено от него лице;

* 1. При акгуализация на лични данни в досието на съответното лице се отразяват регистрационния номер на документа, източник на данните за атуализацията, дата на актуализацията. Актуализацията се извършва от администратора, лицето, отговорно за обработване на личните данни или от обработващия лични данни (външно счетоводство).
  2. Архивиране на личните данни на технически носител се извършва периодично на всеки три месеца от оттоворника за обработване на лични данни с оглед запазване на информацията за съответните лица в актуален вид. Същото се извършва на дискове, достъп до които има само отговорникът за обработване на лични данни.

XI.ОТЧЕТНОСТ

* 1. В случай, че Администраторът разшири дейността си и в резултат на това общият брой на служителите му надвиши 250 души, същият се задължава да създаде и да поддържа регистър на дейностите по обработване съгласно разпоредбата на чл. 30 от Регламента.
  2. Регистърът се води в табличен вид и съдържа следната информация:

11.2.1. име и контакт за връзка с администратора;

11.2.2. целите на обработването;

11.2.3. описанието на категориите субекти на данни;

11.2.4. описание на категориите лични данни;

11.2.5. категориите получатели, пред които са или ще бъдат разкрити личните данни;

11.2.6. когато е възможно - срок за изтриване на различните категории данни;

11.2.7. когато е възможно — общо описание на техническите и организационните мерки за сигурност.

XII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

* 1. За всички неуредени в настоящата Инструкция въпроси са приложими разпоредбите на Общия регламент относно защитата на данните (ЕС) 2016/679, приложимото право на, Европейския съюз и законодателството на Република България относно защитата на личните данни.
  2. За неизпълнение на задълженията, вменени на съответните оправомощени лица по тази инструкция и по ЗЗЛД, се налагат дисциплинарни наказания по Какона за държавния служител, Кодекса на Труда; а когато неизпълнението на съответното задьлжение е констатирано и установено от надлежен орган - предвиденото в ЗЗЛД административно наказание - глоба.
  3. Настоящата Инструкция е утвърдена със Заповед №РД-01-175/17.06.2021г. на Директора на РЗИ-Враца и всички служители и посетители следва да се запознаят с нея.