ПРИЛОЖЕНИЕ № 8 · ПУБЛИЧНО ИЗВЛЕЧЕНИЕ

Политика за защита на личните данни и срокове за съхранение

Сдружение „Мобилен център за приобщаване и развитие - Пловдив“ · ЕИК 208681061

Версия 1.0 / 12.02.2026 г. - Протокол № 1 на УС. Консолидиран източник: Организационен наръчник, утвърден с Протокол № 3 / 17.03.2026 г., т. 2.

Публично текстово извлечение от българския оригинал. Изданието от 26.09.2026 г. е техническо оформление за сайта, без ново приемане или съдържателно изменение. Вътрешните бланки, регистри и полета за подпис не се публикуват. Заличаването на личния адрес е обозначено.

Сдружението не е лицензиран доставчик на социални услуги по ЗСУ. Уредените в документа бъдещи или условни дейности не означават, че се предоставят в момента, и не заменят необходимите разрешения.

Бележка към публичното копие: чл. 27 е запазен според приетия текст. Разликата между него и международното обработване, допустимо по условията на платформата на сайта, изисква решение на УС. Актуалното уведомление за сайта е на страницата „Поверителност“.

Официален оперативен имейл: mobilencentrplovdiv@gmail.com

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Цел на политиката Настоящата политика има за цел да уреди обработването, съхранението, защитата и унищожаването на лични данни, събирани и обработвани от Сдружение „Мобилен център за приобщаване и развитие – Пловдив“ (наричано по-нататък „Организацията“) във връзка с осъществяваната от него дейност – мобилна образователна и психологическа подкрепа, социално посредничество, онлайн консултации, проектна дейност, администрация и комуникация.

Чл. 2. Обхват Политиката се прилага за всички членове на Управителния съвет, служители, външни експерти, стажанти и доброволци, които имат достъп до лични данни, обработвани от или от името на Организацията.

Чл. 3. Приложимо законодателство Политиката е разработена в съответствие с: Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните – GDPR); Закона за защита на личните данни (ЗЗЛД) на Република България; Секторното законодателство, приложимо към дейността на Организацията.

II. ОСНОВНИ ПРИНЦИПИ НА ОБРАБОТВАНЕ

Чл. 4. Организацията обработва лични данни при спазване на следните принципи: Законосъобразност, добросъвестност и прозрачност – данните се обработват законосъобразно, добросъвестно и по прозрачен начин спрямо субекта на данни. Ограничение на целите – данните се събират за конкретни, изрично указани и легитимни цели и не се обработват по начин, несъвместим с тези цели. Минимизиране на данните – обработват се само данни, които са подходящи, свързани с и ограничени до необходимото във връзка с целите, за които се обработват. Точност – данните са точни и при необходимост се актуализират; предприемат се разумни мерки за своевременно заличаване или коригиране на неточни данни. Ограничение на съхранението – данните се съхраняват във форма, която позволява идентифицирането на субекта за период, не по-дълъг от необходимото за целите на обработването. Цялостност и поверителност – данните се обработват по начин, който гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане. Отчетност – Организацията е в състояние да докаже спазването на горепосочените принципи.

III. КАТЕГОРИИ ЛИЧНИ ДАННИ И ПРАВНИ ОСНОВАНИЯ

Чл. 5. Категории субекти на данни Организацията обработва лични данни на следните групи физически лица: Потребители на услуги (възрастни и деца) и техни родители/настойници; Членове на УС, служители, външни експерти и доброволци; Партньори и контактни лица на организации – партньори; Дарители и спонсори – физически лица; Кандидати за работа и стаж.

Чл. 6. Категории обработвани данни В зависимост от конкретната дейност могат да се обработват следните категории данни: Категория Примери Идентификационни данни Имена, ЕГН (когато се изисква по закон), дата на раждане Контактни данни Телефон, имейл, адрес Данни за контакт при спешност Име и телефон на родител/настойник Данни във връзка с предоставяне на услуга Заявена услуга, дата и час на посещение, работни бележки (без медицински диагнози) Данни за трудови/граждански правоотношения Трудов стаж, квалификация, банкова сметка Данни за отчетност по проекти Присъствени списъци, снимков материал (със съгласие), протоколи Данни за дарения Име на дарител, сума, дата

Чл. 7. Специални категории данни Организацията не обработва специални категории лични данни (здравословно състояние, биометрични или генетични данни, данни за сексуален живот и др.), освен ако: това не се налага от конкретен проект или услуга, и е налице изрично писмено съгласие на субекта, и е предвидено в договор с финансираща институция, като във всички случаи се прилагат най-високи стандарти за защита.

Чл. 8. Правни основания за обработване Организацията обработва лични данни само при наличие на някое от следните основания: Изпълнение на договор (например предоставяне на мобилна педагогическа, психологическа подкрепа или

социално посредничество); Спазване на законово задължение (например счетоводна отчетност); Легитимен интерес (например организация на работния процес, комуникация с партньори), при условие че интересите на Организацията не противоречат на основните права на субекта; Изрично съгласие – в случаите, когато няма друго основание (например за снимков материал); Обществен интерес или жизненоважни интереси на субекта (в изключителни случаи). При съмнение се прилага най-консервативният подход и основанието се документира.

