

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

НА

„ЧСУ ДУЖБА- СОФИЯ“ ЕООД

Дата на утвърждаване:	09.03.2018г.
Одобрено от:	ИЛИЯ НЕВЕНОВ ЕМИЛОВ- Изп.директор
Вид на документа:	Вътрешен
Последна ревизия:	04.09.2026 г.

Съдържание

I. ЦЕЛ И ТЕРИТОРИАЛЕН ОБХВАТ	2
II. ОПРЕДЕЛЕНИЯ	3
III. ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ	5
IV. ЦЕЛИ, ОСНОВАНИЯ И НАЧИНИ НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ	6
V. СРОКОВЕ ЗА СЪХРАНЕНИЕ НА ЛИЧНИ ДАННИ	8
VI. СЪВМЕСТНИ АДМИНИСТРАТОРИ, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ И ТРАНСФЕРИ В ТРЕТИ СТРАНИ.....	9
VII. УПРАЖНЯВАНЕ НА ПРАВА ОТ СУБЕКТИ НА ДАННИ	10
VIII. ВЪТРЕШНА ПРОЦЕДУРА ЗА УПРАЖНЯВАНЕ НА ПРАВА ОТ СУБЕКТИ НА ДАННИ.....	12
IX. ПРОЦЕДУРА ПРИ НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ.....	14
X. ЗАДЪЛЖЕНИЕ ЗА ИНФОРМИРАНост	15
XI. РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ	16
XII. МЕРКИ ЗА СИГУРНОСТ	16
XIII. ОЦЕНКА НА ВЪЗДЕЙСТВИЕ.....	18
XIV. КОНТРОЛ И ВЪТРЕШНА ОТЧЕТНОСТ.....	18

ЦЕЛ И ТЕРИТОРИАЛЕН ОБХВАТ

1. Цел

„ЧАСТНО УЧИЛИЩЕ ДРУЖБА - СОФИЯ“ ЕООД, наричано по-нататък за краткост „Дружество“, „Администратор“, приема настоящата Политика за защита на личните данни („Политика“) на основание член 24 от Регламент 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО („Общ регламент за защита на личните данни“, 'GDPR').

С утвърждаването на настоящата Политика Дружеството има за цел да установи правила, които да послужат спазването на задълженията и отговорностите си като администратор на лични данни, както и да удостовери и докаже, че обработването на лични данни се осъществява в съответствие с принципите за защита на личните данни в Общия регламент.

2. Териториален обхват

Тази Политика се прилага във всички случаи на обработване на лични данни в рамките на Дружеството, включително при изпълнение на договорните си задължения по доставка на стоки и услуги на контрагентите си, трудови правоотношения, счетоводство и т.н., с изключение на обработване на лични данни от служители в Дружеството в хода на чисто лични занимания. В последната хипотеза, ако служителите използват информационни и комуникационни средства, собственост на Дружеството, те са длъжни да се съобразяват с изискванията на информационната сигурност.

Политиката се прилага за обработването на лични данни в контекста на дейностите по място на установяване на Администратора в Република България. Когато обработването се извършва извън рамките на Европейския съюз (ЕС) или Европейското икономическо пространство (ЕИП), тогава се прилагат специалните правила на глава V от Общия регламент за защита на личните данни.

II. ОПРЕДЕЛЕНИЯ

„**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;

„**Специални категории лични данни**“ („чувствителни лични данни“) означава лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски

убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице;

„Обработване“ означава 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 комбинирание, ограничаване, изтриване или унищожаване;

„Регистър с лични данни“ означава 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;

„Администратор“ в настоящата Политика е „РАДИ В“ ЕООД, който сам или съвместно с други определя целите и средствата за обработването на лични данни;

„Обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

„Получател“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

„Съгласие на субекта на данните“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

„Дете“ означава всяко лице под 18 години, като съгласно Регламента съгласие от родител/настойник се изисква, тогава, когато лицето е под 16 години или по-ниска възраст в зависимост от националното законодателство. Съгласно чл. 3 от Закона за лицата и семейството установената възраст в България е под 14 години.

