



УТВЪРДИЛ:

НЕЛИ ПЕТРОВА-ДИМИТРОВА
ПРЕДСЕДАТЕЛ НА УС НА ИСДП

ПРАВИЛА
ЗА МЕРКИТЕ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА
СДРУЖЕНИЕ „ИНСТИТУТ ПО СОЦИАЛНИ ДЕЙНОСТИ И ПРАКТИКИ“

ПРЕАМБЮЛ

Сдружение „Институт по социални дейности и практики“, наричано по-долу ИСДП, е българска неправителствена организация, регистрирана като юридическо лице с нестопанска цел в обществена полза. ИСДП е вписано в Регистъра на юридическите лица с нестопанска цел при Министерството на правосъдието под № 20040401008.

ИСДП е администратор на лични данни по смисъла на Закона за защита на личните данни.

Настоящите Правила за мерките за защита на личните данни, наричани по-долу Правилата, се приемат в изпълнение на Регламент (ЕС) 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 относно защитата на данните), наричан по-долу Регламента, и Закона за защита на личните данни. Те засягат техническите 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, при осъществяване на дейността на сдружението, а именно:

1. Предоставяне на социални услуги, като доставчик на социални услуги по смисъла на Закона за социални услуги (ЗСУ);
2. Разработване на изследвания, провеждане на обучения и супервизии и оказване на професионална подкрепа в областта на социалните услуги и относно децата и семействата в риск;
3. ИСДП като работодател на служители, наети по трудово правоотношение;
4. ИСДП като възложител на услуги – на физически лица по нетрудови правоотношения;

Мерките за защита осигуряват ниво на защита, което съответства на рисковете, свързани с обработването, и на естеството на данните, които трябва да бъдат защитени.

I. Принципи

Чл. 1. Принципите в работата по обработка на данните включват:

1. Прозрачност;
2. Справедливост;
3. Законосъобразност;
4. Сигурност;
5. Интегритет.

II. Регистри

Чл. 2. ИСДП поддържа следните регистри:

1. **Регистър „ПОТРЕБИТЕЛИ НА СОЦИАЛНИ УСЛУГИ ЗА ДЕЦА И СЕМЕЙСТВА“.** Данните в този регистър се обработват във връзка с предоставянето на социални услуги от ИСДП като доставчик на социални услуги по смисъла на ЗСУ;
2. **Регистър „ВИДЕОНАБЛЮДЕНИЕ“.** Данните в този регистър се обработват във връзка с осигуряване сигурността и безопасността на потребители на социални услуги, чиито доставчик е ИСДП;
3. **Регистър „ОБУЧЕНИЯ, ЗАПИТВАНЯ И ЗАЯВКИ“.** Данните в този регистър се обработват по повод извършваните от ИСДП обучения, супервизии и консултации и издаваните във връзка с тях сертификати и удостоверения;
4. **Регистър „УПРАВЛЕНИЕ НА ЧОВЕШКИТЕ РЕСУРСИ“.** Данните в този регистър се обработват във връзка със сключване на трудови и граждански договори, изчисляване и изплащане на възнаграждения и хонорари по тях, съхраняване на информация за доказване на трудов и осигурителен стаж;
5. **Регистър „КОНТРАГЕНТИ“.** Данните в този регистър се обработват по повод на дарители, доставчици, клиенти, и контрагенти по сключени договори във връзка с осъществяване на дейността на ИСДП.

III. Носител на лични данни

Чл. 3. Препоръчителният вид на носителите на данните за трайно съхраняване са:

1. хартиен носител;
2. електронен носител (на компютър или крипто флаш памет).

IV. Лица, които отговарят за обработката на лични данни

Чл. 4. Лицата, които отговарят за обработката на лични данни, както и техните права и задължения, се определят от изпълнителния директор на ИСДП в зависимост от целите и мястото на обработването.

