УТВЪРДИЛ: .....
Р.Капланова – директор на
ДГ № 4 „Слънчо“

ПОЛИТИКА

за защита и обработване на лични данни от

ДГ № 4“Слънчо“

ВЛАДАЯ

2018

СЪДЪРЖАНИЕ

1. ОБЩИ ПОЛОЖЕНИЯ

1.1 Настоящата политика има за цел да регламентира:

- Механизмите за защита на личните данни, обработвани от ДГ №4 „Слънчо“
- Определяне на обработващи лични данни и лица, които имат достъп до лични данни и работят под ръководството на обработващите лични данни – права, задължения и отговорност при неизпълнение на тези задължения, свързани с обработване и защита на лични данни.
- Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване, в т.ч. случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни.
- Действия за защита при аварии, произшествия и бедствия.
- Правилата за предоставяне на лични данни на субекта на данни и на трети лица.
- Сроковете за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им.
- Реда за унищожаване или предоставяне на данните на друг администратор.
- Процедура за уведомяване на Комисията за защита на личните данни за нарушение на сигурността на личните данни.

2. ИНДИВИДУАЛИЗИРАНЕ НА АДМИНИСТРАТОРА И ОБРАБОТВАЩИТЕ ЛИЧНИ ДАННИ

2.1 Индивидуализиране на администратора на лични данни.

- Данни за администратора на лични данни:
- Наименование: ДГ №4 „Слънчо“
- Код по БУЛСТАТ: 121571761
- Адрес на седалище: с.Владая, ул.“Ела“ № 6
- Тел. +359 2 999 10 32
- Адрес на електронна поща: sluncho4@abv.bg
- Уеб сайт: www.dg-4.com
- Директор: Румяна Капланова
- Принадлежност**:** Министерството на образованието и науката, Код по БУЛСТАТ:00069114
- Национална отраслова класификация - КИД- 85.10 – Предучилищно образование

Администратора на лични данни ДГ № 4 „Слънчо“, представляван от директор (АЛД) обработва личните данни самостоятелно и/или чрез възлагане със заповед на директора на детската градина на обработващи лични данни

2.2 АЛД може да определи едно или повече лица с право на достъп до лични данни, които да отговарят за координиране и прилагане на мерките за защита.

2.3 Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена 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 процедурите 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.

2.4 Всички обработващи лични данни, 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.

2.5 Всеки субект на данни, чийто лични данни ще се обработват от администратора, следва да бъде уведомен за:

- данните, които идентифицират администратора;
- целите на обработването на личните данни и правните основания за обработване на личните данни;
- категориите лични данни, отнасящи се до съответното физическо лице - субект на данни;
- получателите или категориите получатели, на които могат да бъдат разкрити данните;
- правата му по чл. 15-22 от Регламент 2016/679 в това число правото на достъп и правото на коригиране на събраните данни.

2.6 Администратора поддържат следните регистри с лични данни:

1. Регистър „персонал”
2. Регистър „кандидати за работа”
3. Регистър „заявления за упражняване на права”
4. Регистър „контрагенти”
5. Регистър „деца”
6. Регистър „родители”
7. Регистър „видеонаблюдение”
8. Регистър „пропускателен режим”

3. ТЕХНОЛОГИЧНО ОПИСАНИЕ НА ПОДДЪРЖАНИТЕ РЕГИСТРИ

Носители на данни

Администраторът на лични данни може да съхранява категориите лични данни, съдържащи се в регистрите на хартиении и електронни носители при спазване на приложимото законодателство и необходимите мерки за защита.

Срок на съхранение

Личните данни в Регистрите се съхраняват за периода необходим за изпълнение на задълженията на детската градина, в зависимост от съответния регистър, категорията лични данни и целите за обработването им. Личните данни не се съхраняват по-дълго, отколкото е необходимо за защитата на законните интереси на АЛД или за счетоводни цели, или в съответствие с изискванията на приложимото законодателство. Обработваните данни следва да биват унищожени след изтичане на периода на съхранение, в съответствие с изискванията, изложени в тази политика.