„Дейността на Дружеството“ означава дейността по предоставяне на социално-педагогически услуги, както и всички дейности, които са свързани с нея, включително предоставяне на транспорт до учебното заведение, предоставяне на столова на учащите в учебното заведение, предоставяне на пансион за учащите в учебното заведение, участие в състезания, конкурси и др. извънкласни дейности.

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

„Надзорен орган“ означава Комисията за защита на личните данни.

III. ПРИНЦИПИ НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

А) Принцип на законосъобразност, добросъвестност и прозрачност

Законосъобразно – личните данни се обработват единствено при наличие на правно основание по смисъла на чл. 6 или чл. 9 от Общия регламент;

Добросъвестно - личните данни се обработват по прозрачен начин, като се отчитат легитимните очаквания на субектите на данните;

Прозрачност – Дружеството предоставя на субекта на данните информация относно обработването на личните му данни в кратка, прозрачна, разбираема и лесно достъпна форма и на ясен и прост език.

Б) Принцип на ограничение на целите

Дружеството събира лични данни за конкретни, изрично указани и легитимни цели и не ги обработва по-нататък по начин несъвместим с тези цели;

В) Принцип на свеждане на данните до минимум

Администраторът събира и обработва лични данни, които са свързани с ограничени до необходимото във връзка с целите, за които се обработват;

Г) Принцип на точност

Дружеството гарантира, че личните данни, които обработва, са точни като при необходимост ги актуализира. За целта Администраторът предприема всички разумни мерки за своевременно изтриване или коригиране на неточни лични данни, като отчита целите, за които те се обработват;

Д) Принцип на ограничение на съхранението

Дружеството съхранява личните данни във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни;

Е) Принцип на цялостност и поверителност

Администраторът гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като прилага техническите или организационни мерки, посочени в настоящата Политика. Дружеството също така изисква от обработващите лични данни, с които работи, да предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки, които осигуряват равностойно или по-високо ниво на защита и сигурност на данните;

Ж) Принцип на отчетност

Дружеството обработва лични данни в съответствие с горепосочените принципи.

IV. ЦЕЛИ, ОСНОВАНИЯ И НАЧИНИ НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

1. Цели на обработване

А) Предоставяне на услуги по Закона за училищното и предучилищното образование (ЗУПО) – Дружеството като частно училище по смисъла на чл. 40, ал. 1 от ЗУПО обработва лични данни на ученици и родители на ученици във връзка с дейността по предоставяне на социално-педагогически услуги, както и всички дейности, които са свързани с нея, включително предоставяне на транспорт до учебното заведение, предоставяне на столова на учащите в учебното заведение, предоставяне на пансион за учащите в учебното заведение, участие в състезания, конкурси и др. извънкласни дейности. Личните данни, които се обработват във връзка с ученическото досие са изброени в Приложение №2, а видовете, предназначението, съдържанието на информацията в основни реквизити на документите за децата и учениците са определени в Приложение № 3.

Б) Търговска дейност – Дружеството обработва лични данни на свои контрагенти за целите на търговската му дейности, включително при извършването на доставки на стоки и услуги в съответствие със ЗЗД. Дружеството също така обработва лични данни на свои клиенти и контрагенти при предоставянето на услуги в сферата на ресторантьорството, както и транспортна дейност в съответствие с Търговския закон, Закона за автомобилните превози и подзаконовите нормативни актове.

В) Трудовоправни отношения

В качеството си на работодател, Дружеството обработва лични данни на служители си в съответствие с изискванията на трудовото и социалното законодателство, включително за осигуряването на здравословни и безопасни условия на труд;

Г) Счетоводство

В качеството си на данъчно задължен субект, Администраторът обработва лични данни в съответствие със Закона за счетоводството, Данъчно-осигурително процесуалния кодекс и другите приложими закони в тази област;

Д) Сигурност и охрана

Дружеството обработва лични данни за осигуряване на сигурността на учениците, служителите, посетителите и имуществото чрез видеонаблюдение;

Д) Други дейности

Администраторът обработва лични данни за целите на защитата на легитимните си интереси и правното обслужване, включително при обработване на лични данни чрез автоматизирани средства.