IV. ИНФОРМИРАНЕ И ПРАВА НА СУБЕКТИТЕ

Чл. 9. Информация при събиране на данните При събиране на лични данни Организацията предоставя на субектите следната информация (в достъпна и разбираема форма): Идентичност и данни за контакт на администратора; Целите и правното основание за обработване; Получателите на данните (ако има такива); Срок на съхранение; Наличие на право на достъп, коригиране, изтриване и др.; Право на жалба до КЗЛД.

Чл. 10. Права на субектите на данни Всяко физическо лице, чиито лични данни се обработват, има следните права: Право на достъп – да получи потвърждение дали данните му се обработват и да получи копие от тях; Право на коригиране – да поиска поправка на неточни данни; Право на изтриване (право „да бъдеш забравен“) – при определени условия; Право на ограничаване на обработването; Право на възражение срещу обработване; Право на преносимост на данните – да получи данните в структуриран вид; Право да не бъде обект на автоматизирано вземане на решения, включващо профилиране.

Чл. 11. Процедура по упражняване на правата Исканията се подават писмено на електронна поща [mobilencentrplovdiv@gmail.com] или на адреса на управление. При необходимост Организацията може да изиска допълнителна информация за потвърждаване на самоличността на заявителя. Отговор се предоставя в едномесечен срок (с възможност за удължаване с два месеца при сложни искания, като заявителят се уведомява). Отказът за предоставяне на информация се мотивира писмено.

V. СРОКОВЕ ЗА СЪХРАНЕНИЕ

Чл. 12. Общи правила Организацията съхранява личните данни само за периода, необходим за изпълнение на целите, за които са събрани. След изтичане на срока данните се унищожават, анонимизират или архивират по начин, който не позволява идентификация, освен ако закон не изисква по-дълго съхранение.

Чл. 13. Конкретни срокове

Вид документ/данни	Максимален срок на съхранение	Основание/бележка
Заявления за услуга, контактни данни на неактивни потребители	До 12 месеца след последния контакт	След това се изтриват, ако няма друго основание
Работни бележки, досиета на потребители (без медицински данни)	5 години след приключване на услугата	За проследяване и вътрешен анализ
Финансово-счетоводни документи (фактури, договори, ведомости)	10 години	Съгласно Закона за счетоводството
Документи по проекти (вкл. присъствени списъци, отчети)	5–10 години според изискванията на донора	След изтичане на договорения срок се преценява нуждата от архивиране
Трудови досиета на служители	50 години след напускане	Съгласно Кодекса на труда
Снимков и видеоматериал	Съгласно изрично дадено съгласие, но не повече от 5 години	При липса на съгласие – не се заснемат или веднага се изтриват
Данни за дарения (физически лица)	5 години след края на годината на дарението	За данъчни цели и отчетност
Кореспонденция с партньори	До 3 години след последния контакт	При необходимост се преценява

Чл. 14. Унищожаване на данните Хартиени документи – се унищожават чрез шредиране или предаване на лицензирана фирма за унищожаване. Електронни данни – се изтриват сигурно (чрез софтуер за сигурно изтриване или форматиране на носителите).

VI. ДОСТЪП, РОЛИ И ВЪТРЕШЕН КОНТРОЛ

Чл. 15. Принцип на минимален достъп Достъп до лични данни имат само лица, на които това е необходимо за изпълнение на служебните им задължения (принцип „необходимост да знае“).

Чл. 16. Нива на достъп Ниво 1 (Администратор) – председател на УС: пълен достъп до всички данни. Ниво 2 (Ръководител проект/услуга) – достъп до данни, свързани с конкретен проект/услуга. Ниво 3 (Изпълнител – експерт, доброволец) – достъп само до данни на конкретни потребители, с които работи. Ниво 4 (Счетоводство) – достъп до финансови и трудови данни.

Чл. 17. Регистър на достъпите Води се електронен или писмен регистър, в който се отразява: кой е имал достъп; кога; до какви данни; с каква цел. Регистърът се съхранява най-малко 5 години.

Чл. 18. Задължения на лицата с достъп Всички лица, които обработват лични данни, са длъжни: да пазят данните в тайна; да не ги споделят в незащитени канали (лични чатове, незащитен имейл); да използват само предоставените от Организацията средства за достъп; незабавно да докладват за съмнения за нарушение на сигурността.

VII. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА СИГУРНОСТ

Чл. 19. Минимални технически мерки Двуфакторно удостоверяване (2FA) – задължително за всички акаунти в Google Workspace, CRM системи и др. Силни пароли – минимум 12 знака, с главни и малки букви, цифри и специални знаци; задължителна смяна при съмнение за компрометиране. Мениджър на пароли – използване на одобрен мениджър за съхранение на пароли. Шифроване – всички устройства, съхраняващи лични данни, се шифроват; преносимите носители – само при необходимост и с шифроване. Защитени cloud услуги – Google Drive за съхранение на документи с контрол на достъпа (права „само за четене“/„редакция“ според ролята). Антивирусна защита – на всички устройства.