Сроковете за съхранение на личните данни по отделните регистри, са определени както следва:

№	Регистър	Срок	Определен от
1	Персонал	50 години	Закона за счетоводството
2	Кандидати за работа	1 години	Проекта на ЗИД ЗЗЛД е до 3 години
3	Деца	50 години	наредба№ 8/2016 г. на МОН
4	Родители	50 години	преценка на АЛД
5	Контрагенти	10 години	Закона за счетоводството
6	Заявления за упражняване на права	1 година	преценка на АЛД
7	Видеонаблюдение	14 дни	преценка на АЛД
8	Пропускателен режим	1 година	преценка на АЛД

Определяне на длъжностите/лицата свързани с обработване и защита на лични данни, правата и задълженията им

Директорът със заповед определя лицата, обработващи лични данни, правомощията им във връзка със защитата на обработваните лични данни, правата и задълженията им.

Директорът и/или упълномощените от него лица имат следните правомощия:

- Осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
- Следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата, и нивото на защита на водените регистри;
- Осъществяват контрол по спазване на изискванията за защита на регистрите;
- Поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите и подадените заявления за предоставяне на лични данни. Това правомощие е предоставено изключително на Директора на детската градина.
- Специфицира техническите ресурси, прилагани за обработка на личните данни;
- Следи за спазване на организационните процедури за обработване на личните данни и за спазване на контролирания достъп до носителите на лични данни;
- Провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.

Достъп до личните данни, съхранявани в Регистрите имат само служителите на детската градина, на които такъв достъп е необходим за изпълнение на служебните им задължения, при стриктно спазване на принципа „Необходимост да знае” (т.е. в съответствие с правата и задълженията му по длъжностна характеристика и/или договор за съответното правоотношение с Директора). По-конкретно тези служители са упълномощени на принципа „Необходимост да знае” със заповед на директора на на детската градина.

Възможността за достъп до личните данни при обработването им, на други служители в на детската градина е ограничена до случаите, когато на тях изрично е предоставено такова право на достъп и в съответствие с принципа „Необходимост да знае”. В този случай правото на достъп се предоставя за всеки конкретен случай от директора на детската градина, с изрично

разрешение, в което се посочват личните данни и целите, за които се предоставя достъпът, както и времето, за което той се предоставя.

Личните данни, обработвани от детската градина са защитени от разкриване на трети лица. Трети лица могат да имат достъп до такава информация, единствено ако имат такова нормативно установено правомощие или друго правно основание им дава такова право. Разкриване на такава информация трябва да бъде изрично разрешено от директора, като се предприемат подходящи мерки, които да осигурят спазването на законодателството в областта на личните данни, както и спазване на задължението за конфиденциалност и обезопасяване предаването на лични данни.

Настоящата политика е задължителна за всички служители на АЛД, доколкото те участват в обработването на личните данни по горните регистри, и за други лица, които могат имат постоянен или временен достъп до лични данни от всички или някой от регистрите.

Упълномощените служители, на които е възложено обработването на лични данни от Регистрите са длъжни:

- да обработват личните данни законосъобразно и добросъвестно;
- да използват личните данни, до които имат достъп, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели;
- да актуализират регистрите с личните данни (при необходимост);
- да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
- да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват,
- да спазват тази политика и процедурите, касаещи личните данни, утвърдени от администратора.

4. ВИДОВЕ ЗАЩИТА, ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

Физическа защита на личните данни, съдържащи се в Регистрите.

Организационни мерки:

Определяне на зони с контролиран достъп; Всички физически зони с хартиени и електронни записи, се съхраняват и са ограничени само за служители, които трябва да имат достъп чрез принципа „Необходимост да знае” с оглед изпълнението на работните им задължения. Всички записи и документи на хартиен носител, съдържащи лични данни, са в заключени шкафове, които са заключени в помещение с ограничен достъп, достъпен само от упълномощен персонал.