2. Основания за обработване на лични данни

А) Дружеството обработва лични данни на своите контрагенти на основание изпълнение на договор, по който субектът на данните е страна, включително преддоговорни отношения (член 6, параграф 1, буква „б“ от Общия регламент за защита на личните данни);

Б) Администраторът обработва лични данни на субекти на данни във връзка с изпълнение на законовите си задължения съгласно Закон за училищното и предучилищното образование, Закон за народната просвета, Закон за държавния архив, Наредба № 8/11.08.2016 г. на МОН- във връзка с обучението, възпитанието и социализацията на ученика и предоставяне на частна социално-педагогически услуги. При извършване на транспортна дейност - Търговския закон, Закона за автомобилните превози (член 6, параграф 1, буква „в“ от Общия регламент за защита на личните данни);

В) Дружеството, в качеството си на работодател, обработва личните данни на служителите си и кандидатите за работа на основание трудов договор, съответно преддоговорни отношения (член 6, параграф 1, буква „б“ от Общия регламент за защита на личните данни) и за спазване на законовите задължения в трудовото и социалното законодателство, приложими спрямо Администратора (член 6, параграф 1, буква „в“ от Общия регламент за защита на личните данни);

Г) Дружеството, в качеството си на работодател, обработва специални категории лични данни на служителите си - данни за здравословното състояние, когато обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила в съответствие с приложимото национално законодателство (член 9, параграф 2, буква „б“ от Общия регламент за защита на личните данни);

Д) Обработването на лични данни за счетоводни цели се извършва на основание на законовите задължения на Администратора съгласно Закона за счетоводството (член 6, параграф 1, буква „в“ от Общия регламент за защита на личните данни);

Е) Дружеството обработва лични данни за целите на сигурността и охраната чрез видеонаблюдение за защита на легитимните си интереси, доколкото те имат преимущество над интересите или основните права и свободи на субектите на данни (член 6, параграф 1, буква „е“ от Общия регламент за защита на личните данни);

Ж) Администраторът може да обработва лични данни за целите на директния маркетинг въз основа на свободно изразено, конкретно, информирано и недвусмислено съгласие на лицето, дадено в писмена или електронна форма или за друга цел, за която няма друго правно основание освен съгласието на субекта на данните (член 6, параграф 1, буква „а“ от Общия регламент за защита на личните данни).

3. Начини за събиране на личните данни

Дружеството събира личните данни на учащи в учебното заведение, родители на учащи, кандидати за работа, служители, контрагенти, посетители и други пряко от субектите на данни. То обработва лични данни с автоматични и неавтоматични средства. Администраторът не извършва автоматизирано вземане на индивидуални решения или профилиране.

V. СРОКОВЕ ЗА СЪХРАНЕНИЕ НА ЛИЧНИ ДАННИ

Дружеството съхранява лични данни за следните срокове:

А) Данните на за ученици, родители и учители се съхраняват в съответствие с изискванията на НАРЕДБА № 8 ОТ 11 АВГУСТ 2016 Г. ЗА ИНФОРМАЦИЯТА И ДОКУМЕНТИТЕ ЗА СИСТЕМАТА НА ПРЕДУЧИЛИЩНОТО И УЧИЛИЩНОТО ОБРАЗОВАНИЕ, подробно описани в Приложение № 1, неразделна част от настоящата вътрешна политика.

Б) Личните данни на служители, съдържащи се в посочените по-долу документи, се съхраняват за срок от 50 години в съответствие със Закона за Националния архивен фонд, Закона за счетоводството и ДОПК:

- ведомости за заплати;
- трудови договори;
- заповеди за преназначаване;
- заповеди за ползван неплатен отпуск над 30 работни дни;
- заповеди за прекратяване на трудови правоотношения;
- трудова книжка.