V. Мерки за осигуряване на защита

Чл. 5. Препоръчителни мерки за осигуряване на необходимото ниво на защита на личните данни съобразено с вида и чувствителността на данните са:

- заключване на документи и досиета, съдържащи лични данни в шкафове (метални и други);
- отделен сървър за съхранение на данните;
- работа на компютър с антивирусна програма;
- изключване на компютрите след работа;
- заключване на интернет достъпа (Wi-Fi мрежата) за трети лица чрез парола.

VI. Спецификация на техническите ресурси

Чл. 6. Препоръчителните техническите ресурси за обработка на личните данни са:

1. компютри и крипто флаш памет – за данните в електронен вид;
2. класъори и папки – за данните в хартиен вид.

VII. Организационна процедура за обработване

Чл. 7. Организационната процедура за обработване на личните данни, включва време, място и ред за обработване.

1. Всяка информация, свързана с работа по конкретен случай или потребител, служител, дарител и контрагент се обработва от лицето, което отговаря за обработката на личните данни.
2. Няма достъп на трети лица до техническите ресурси за обработка на личните данни.

VIII. Мероприятия за защита при аварии, произшествия и бедствия

Чл. 8. Мероприятията за защита на техническите и информационните ресурси при аварии, произшествия и бедствия като пожар, наводнение и други форсмажорни обстоятелства са метална врата и шкафове.

IX. Средства за предотвратяване на умишлено или небрежно повреждане или нерегламентиран достъп

Чл. 9. Средствата за предотвратяване на умишлено или небрежно повреждане или нерегламентиран достъп до личните данни са антивирусни програми, пароли на компютрите, пароли на електронната поща, заключване на интернет достъпа (Wi-Fi мрежата) за трети лица чрез парола, заключване на шкафовете; СОТ.

X. Ред за унищожаване на информационни носители

Чл. 10. (1) След изтичане на срока за съхранение информационните носители на данни се

унищожават както следва:

1. Унищожаването на електронните файлове се извършва чрез тяхното изтриване, лично от лицето, което отговаря за обработката на личните данни.
2. Унищожаването на информацията от сървъра, се извършва чрез нейното изтриване, от лицето, което е натоварено да отговаря за поддръжката.
3. Унищожаването на хартиените носители се извършва чрез нарязване от машина за унищожаване на документи (шредер), след изготвяне на протокол за унищожаването на съответните документи от Комисия, определена от изпълнителния директор и/или ръководителя на всяка социална услуга.

(2) Унищожаването на информационните носители се осъществява, съгласно Вътрешни правила за архивиране на информацията във всяка услуга.

XI. Профилактика на комуникационните средства

Чл. 11. ИСДП провежда редовна профилактика на комуникационните средства чрез проверка за вируси, за нелегално инсталиран софтуер и актуализиране на антивирусните програми.

XII. Обекти, в които ще се обработват данните

Чл. 12. (1) Лични данни са обработват в следните обекти:

1. Централен офис – гр. София, ул. Пиротска 175;
2. Адресът на предоставяне на съответната социална услуга.

(2) Обектите, в които се обработват лични данни се охраняват чрез СОТ.

(3) Достъпът до помещенията, в които се обработват лични данни, е ограничен за външни лица.

(4) Мерките за ограничаване на достъпа до данните включват заключване на регистрите и индивидуалните досиета в шкафове, пароли на компютрите, пароли на електронната поща и заключване на интернет достъпа (Wi-Fi мрежата) за трети лица чрез парола.

(5) Мерките за защита при предаване на данните по електронен път обхващат стандартна защита чрез антивирусна програма и парола на електронните пощи.

XIII. Осигуряване на достъп на лицата до личните им данни

Чл. 13. (1) Всяко физическо лице има право на достъп до отнасящи се за него лични данни.

(2) В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, ИСДП предоставя на съответното физическо лице достъп до частта от тях, отнасяща се само за него.

(3) Правото на достъп до лични данни се осъществява с писмено заявление по образец (Приложение № 1) на адрес: гр. София, ул. „Пиротска“ № 175.