Данни са защитени чрез използването на средства за физически контрол на достъпа, като заключване на вратите. Всички помещения, където се съхраняват данни на хартиен носител, се намират в зони със ограничен достъп и са защитени чрез заключване на вратите, заключване на шкафовете или други подобни средства. Електронни носители включително сървъри, са защитени по подобен начин, в зони с контрол.

Определяне на помещенията, в които ще се обработват лични данни. Личните данни се обработват в непублична част от помещенията, която е физически ограничена и достъпна само от служители, за които е необходимо да имат достъп с оглед на изпълнението на служебните им задължения.

Определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни; Комуникационно-информационните системи, използвани за обработка на лични данни са отделени от зоните достъпни за външни лица и са физически защитени, като достъпът е ограничен само до тези служители, които за изпълнение на служебните си задължения се нуждаят от такъв достъп до данните.

Определяне на организацията на физическия достъп: Физически достъп до зоните с ограничен достъп, включително и тези, в които са намират информационните системи (компютри, сървъри), е възможен само през заключени врати за достъп. Достъп се предоставя само на служителите, на които е пряко възложено това или от счетоводство, на които той е необходим, за изпълнение на служебните им задължения, след оторизация.

С ключове за помещенията разполагат само отделни служители и не се предоставят на външни лица. Пароли за активиране и деактивиране на СОТ-системата, с която разполага администратора знаят определени служители.

Определяне на техническите средства за физическа защита.

Технически мерки:

- Ключалки
- Шкафове. Шкафове с ограничен достъп са физически заключени, с цел защита на регистрите с лични данни.

Оборудване на помещения.

Пожарогасителни средства

Персонална защита

Познаване на нормативната уредба в областта на защитата на лични данни се: разглежда в обучителната програма, която трябва да бъде премината от възпитателите и служителите и организирана от директора на на детската градина. Същите са длъжни да прочетат и да се запознаят с политиката и процедурите на на детската градина след наемането им, както и да актуализират познанията си във връзка със защитата на личните данни най-малко веднъж годишно. Запознаването с тази политика се осъществява срещу подпис.

Споделяне на критична информация между персонала (например идентификатори, ключове от шкафове, пароли за достъп и т.н.) е забранено, освен ако форсмажорни обстоятелства наложат това.

Обучение. Служителите трябва да преминат обучителна програма непосредствено след наемането им и най-малко веднъж годишно.

Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните се предоставя в обучителна програма, която трябва да бъде премината от служителите, непосредствено след наемането им и най-малко веднъж годишно. Служителите са обучени, незабавно да уведомят прекия си ръководител, ако имат съмнение или е известна заплаха за сигурността.

Документална защита

Определяне на регистрите, които ще се поддържат на хартиен носител;

Определяне на условията за обработване на лични данни

Личните данни се събират само с конкретна цел, за да подкрепят законните интереси на администратора на лични данни или до колкото е необходимо да се съобразят със законовите задължения на администратора на лични данни. Всеки тип данни се класифицира в съответствие с неговото предназначение и характер, и са защитени в съответствие с изискванията, посочени по-горе.

Регламентиране на достъпа до регистрите

Достъпът до регистрите е ограничен и се предоставя само на упълномощения персонал, в съответствие с принципа на „Необходимост да знае".

Контрол на достъпа до регистрите

Достъпът до данните е ограничен само до конкретни, минимално необходими данни, нужни на служителя да изпълнява неговите задължения.

Определяне на срокове за съхранение на личните данни

Съхраняването на данни е в съответствие с целите, за които са събрани данни и законоустановения срок. Личните данни се съхраняват толкова дълго, колкото е необходимо, за да се осъществи целта, за която са били събрани или както се изисква от приложимото право. Например, данни от регистър "Персонал" се обработват за 50 години след приключване на правоотношението, в съответствие с българското законодателство. След изтичането на определения срок, или при отпаднало основание, данните трябва да бъдат унищожени по безопасен начин.