В) Личните данни на служители, съдържащи се в документи, част от трудовото досие, извън изброените по т. 5.4.2., се съхраняват за срок от 6 месеца след изтичане на сроковете за предявяване на искове за трудови спорове по чл. 358 КТ;

Г) Личните данни на кандидати за работа, които не са одобрени за назначаване в Дружеството, се съхраняват за срока, определен съгласно действащата нормативна уредба в областта на защитата на личните данни, но за не повече от 6 месеца, от приключване на процедурата, след което се връщат на лицето или се унищожават. Личните данни могат да се съхраняват за по-дълъг период с цел отправяне на предложения за работа само при наличие на съгласие на кандидата в писмена форма.

Д) Личните данни съдържащи се в счетоводните документи на Дружеството се съхраняват в сроковете по чл. 12 от Закона за счетоводството;

Е) Личните данни на контрагенти се съхраняват за срок от 5 години след изтичане на срока на договора в съответствие с общата погасителна давност по чл. 110 от ЗЗД;

Ж) Записите от видеонаблюдението се съхраняват за срок от 2 месеца съгласно Закона за частната охранителна дейност.

З) Когато лични данни са предоставени от субекта на данни на администратор или обработващ лични данни без правно основание по чл. 6, параграф 1 от Регламент (ЕС) 2016/679 или в противоречие с принципите по чл. 5 от същия регламент, в срок един месец от узнаването администраторът или обработващият лични данни ги връща, а ако това е невъзможно или изисква несъразмерно големи усилия, ги изтрива или унищожава. Изтриването и унищожаването се документират.

VI. СЪВМЕСТНИ АДМИНИСТРАТОРИ, ОБРАБОТВАЩИ ЛИЧНИ ДАННИ И ТРАНСФЕРИ В ТРЕТИ СТРАНИ

1. Съвместни администратори

Дружеството е съвместен администратор с други дружества, в случаите когато те определят съвместно целите и средствата на обработване на лични данни. Отношенията между Дружеството и останалите съвместни администратори се регламентират с писмена договореност, в която се определят по прозрачен начин съответните отговорности за изпълнение на задълженията по Общия регламент, по-специално що се отнася до упражняването на правата на субекта на данни и съответните им задължения за предоставяне на информация.

2. Обработващи лични данни

Дружеството използва само обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на Общия регламент и Закона за защита на личните данни и да осигурява адекватно ниво на защита на правата на субектите на данни. За целта, преди сключване на договор с обработващ лични данни, Дружеството задължително се запознава с неговата Политика за защита на личните данни, а в договора за предоставяне на услуги се включват стандартни клаузи за защита на личните данни в съответствие с член 28 от Общия регламент.

3. Трансфер на данни в трета държава

Дружеството може да предава лични данни, които се обработват или са предназначени за обработване след предаването на трета държава, при спазване на изискванията на Общия регламент и по-специално на Глава V от него.

Трансферът на лични данни към трета държава се основава на стандартни договорни клаузи за защита на данните, приети от Европейската комисия или от Комисията за защита на личните данни.

В случаите, когато предаването не е повторяемо и засяга само ограничен брой субекти на данни, трансферът може да се основава на някоя от дерогациите по член 49 от Общия регламент, по-специално изрично съгласие на лицето за предаването на данни, след като е било информирано за възможните рискове поради липсата на решение относно адекватното ниво на защита или на подходящи гаранции.

VII. УПРАЖНЯВАНЕ НА ПРАВА ОТ СУБЕКТИ НА ДАННИ

Всяко физическо лице, чийто лични данни се обработват от Администратора, има следните права:

А) Право на достъп да получи от Дружеството потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните, включително и копие от тях, и следната информация:

- целите на обработването;
- съответните категории лични данни;
- получателите и категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави и международни организации;
- когато е възможно, предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;
- съществуването на право да изиска от Администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване;
- правото на жалба до надзорен орган;
- когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;
- съществуването на автоматизирано вземане на решения, включително профилиране;

Когато личните данни се предават на трета държава или на международна организация, субектът на данните има право да бъде информиран относно подходящите гаранции по член 46 във връзка с предаването (**право на достъп**).

Б) Да коригира без ненужно забавяне не неточните лични данни, свързани с него. Като се имат предвид целите на обработването субектът на данните има право непълните лични данни да бъдат попълнени, включително чрез добавяне на декларация (**право на коригиране**).