(4) Заявлението се отправя лично от физическото лице, от упълномощен от него адвокат чрез адвокатско пълномощно по Закона за адвокатурата или от изрично упълномощено от него лице чрез нотариално заверено пълномощно.

(5) Заявлението за достъп до лични данни 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;
5. пълномощно, когато заявлението се подава от упълномощено лице.

(6) Заявлението за достъп до лични данни се завежда в общия входящ регистър на ИСДП.

(7) Достъп 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 на предпочитан носител.

(8) ИСДП разглежда заявлението за достъп до лични данни и се произнася в 14-дневен срок от неговото подаване. Този срок може да бъде удължен до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни.

(9) В 14-дневен срок ИСДП взема решение за предоставянето на пълна или частична информация на заявителя или мотивирано отказва предоставянето ѝ, като уведомяването за това заявителя лично срещу подпис или по пощата с обратна разписка.

XIV. Осигуряване на достъп на трети лица до лични данни, обработвани от ИСДП (правомерен достъп)

Чл. 14. Освен лицето, което отговаря за обработката на личните данни, **правомерен** е достъпът до лични данни на: председателя на УС; изпълнителния директор на ИСДП; завеждащия ТРЗ; главния счетоводител, програмните директори, като при поискване от тяхна страна, лицето, което отговаря за обработката на личните данни, им осигурява достъп.

Чл. 15. (1) Никое друго трето лице няма право на достъп до регистъра с личните данни на лицата, освен ако достъпът е изискан по надлежен път от орган на надзора (Комисия за защита на личните данни) или на съдебната власт (Комисия за финансов надзор, съд, прокуратура, следствени органи и др.). Достъпът на тези органи до личните данни на лицата е правомерен.

(2) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирани се със съответни документи – писмени разпореждания на съответния орган, в които се посочва основанието, имената на лицата, когато за целите на дейността им е необходимо да им се осигури достъп до данните.

(3) При промени в статуса на ИСДП, налагащи прехвърляне на личните данни на друг администратор на лични данни, предаването се извършва след разрешение на Комисията за

защита на лични данни (КЗЛД).

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

XV. Контрол

Чл. 16. Контролът върху дейностите по обработка на личните данни се осъществява от изпълнителния директор на ИСДП.

XVI. Основания за назначаване на длъжностно лице по защита на данните

Чл. 17. Не са налице основания за назначаване на длъжностно лице по защита на данните, тъй като основните дейности на ИСДП не се състоят в операции по обработване, които поради своето естество, обхват или цели да изискват редовно и систематично мащабно наблюдение на субектите на данните.

ПРИЛОЖЕНИЯ

Приложение № 1 – Образец на Заявление за достъп до лични данни;

Приложение № 2 – Образец на Искане за изтриване на лични данни;

Приложение № 3 – Образец на Исканеза коригиране на лични данни;

Приложение № 4 – Образец на Декларация – съгласие за обработване на лични данни за предоставяне на социални услуги, обучителни и други услуги;

Приложение № 5 – Образец на Декларация – съгласие за обработване на лични данни на кандидати за работа;

Приложение № 6 – Регистър „ПОТРЕБИТЕЛИ НА СОЦИАЛНИ УСЛУГИ ЗА ДЕЦА И СЕМЕЙСТВА“;

Приложение № 7 – Регистър „ВИДЕОНАБЛЮДЕНИЕ“;

Приложение № 8 – Регистър „ОБУЧЕНИЯ, ЗАПИТВАНИЯ И ЗАЯВКИ“;

Приложение № 9 – Регистър „УПРАВЛЕНИЕ НА ЧОВЕШКИТЕ РЕСУРСИ“;

Приложение № 10 – Регистър „КОНТРАГЕНТИ“.

Настоящите Правила влизат в сила от 01.10.2018 година.

Настоящите Правила са актуализирани на 01.09.2023 година.