ДЕТСКА ГРАДИНА № 87 "БУКАТА"
Р-Н "ТРИАДИЦА" ул. "ЦАР ПЕТЪР" № 5 т./ф. 954 30 64
kg.bukata@gmail.com

УТВЪРЖДАВАМ:.....
ДИРЕКТОР НА ДГ № 87 „БУКАТА"
АЛБЕНА ИВАНОВА
Със Заповед № 5-5/15.09.2023 г.

ВЪТРЕШНИ ПРАВИЛА
за
сигурност при администриране на лични данни
на
Детска градина № 87 „Буката"

Р-Н „Триадица" Гр. София

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

Чл.1. (1) Настоящите Вътрешни правила за сигурност при администриране на лични данни от служители на Детска градина № 87 „Буката“ уреждат организацията и реда за упражняване на контрол при обработването на лични данни от служителите по смисъла на Закона за защита на личните данни (ЗЗЛД), както и условията и реда за водене на регистри съгласно ЗЗЛД.

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

(3) Достъп до определена информация във връзка с обработването на личните данни се осигурява само за оправомощени за това лица.

Чл.2. Правилата се приемат с цел да регламентират:

1. създаване на процедури и механизми за гарантиране неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица от неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;
2. задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, и отговорността при неизпълнение на тези задължения;
3. необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване;
4. видовете регистри, които се водят и тяхното описание.

Чл.3. (1) В дейността си Детска градина № 87 „Буката“ обработва лични данни на физически лица, предоставени от служители и родители.

(2) Всички действия спрямо постъпили във детската градина документи и изявления в устен, електронен вид или на хартия се извършват при стриктно спазване на изискванията за защита на личните данни съгласно ЗЗЛД и останалите съотносими нормативни актове, както и настоящите правила.

Чл.4. (1) Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

(2) Защитата на лични данни се осъществява въз основа на следните принципи за:

1. Законосъобразно и добросъвестно обработване;
2. Ограничено събиране, използване, разкриване и съхранение:

- Ограничено събиране - личните данни се събират за конкретни, точно определени нормативно цели и не може да се обработват допълнително по начин, несъвместим с тези цели; допълнителното им обработване за други цели, различни от целите, за които са събирани е допустимо само при посочени в закона условия; личните данни трябва да бъдат съотносими, свързани с и не надхвърлящи целите, за които се обработват;
- Ограничено използване - личните данни не трябва да се използват за цели, различни от тези, за които са били събрани;
- Ограничено разкриване - служителите на детската градина, които имат достъп до лични данни, са длъжни да не допускат разкриването и разпространението на свързана с тези данни информация извън предвидените в закона случаи;

- Ограничено съхранение - личните данни се поддържат във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват, освен в предвидените в закона случаи;
3. Прецизност – личните данни трябва да са точни, пълни и актуални, доколкото това е необходимо за регламентираните цели на използването им;
4. Сигурност и опазване – личните данни са защитени с мерки за сигурност в съответствие с вида и рисковете при обработването им и се съхраняват според нормативно определени изисквания и срокове.

РАЗДЕЛ II. ВИДОВЕ РЕГИСТРИ И ФОРМИ НА ВОДЕНЕТО ИМ

Чл.5. В детската градина се водят и съхраняват следните официални регистри и бази данни:

№ Видове регистри Видове лични данни

1 Регистър "Човешки ресурси" трите имена на служителя, ЕГН, адрес, паспортни данни, месторождение, образование, трудова дейност, земана длъжност, медицински данни, данни относно гражданско-правния статус на лицата

2 Регистър "Досиета на децата" трите имена на детето и родителите му, ЕГН, адрес, паспортни данни на родителите, месторождение, образование, трудова дейност, земана длъжност, медицински данни, данни относно гражданско-правния статус на лицата

3 Регистър "Клиенти и доставчици" данни за фирми, ЕГН, паспортни данни на управителя на фирмата, статут, актуално състояние, Булстат

Чл.6. Регистрите и базите данни по чл. 5 се водят и поддържат на хартиен, респективно – електронен носител, от съответните длъжностни лица по чл. 7, ал. 2.

РАЗДЕЛ III. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл.7. (1) Администраторът възлага обработването на лични данни на служители на детската градина, обработващи лични данни, съобразно спецификата на изпълняваните от тях служебни функции.