В) Да поиска от Администратора изтриване на свързаните с него лични данни без ненужно забавяне, а Администраторът има задължението да изтрие без ненужно забавяне личните данни, когато е приложимо някое от посочените основания:

- личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
- субектът на данните оттегля своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването;
- субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество;
- личните данни са били обработвани незаконосъобразно;
- личните данни трябва да бъдат изтрети с цел спазването на правно задължение по правото на ЕС или правото на държава членка, което се прилага спрямо Администратора;
- личните данни са били събрани във връзка с предлагането на услуги на информационното общество (**право на изтриване**).

Г) Да изиска от Администратора ограничаване на обработването, когато се прилага едно от следното:

- точността на личните данни се оспорва от субекта на данните, за срок, който позволява на Администратора да провери точността на личните данни;
- обработването неправомерно, но субектът на данните не желае личните данни да бъдат изтрети, а изисква вместо това ограничаване на използването им;
- Администраторът не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;
- субектът на данните е възразил срещу обработването в очакване на проверка дали законните основания на Администратора имат преимущество пред интересите на субекта на данните (**право на ограничаване**).

Д) Да получи личните данни, които го засягат и които той е предоставил на Администратора, в структуриран, широко използван и прогден за машинно четене формат и има право да прехвърли тези данни на друг администратор без възпрепятстване от Администратора (**право на преносимост**).

Е) По всяко време и на основания, свързани с неговата конкретна ситуация, на възразение срещу обработване на лични данни (**право на възразение**).

Ж) Да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включително профилиране, което поражда правни последствия за субекта на данните или по

подобен начин го засяга в значителна степен (право да не бъде обект на автоматизирано вземане на индивидуални решения, включително профилиране).

VIII. ВЪТРЕШНА ПРОЦЕДУРА ЗА УПРАЖНЯВАНЕ НА ПРАВА ОТ СУБЕКТИ НА ДАННИ

Правата по глава VII от настоящата Политика се упражняват от субекта на данни или от изрично упълномощено от него лице с по един от следните начини:

А) Подаване на писмено заявление на място в Дружеството на адрес: гр. София, ж.к. „Обеля“, ул. „106-та“ №3

Б) По куриер на посочения адрес по буква „А“ от настоящата глава;

В) Искания от субекти на данни може да бъдат получавани и на служебна електронна поща на Дружеството.

В случай че служител получи съобщение на служебната си електронна поща от субект на данни с искане за упражняване на права във връзка с предоставяне на лични данни, той уведомява незабавно Длъжностното лице по защита на личните данни в рамките на работния ден от получаване на съобщението като му изпраща цялата налична кореспонденция;

Ако служител получи искане от субект на данни, в случаите в които служителът извършва доставка на стоки, той указва на искателя за възможностите за подаване на заявление съгласно букви „А“, „Б“ и „В“ от настоящата глава;

Заявленията от субектите на данни се приемат от упълномощен за това служител на Дружеството и се изпращат на Длъжностното лице по защита на личните данни не по-късно от следващия работен ден, който от своя страна ги въвежда в регистър „Упражняване на права по защита на личните данни“;

Служителят задължително проверява самоличността на заявителя в случаите на буква „А“ чрез справка в документ за самоличност, представен от последния. В случай, че упълномощеният за това служител не е в състояние да идентифицира субекта на данни, той отказва да приеме заявлението, като информира лицето за причината и му указва, че за да упражни правата си следва да предостави допълнителна информация, позволяваща неговото идентифициране. Забранява се снемането на копия от документи за самоличност;

Постъпилите заявления се докладват на управителя и/или директора и Длъжностното лице по защита на личните данни, не по-късно от един работен ден след постъпването им, като му се предоставя цялата преписка на хартиен носител или по електронен път. Упълномощеният служител е длъжен да оказва съдействие на управителя и/или директора и длъжностното лице по защита на личните данни, като му предоставя в подходяща форма релевантна към искането

документация, съхраняваща се в Дружеството, в срок до пет дни от уведомяването на управителя и/или директора;