Правила за размножаване и разпространение на лични данни

Личните данни могат да бъдат само копирани и разпространявани от упълномощените служители, само ако е необходимо за юридически нужди, както и да бъдат предоставяни само на лица, на които са необходими във връзка с извършване на възложена работа. Неразрешеното копиране и разпространение е обект на официални санкции, в зависимост от тежестта на престъплението, включително прекратяване на трудовите/ гражданските правоотношения.

Процедури за унищожаване

Документи на хартиен носител, които съдържат лични данни, трябва да бъдат унищожени по сигурен начин, когато вече не са необходими за чрез шредиране, или чрез

изгаряне. Всеки служител, който е в притежание на такива документи, е отговорен за сигурното унищожаване на документите. За всяко унищожаване се издава нарочна заповед на директора на на детската градина на и съставяне на надлежен протокол за унищожаване.

Защита на автоматизираните информационни системи и/или мрежи.

Идентификация и автентификация.

Потребителски акаунти и пароли. С цел да се въведе достъп, съобразен с принципа "Необходимост да знае", администратора на лични данни изисква да прилагат уникални потребителски акаунти и лични пароли за всеки потребител с акаунт за достъп до мрежата.

Отговорност на целия персонал - Членовете на персонала са лично отговорни за правилното използване на техните потребителски акаунти и пароли.

Управление на регистрите.

Със заповед на директора се посочват звената/ конкретните служители от администрацията на на детската градина отговорени за управлението на регистрите и само ограничен брой служители могат да имат достъп до данните, съдържащи се в регистрите, в съответствие с принципа на „Необходимост да знае”. Служителите с достъп до регистрите се определят от директора при необходимост.

Телекомуникации и отдалечен достъп:

Интернет достъп - на членовете на персонала може да бъде предоставен достъп до интернет, за да изпълняват служебните си задължения, но индивидуалният достъп може да бъде прекратен по всяко време по преценка на директора. Цялата информация, получена чрез интернет трябва да бъде под съмнение, докато не бъде потвърдена от надеждни източници.

Защита от вируси:

АЛД създава и поддържа стандартни и сигурни конфигурации за всяка компютърна и мрежова платформа, с която оперира. Системният софтуер се контролира и се поддържа от оторизирани лица. Сканиране на компютърни вируси -хардуерът на АЛД трябва да работи и да бъде актуализиран с версии на одобрен антивирусен софтуер скрининг и вирусните подписи на компютрите да бъдат активирани. Потребителите не трябва да отказват автоматични софтуерни процеси, които актуализират вирусните подписи. Антивирусният софтуер скрининг трябва да се използва, за да сканира всички софтуери и файлове с данни, идващи от или до трети страни или други служители на АЛД. Служителите не трябва да избягват или да изключват сканиране на процесите, които биха могли да предотвратят предаването на компютърни вируси. Флопи дискове и други магнитни носители, използвани от заразен компютър не трябва да се използват на друг компютър, докато вирусът не бъде успешно премахнат. Заразеният компютър също трябва да бъде незабавно изолиран от вътрешните мрежи. Потребителите не трябва да се опитват да премахнат вируса, тъй като информационните технологии ще премахнат вирусите. Антивирусните логове трябва да се съхраняват в продължение на най-малко седем (7) дни.

Поддържане/експлоатация;

Оценка на сигурността и тестване – на детската градина периодично провежда оценки на сигурността, уязвимостта и тестове за проникване в системи и мрежи. Детската градина ще провежда оценки за сигурността на информацията и/или неприкосновеността на личните данни. Членовете на персонала не трябва да придобиват, притежават, търгуват или използват хардуерни или софтуерни инструменти, които биха могли да бъдат използвани, за да се компрометира сигурността на информационните системи. Примери за такива инструменти са тези, които поразяват софтуера за защита на авторските права, разкриване на тайни пароли, идентифициране на уязвимост в сигурността или дешифриране на криптирани файлове. Без одобрение на прекия ръководител или по-горестоящ, е забранено използването на хардуер или софтуер, който отдалечено наблюдава трафика в мрежа или опериращ компютър. Неоторизирано използване на такива инструменти може да доведе до дисциплинарни действия.