(2) Достъп до личните данни има само обработващият лични данни и/или действащото под негово пряко или на администратора ръководство оправомощено лице. Възможността за предоставяне на достъп до личните данни на друго лице е ограничена и регламентирана в Раздел V на Правилата - Предоставяне на лични данни.

(3) Служителите обработващи лични данни имат оторизиран достъп само до тези регистри, които са необходими за изпълняване на техните служебни задължения.

(4) Предоставянето, промяната или прекратяването на оторизиран достъп до регистрите се контролира от администратора.

Чл.8. (1) Администратора осъществява контрол върху законосъобразното водене и поддържане на регистрите и базите данни.

(2) Контролът върху обработването на личните данни се осъществява от отговорниците за защита на личните данни, определени в заповед на Директора.

Чл.9. (1) Служители и родители подават документите, съдържащи лични данни на служителя, отговарящ за съответния регистър.

(2) Обработващият данните информира служителите и родителите относно необходимостта от набирането им и целите, за които ще бъдат използвани.

(3) Носител (форма) за предоставяне на данните от физическите лица – личните данни за всяко лице се набират в изпълнение на нормативно задължение (разпоредбите на закони, подзаконови нормативни актове, кодекси и други) чрез:

- устно подаване на данните от лицето;
- хартиен носител (писмени документи);
- електронен носител;
- технически носител;
- външни източници, в изпълнение на нормативни изисквания.

Чл.10. При въвеждане, промяна или предаване на лични данни в базите данни администраторът осигурява съхраняване на информация за:

1. времето (дата и час) на въвеждане, промяна или предаване на личните данни;

2. лицата, извършващи въвеждането, промяната или предаването на личните данни;
3. лицата, предоставили личните данни;
4. променените или предадени лични данни, които са били въведени.

Чл.11. (1) Личните данни, организирани на хартиен носител и технически носител се съхраняват в папки в канцеларията на служителя, обработващ личните данни, която в извънработно време се заключват.

(2) Личните данни не се изнасят от сградата на детската градина.

Чл.12. (1) Личните трудови досиета на служителите на детската градина се обработват при длъжностното лице, отговарящо за тях и се съхраняват в картотечен шкаф.

(2) Личното трудово досие представлява съвкупност от писмени документи, които отразяват в цялост професионалното развитие и поведение на отделния служител и включват всички документи във връзка със създаването, изменението, развитието и прекратяването на трудовото правоотношение, длъжностната характеристика, както и други документи съгласно Кодекса на труда.

(3) Личните трудови досиета се съхраняват съгласно нормативно определените срокове.

Чл.13. (1) Информацията, която личното трудово досие съдържа, е конфиденциална и не може да бъде разгласявана без изричното писмено съгласие на работника или служителя.

(2) Личните трудови досиета имат следните нива на защита:

1. При начално ниво на защита (за лични данни, обработвани на хартиен носител) формата на организация и съхраняване на лични данни е писмена (документална);

- личните трудови досиета за всеки служител или нает по граждански договор лице се съхраняват в папки, които се поставят в картотечен шкаф;
- картотечният шкаф се намира в работно помещение, предназначено за самостоятелна работа на обработващия лични данни;
- служителят, работещ с личните трудови досиета, след приключване на работа с тях, и/или напускане на работното място заключва помещението.

2. При средно ниво на защита (за лични данни, обработвани на хартиен и технически носител, в компютърна система на локален компютър) формата на организация и съхраняване на лични данни е въвеждането им на твърд диск, на отделни компютри, който е непосредствен само от страна на обработващия лични данни.

Чл.14. (1) Личните данни, организирани и съхранявани в електронен вид, се въвеждат на твърд диск на компютър със защитен достъп до личните данни, с който може да работи само обработващият лични данни.

(2) При работа с данните се използват съответните софтуерни продукти за обработка на същите, включително относно управлението на човешките ресурси, възнагражденията на персонала, в това число основни и допълнителни възнаграждения, данъчни и други (вноски по заеми, запори и пр.) задължения, трудов стаж, присъствени и неприсъствени дни и други подобни.

(3) Достъп до операционната система, съдържаща файловете за обработка на лични данни, имат само обработващите лични данни чрез персонална парола за отваряне на тези файлове, известна само на съответния служител, а в негово отсъствие - друг служител, изрично определен със заповед на Директора.