Когато личните данни на заявителя са предоставени на обработващ лични данни, те се изискват от него в писмена форма. Данните се предават от обработващия на представител на Дружеството, а когато това е практически невъзможно или нецелесъобразно, те се изпращат по електронна поща с подходяща защита срещу неразрешен достъп или разкриване (криптиране). Упълномощеното лице предоставя данните получени от обработващия на Длъжностното лице по защита на личните данни ;

Становище по искането за упражняване на права се изготвя от Длъжностното лице по защита на личните данни или управителя и/или директора в случаите на отказ или когато следва да се дадат указания за допълнителния действия на заявителя. Становището се изготвя на хартиен носител и се получава от заявителя на адреса на Дружеството или по друг посочен от заявителя начин, не по-късно от 60 дни от постъпването на искането. В случай че заявителят получава становището на адреса на Дружеството упълномощеният служител проверява самоличността му чрез справка в документ за самоличност, представен от заявителя, и предоставя становището в два екземпляра, по един за всяка страна, подписан от заявителя. Получаването/изпращането на становището се отразява от Длъжностното лице по защита на личните данни в регистър „Упражняване на права по защита на личните данни“, след представянето му от упълномощения служител;

В случаите когато се одобрява искане за упражняване на права от заявител, поисканата информация се предоставя след резолюция от управителя и/или директора на Дружеството. Упълномощеният служител отразява получаването/изпращането на документацията от/до заявителя в регистър „Упражняване на права по защита на личните данни“;

Когато с упражняването на правото си на достъп, заявителят иска и копие от личните му данни, които са в процес на обработване, същите се предоставят на хартиен носител или на CD/DVD, или на друг подходящ носител. Предаването се извършва лично на субекта на данните или на изрично упълномощено от него лице. По изключение лични данни може да бъдат предоставяни по електронна поща или изпратени на адрес с куриер само ако субектът на данните предварително лично или чрез упълномощено трето лице е декларирал писмено или с електронен подпис електронната си поща или адреса си за кореспонденция;

Когато към заявлението за коригиране на лични данни не са приложени официални документи, подкрепящи искането, на лицето се дава възможност да ги представи в разумен срок, като за целта му се изпраща писмо с обратна разписка или на електронна поща;

При постъпване на искане за изтриване на лични данни (право „да бъдеш забравен“), в становището задължително се посочва дали е налице нормативно задължение или друго правно основание за Дружеството да продължи да обработва данните или правен спор с лицето;

В случаите, когато искането за коригиране, изтриване или ограничаване на обработването на лични данни е уважено, Дружеството уведомява за това обстоятелство обработващия лични данни и получателите на данните, ако има такива, в писмена форма, в срок от 5 работни дни;

Искания за преносимост на данните се уважават само ако Дружеството обработва данните по автоматизиран начин и на основание договор или съгласие. В тези случаи данните се предават в някой от следните машинно четими формати (XML, JSON, CSV или други).

IX. ПРОЦЕДУРА ПРИ НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Всеки един случай на нарушение на сигурността на личните данни, които се съхраняват или обработват по друг начин от Дружеството, който води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до данните, се докладва незабавно на управителя и/или директора или на упълномощено лице от персонала на Дружеството. При докладването се посочват, доколкото са известни към момента, естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни.

Дружеството, в качеството му на администратор, се счита за уведомено за нарушението в момента, когато същото е установено от служител на Дружеството или е получено уведомление от обработващ лични данни.

В срок от 48 часа от узнаването, управителят и/или директорът или упълномощено от него лице изготвя проект на уведомление до Комисията за защита на личните данни със следната информация, доколкото е налична:

- описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
- посочване на точка за контакт с Дружеството;
- описание на евентуалните последици от нарушението на сигурността на личните данни;
- описание на предприетите или предложените от Администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

Уведомлението се изпраща на Комисията за защита на личните данни, след като бъде предварително подписано от управителя и/или директора на Дружеството, не по-късно от 72 часа от момента на узнаването по. Ако това е невъзможно по обективни причини, в уведомлението задължително се посочва какво е наложило забавянето. В случай, че надзорният орган е публикувал бланка за подобно уведомление, информацията се изготвя и изпраща в съответната форма.