Копия/резервни копия за възстановяване;

Архивиране на информацията - Целта на администратора е да поддържа наличността на информацията. Информацията, съдържаща лични данни трябва да бъде архивирана в съответствие със стандартите за архивиране на данни. Ако бъде необходимо, трябва да се инсталира или предостави техническа помощ за инсталирането на резервен хардуер. Всички архиви, съдържащи лични данни, от поддържаните от администратора регистри данни трябва да се съхранява с физически контрол на достъпа и трябва да се инвентаризира поне веднъж годишно

Физическа среда/обкръжение;

Физически контрол включително заключени врати, поддържане на подходяща температура и нива на влажност и наличието на детектори за пожар и пожарогасителната система са осигурени за защита на ИТ оборудването от неоторизиран достъп и контрол на риска от повреда и унищожаване.

Персонална защита;

До работа с информационните системи се допускат само обучени служители, при спазване на принципа „Необходимост да се знае“.

Процедури за унищожаване/заличаване/изтриване на носители:

Данни, които вече не са необходими, трябва да бъдат унищожени по безопасен начин чрез средства, като шредиране, изгаряне или постоянно заличаване от електронните средства. Съществува възможност трето лице да е ангажирано със съответен договор да провежда безопасни процеси по унищожаване от името на АЛД, за извършеното унищожаване на документи с лични данни трябва да се изиска съответно представи надлежен протокол за същото.

5. САНКЦИИ И ОТГОВОРНОСТ ПРИ НАРУШАВАНЕ НА ПРАВИЛАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ.

Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от служители на администратора може да бъде основание за налагане на дисциплинарни санкции, включително и уволнение.

6. ДЕЙСТВИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ (ПОЖАР, НАВОДНЕНИЕ И ДР.).

Следват се процедурите за управление по време на такова събитие за защита на физическите и информационни активи, включително ангажиране на допълнителна сигурност на помещенията и възстановяване на личните данни и други данни на администратора.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§ 1. По смисъла на настоящата политика:

1. „Лични данни" е всяка информация, свързана с идентифицирано физическо лице или физическо 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. Това лице се нарича субект на данни.

2. "Обработване" е всяка операция или съвкупност от операции, извършвана с лични данни или набор от 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.

3. "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.

4. „Контрагент" е физическо или юридическо лице - търговско дружество, сключило договор с АЛД за осъществяване на дадена дейност.

5. „Лице с достъп до данни" е всяко лице, действащо под ръководството на директора или на обработващия, което има достъп до лични данни, може да ги обработва само по указание на Директора, освен ако в закон е предвидено друго.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. По отношение на обработването и защитата на личните данни всички вътрешни процедури от документооборота на детската градина трябва да бъдат в съответствие с разпоредбите на Регламент 2016/679, ЗЗЛД и настоящата политика.

§ 2. Политиката е задължителна за всички служители и други лица, наети на граждански договори от детската градина и същите са длъжни да я спазват.

§ 3. Тази политика с приложенията към нея представлява регистър на дейностите по чл.30 от Регламент 2016/679.

§ 4. Контрол по изпълнението на настоящата политика се осъществява от Директора на детската градина и/или от упълномощените от него длъжностни лица.

§ 5. Изменения и допълнения на тази политика се правят по реда на издаването и утвърждаването ѝ.

§ 6. Тази политика отменя всички предишни документи, касещи мерките и средствата за защита на личните данни събирани, обработвани, съхранявани и предоставяне от/на детската градина и влиза в сила от датата на утвърждаването ѝ от директора на детската градина.