РАЗДЕЛ IV. МЕРКИ ЗА ГАРАНТИРАНЕ НИВОТО НА СИГУРНОСТ

Чл.16. (1) В детската градина са предприети необходимите технически и организационни мерки за защита на личните данни от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

(2) Мерките по ал. 1 включват следните средства за защита на личните данни:

1. програмно-апаратни:

- разработване и прилагане на система за ограничаване на достъпа до лични данни;
- защита на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми,

периодично архивиране на данните на отделни електронни носители, както и чрез съхраняване на информацията на хартиен носител;

2. физически:

- заключване на помещенията в извънработно време и регламентиране на достъпа до тях;
- заключване в определените случаи на шкафовете за съхранение на информация, свързана с лични данни;
- осигуряване на физическа охрана на сградата, в която се намират работните помещения, в които се съхраняват носители на лични ранни и са разположени компютърни и комуникационни средства, и осигуряване на СОТ в тези помещения;

3. организационни:

- осигуряване на възможност за установяване самоличността на лицето, отговорно за сигурността – при мерки при средно ниво за сигурност;
- разработване и прилагане на процедури за създаване на архивни копия и за възстановяване на данни – при мерки при средно ниво за сигурност;
- разработване и прилагане на система за докладване, управляване и реагиране при инциденти.

4. нормативни:

- спазване на законовите изисквания и прилагане на процедурите за защита на техническите и информационни ресурси от аварии, произшествия и бедствия (пожар, наводнение и др.);
- осигуряване на ефективни механизми за контрол над спазването на вътрешните правила и съответните нормативни актове.

(3) Мерките по ал. 1 и 2 са съобразени със съвременните технологични постижения и осигуряват ниво на защита, което съответства на рисковете, свързани с обработването, и на вида на защитените данни.

Чл.17. Всички действия, които водят или могат да доведат до нерегламентирано изтриване, унищожаване или изменение на постъпили в детската градина лични данни в електронен вид или на хартиен носител са забранени.

Чл.18. **(1)** След приключване на обработване на личните данни или преди преустановяване на работа обработващия лични данни:

1. ги унищожава, или

2. ги прехвърля на друг администратор, като предварително уведоми за това Комисията за защита на личните данни, ако прехвърлянето е предвидено в закон и е налице идентичност на целите на обработването.

(2) След постигане целта на обработване на личните данни администратора ги съхранява само в случаи на искане от страна на клиента .

(3) В случаите, когато след постигане целта на обработване администратора иска да съхрани обработените лични данни като анонимни данни за цели по чл. 25, ал. 3 от ЗЗЛД, уведомява за това Комисията за защита на личните данни.

Чл.19. В детската градина се извършва проверка на всички работни компютърни конфигурации съгласно чл. 5, ал. 1, т. 10 от Наредбата за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни на всеки шест месеца от компетентно длъжностно лице.

Чл.20. **(1)** При възникнал инцидент (непредвидимо обстоятелство, което би могло да засегне сигурността на личните данни) узналото за инцидента длъжностно лице докладва незабавно на отговорниците за защита на личните данни, а те на администратора.

(2) Узналото за инцидента отговорното за защита на личните данни длъжностно лице попълва Регистъра на инцидентите под № 10 от чл. 5, ал. 2, в който се вписват инцидента, времето на установяването му, лицето, което го докладва, лицето, на което е бил докладван, както и последствията от него и мерките за отстраняването му. За описване

на последствията от инцидента и мерките за отстраняването му длъжностното лице е задължено да потърси съдействие на администратора.

РАЗДЕЛ V. ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ

Чл.21. (1) Администраторът предоставя лични данни в изпълнение на нормативно установени задължения.

(2) Лични данни се предоставят служебно между служителите, които ги обработват след обосновано искане и при уведомяване на отговорниците за защита на личните данни.

Чл.22. (1) Достъп до личните данни и разкриването им се осъществява по реда и при условията на ЗЗЛД от страна на следните лица:

1. физическите лица, за които се отнасят данните;
2. изрично упълномощени с нотариално заверено пълномощно представители на лицата по т.1;
3. трето лице, в случай, че е предвидено в нормативен акт;
4. обработващия личните данни.

(2) Достъпът се предоставя под формата на:

- устна или писмена справка,
- преглед на данните;
- предоставяне на копие от обработените данни.