Нарушението на сигурността на лични данни се съобщава на субектите на данните, ако то може да породи висок риск за правата и свободите им и данните не са защитени чрез криптиране или други подходящи технически и организационни мерки за защита. Съобщаването се извършва писмено, включително по електронна поща. В него се включва описание на евентуалните последици от нарушението на сигурността на личните данни и описание на предприетите или

предложените от Дружеството мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните негативни последици.

Дружеството документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. В документацията се включва и копие от цялата кореспонденция по случая.

Х. ЗАДЪЛЖЕНИЕ ЗА ИНФОРМИРАНост

Дружеството предприема необходимите мерки за предоставяне на кратка, прозрачна, разбираема и лесно достъпна информация на субектите на данни относно следното:

- Данните, които идентифицират Администратора и координатите за връзка с него;
- Координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;
- Целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;
- Получателите или категориите получатели на личните данни;
- Срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използване за определяне на този срок;
- Правата на субектите на данни;
- Правото на жалба до Комисията за защита на личните данни;
- Дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени;
- Когато е приложимо, намерението на Администратора да предаде личните данни на трета държава или международна организация;
- Съществуването на автоматизирано вземане на решения, включително профилиране.

Дружеството предоставя горепосочената информация по следния начин:

А) Когато е приложимо, информацията се публикува на интернет страницата на Администратора по начин, по който субектите на данни лесно да достъпят;

Б) Поставя се на видно място в офиса/сградата на Администратора, така че да се сведе до знанието на субектите на данни;

В) Служителите на Дружеството, когато извършват дейностите по доставка, описани в глава IV, точка 1, буква „А“, разполагат с разпечатана информацията, която се предоставя на субектите на данни при поискване.

Информацията се актуализира своевременно при необходимост и се свежда до знанието на субектите на данни по начините, описани по-горе.

Информацията относно видеонаблюдението се предоставя и чрез поставяне на информационни табели на подходящи места в съответствие със Закона за частната охранителна дейност.

XI. РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ

Дружеството поддържа вътрешен регистър на дейностите по обработване на лични данни в съответствие с член 30 от Регламент 2016/679 със следната информация:

- Името и координатите за връзка на администратора, а когато е това е приложимо на всички съвместни администратори, на представителя на администратора и на длъжностното лице по защита на данните, ако има такива;
- Целите на обработването;
- Описание на категориите субекти на данни и на категориите лични данни;
- Категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
- Когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификация на тази трета държава или международна организация;
- Когато е възможно, предвидените срокове за изтриване на различните категории данни;
- Когато е възможно, общо описани на техническите и организационни мерки за сигурност.

Регистрите се поддържат в писмена форма, включително в електронен формат.

XII. МЕРКИ ЗА СИГУРНОСТ

1. Физическа защита

Мерките за физическа защита включват, но не само, изброените по-долу параметри:

- С всички хартиени и електронни документи, съдържащи лични данни работят само служители в кръга на служебните им задължения в съответствие с принципа „Необходимост да се знае“.
- Документите на хартиен носител се съхраняват в заключени шкафове, достъп до които имат упълномощените за това служители;
- Документите на електронен носител се съхраняват на служебните компютри на Дружеството, които са защитени с персонален акаунт и парола за всеки служител. Електронни документи се съхраняват и на техническо устройство (флаш памет), което е защитено с уникална парола за достъп;
- Вратите и помещенията в офиса на Дружеството са защитени чрез заключването им и поставяне на алармена система за сигурност;

- Дружеството има приета противопожарна система за безопасност и реагиране в случай на пожар в помещенията. Офисите на Администратора имат климатизация.