(3) При поискване администратора на лични данни или упълномощените от него служители, обработващи лични данни предоставят копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

Чл.23. (1) При упражняване на правото си на достъп физическото лице има право по всяко време да поиска от администратора на лични данни:

1. потвърждение за това дали отнасящи се до него данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват;
2. съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват, както и всяка налична информация за техния източник;
3. информация за логиката на всяко автоматизирано обработване на лични данни, отнасящи се до него, поне в случаите на автоматизирани решения по чл. 34б от ЗЗЛД.

(2) При смърт на физическото лице правата му на достъп до личните данни и разкриването им се упражняват от неговите наследници.

(3) Информацията по ал.1 може да бъде предоставена под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице.

(4) Администраторът на лични данни е длъжен да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията по ал.1.

(5) Администраторът на лични данни предоставя информацията по ал. 1 безплатно.

7

Чл.24. Физическото лице има право по всяко време да поиска от администратора на лични данни да:

1. заличи, коригира или блокира негови лични данни, обработването на които не отговаря на изискванията на този закон;
2. уведоми третите лица, на които са били разкрити личните му данни, за всяко заличаване, коригиране или блокиране, извършено в съответствие с т.1, с изключение на случаите, когато това е невъзможно или е свързано с прекомерни усилия.

Чл.25. (1) Лични данни се предоставят на трети лица само след получаване на писмено съгласие от лицето, за което се отнасят данните.

(2) При неполучаване на съгласие от лицето или при изричен отказ да се даде съгласие, данните не се предоставят.

(3) Не е необходимо съгласие на лицето в случаите, когато е задължен субект по закон.
(4) В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, администратора предоставя на съответното физическо лице достъп до частта от тях, отнасяща се само за него.

Чл.26. (1) Правото на достъп и правата по чл.23 се осъществяват с писмено заявление/молба до администратора на лични данни, което може да бъде отправено и по електронен път по реда на Закона за електронния документ и електронния подпис и съдържа:

1. име, адрес и други данни за идентифициране на съответното физическо лице;
2. описание на искането;
3. предпочитана форма за предоставяне на информацията;
4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) При подаване на заявление от упълномощено лице към заявлението се прилага и нотариално завереното пълномощно.

(3) Заявленията се завеждат от администратора в регистъра №8 по чл.5, ал.2.

Чл.27. (1) Администраторът разглежда заявлението по чл.26, ал.1 и се произнася в 14-дневен срок от постъпването му в детската градина.

(2) При заявленията за достъп администратора на лични данни разрешава пълен или частичен достъп на заявителя или мотивирано отказва извършването му.

(3) Срокът по ал. 1 може да бъде удължен от администратора до 30 дни в определените в чл.28, ал. 1, т. 1 и 2 от ЗЗЛД случаи, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява дейността на администратора.

(4) Администраторът уведомява заявителя за решението си или отказа по ал.2 в съответния определен срок, лично срещу подпис или по пощата с обратна разписка.

(5) Липсата на уведомление по ал.4 се счита за отказ.

(6) Администраторът на лични данни е длъжен да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията.

(7) Администраторът отказва достъп до лични данни, когато те не съществуват или предоставянето им е забранено със закон.

Чл.28. Действията на администратора на лични данни се обжалват по реда на Глава VII от ЗЗЛД.

РАЗДЕЛ VI. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ

Чл.29. (1) Във връзка с обработването на лични данни служителите в детската градина имат права и задължения в съответствие с длъжностните си характеристики и са длъжни да спазват и изпълняват Вътрешните правила и съотносимите нормативни актове.

(2) За неспазване на нормативно установените си задължения във връзка с обработването на лични данни лицата по ал.1 носят имуществена отговорност съгласно ЗЗЛД както и дисциплинарна отговорност.

РАЗДЕЛ VII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите правила са приети на основание чл.3, ал.3, чл.4, т.4, чл.5, ал.1, чл. 13 и чл. 20 от Наредбата за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, във връзка с чл.24, ал.4 от ЗЗЛД.

§ 2. Контролът по изпълнение на настоящите Вътрешни правила се упражнява от отговорниците за защита на личните данни.

§ 3. Настоящите правила влизат в сила от деня на утвърждаването им със заповед на Директора.

§ 4. Изменението и допълнението на Правилата се извършва по реда за приемането им.

§ 5. За неуредените с Правилата въпроси се прилагат ЗЗЛД и относимите нормативни актове.