2. Документална защита

Мерките за документална защита включват, но не само, изброените по-долу параметри:

- Определяне на регистри от управителя и/или директора на Дружеството, които се поддържат на хартиен носител, както и служителите пряко отговорни за тяхното поддържане;
- Документите на хартиен носител, съдържащи лични данни, които вече не са необходими и/или липсва правно основание за тяхното по-нататъшно съхранение, се унищожават по сигурен начин, по-специално чрез шредирание, изгаряне или по друг подходящ начин, гарантиращ тяхното унищожаване;
- Документи с лични данни могат да бъдат копирани/сканирани и разпространявани между служителите на Дружеството в съответствие с принципа на „Необходимост да се знае“.

3. Мерки за персонална защита

Мерките за персонална защита включват, но не само, изброените по-долу параметри:

- Познаване на нормативната уредба в областта на защитата на лични данни, както и на Политиката за защита на личните данни на Дружеството;
- Забрана за споделяне между персонала на персонални идентификатори, пароли за достъп и друга подобна конфиденциална информация;
- Обучение на служителите непосредствено след наемането им и най-малко веднъж годишно;
- Тренировки на персонала за реакция при събития, застрашаващи сигурността на данните, като част от обучителната програма на служителите;
- Поемане на задължение от служителите за неразгласяване на лични данни, до кои са получили достъп при и по повод изпълнението на задълженията си.

Когато служител постъпва за първи път на работа, управителя и/или директора на Дружеството предприема необходимите действия, новият служител да бъде запознат с изискванията на настоящата Политика.

При провеждането на обученията на служителите, управителя и/или директора или упълномощени от него лица запознават служителите с изискванията и последствията от нарушаване на конфиденциалността на информацията, включително за възможността от налагане на дисциплинарни наказания по Кодекса на труда.

4. Мерки за информационна защита

Мерките за информационна защита включват, но не само, изброените по-долу параметри:

- Определяне на регистри от управителя и/или директора на Дружеството, които се поддържат на електронен носител, както и служителите пряко отговорни за тяхното поддържане;

- Използването на вътрешни мрежи за достъп до интернет се извършва само от служителите на Дружеството. Забранено е предоставянето на парола за достъп до вътрешните мрежи за външни лица;
- Администраторът 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. Служебните компютри на Дружеството следва да бъдат защитени с актуални антивирусни програми;
- Забранява се на служителите да използват програми и софтуери, които могат да доведат до неоторизиран достъп до базата данни на Дружеството;
- Технически средства, в които се съхраняват лични данни, се унищожават по сигурен начин, по който не може да се възстанови информацията.

XIII. ОЦЕНКА НА ВЪЗДЕЙСТВИЕ

Когато съществува вероятност определен вид обработване да породи висок риск за правата и свободите на физическите лица, по-специално поради използване на нови технологии за мащабно обработване на специални категории данни, като се отчита и естеството, обхвата, контекста и целите на обработването, преди да бъде извършено обработването Дружеството извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни по реда на чл. 35 от Общия регламент за защита на данните.

Дружеството се консултира с Комисията за защита на личните данни преди обработването, когато оценката на въздействието върху защитата на данните предходния абзац покаже, че обработването ще породи висок риск, и то не възнамерява или не е в състояние да предприеме мерки за ограничаване на този риск. В тези случаи се прилага процедурата по чл. 36 от Общия регламент за защита на данните.

XIV. КОНТРОЛ И ВЪТРЕШНА ОТЧЕТНОСТ

Общият контрол за спазване на настоящата Политика за защита на личните данни се осъществява от управителя и/или директора на Дружеството или от упълномощенот от него лице.

Всички служители на Дружеството имат достъп и следва да бъдат запознати с правилата на настоящата Политика за защита на личните данни.

Документацията по защита на личните данни се съхранява от управителя и/или директора или изрично упълномощено от него лице за това.

При поискване, Дружеството осигурява достъп до документацията по защита на личните данни на Комисията за защита на личните данни.

Настоящата Политика за защита на личните данни подлежи на преразглеждане и актуализиране всяка година, както и до две седмици от всяка промяна, влязла в сила, на законодателството в областта на защитата на личните данни и което създава необходимост от промяна на Политиката.

Промени в настоящата Политика за защита на личните данни се извършват при обоснована необходимост по същия ред, по който е приета.

Утвърдил:

/д-р Илия Емелов – Изп. директор/