Чл. 20. Организационни мерки Политика за чисто бюро – не се оставят документи с лични данни на видими места в офиса. Забрана за локално съхранение – данни не се съхраняват на локални дискове, освен ако не е неизбежно и само при наличие на шифроване. Редовни бекъпи – ежеседмично архивиране на критични данни, с проверка за възстановяване веднъж месечно. Обучения – всички лица с достъп преминават през начално и периодично обучение за защита на данните. Специфични мерки при мобилна работа на терен: Предвид спецификата на предоставяните услуги в естествената среда на потребителите, се въвеждат следните задължителни правила за работа с физически носители (бланки, скрининг форми, еко-карти): Транспортиране: Всички хартиени документи се транспортират до и от адреса на посещението единствено в непрозрачни, затворени папки или чанти. Абсолютно се забранява оставянето на попълнени документи без надзор в автомобила на Сдружението. Работа в дома: По време на сесията в дома на потребителя, попълнените формуляри не се оставят на видни места, достъпни за трети лица (вкл. разширеното семейство или външни посетители). Дигитализиране и унищожаване: След приключване на мобилната визита, водещият специалист или координаторът е длъжен във възможно най-кратък срок да въведе данните от хартиените носители в защитеното облачно пространство на Сдружението. След успешно дигитализиране, работните хартиени бланки се унищожават (чрез шредер) или се архивират в заключен шкаф, като изнасянето им отново на терен е строго забранено.

Чл. 21. Използване на лични устройства Лични устройства (BYOD) се допускат само при изрично разрешение и при условие, че са изпълнени следните изисквания: устройството е заключено с парола/биометрия; данните се съхраняват само в защитеното облачно пространство на Организацията, не локално; при загуба/кражба незабавно се уведомява ръководството.

VIII. ИНЦИДЕНТИ СЪС СИГУРНОСТТА

Чл. 22. Дефиниция за инцидент Инцидент със сигурността е всяко събитие, което води до случайно или незаконосъобразно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни.

Чл. 23. Процедура при инцидент Констатиране и ограничаване – лицето, забелязало инцидента, незабавно преустановява достъпа (ако е възможно) и уведомява председателя на УС. Оценка на риска – председателят (или определено лице) оценява вероятните последици за засегнатите лица. Документиране – попълва се Регистър на инцидентите, съдържащ: дата, описание, засегнати данни, предприети действия. Уведомяване на КЗЛД – при риск за правата и свободите на физическите лица, в срок до 72 часа от узнаването, се подава уведомление до Комисията за защита на личните данни. Уведомяване на засегнатите лица – ако съществува висок риск, без ненужно забавяне се уведомяват засегнатите лица и се предоставя информация за препоръчани мерки за защита. Последващи действия – анализ на причините и предприемане на мерки за недопускане в бъдеще.

IX. ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ (ДЛЗД)

Чл. 24. Съгласно чл. 37 от GDPR, Организацията не е задължена да назначава ДЛЗД, тъй като обработването на данни не попада в категориите, изискващи задължително назначаване. Въпреки това функциите по наблюдение на спазването на политиката се възлагат на член на УС, определен с решение на УС.

Чл. 25. Контакт за въпроси, свързани със защитата на данните За всички въпроси, искания и сигнали, свързани с лични данни, може да се обръщате към:

Име: Борис Русев – председател на УС Имейл: mobilencentrplovdiv@gmail.com Адрес: [личният адрес е заличен в публичното копие]

X. ПРЕДОСТАВЯНЕ НА ДАННИ НА ТРЕТИ СТРАНИ

Чл. 26. Общо правило Лични данни не се предоставят на трети лица, освен ако: това се изисква от закона (например пред НАП, МТСП, съд); е необходимо за изпълнение на договор с подизпълнител (например счетоводител, IT поддръжка), като с подизпълнителя се сключва договор, съдържащ клаузи за защита на данните; е налице изрично съгласие на субекта.

Чл. 27. Предаване на данни в чужбина Организацията не предава лични данни в трети държави (извън ЕС/ЕИП). Ако в бъдеще възникне такава необходимост, ще се прилагат всички изисквания на Глава V от GDPR.

XI. ОТГОВОРНОСТ И САНКЦИИ

Чл. 28. Неспазването на изискванията на настоящата политика от членове на екипа, експерти или доброволци може да доведе до: дисциплинарна отговорност (при служители); прекратяване на договорните отношения (при външни изпълнители); отстраняване от доброволческата програма (при доброволци); предявяване на иск за обезщетение, ако са причинени вреди на Организацията или трети лица.

Чл. 29. Организацията носи отговорност пред контролните органи и засегнатите лица за вреди, причинени от неправомерно обработване на лични данни, съгласно приложимото законодателство.

XII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 30. Настоящата политика е приета с решение на Управителния съвет на Сдружението (Протокол № 1 / 12.02.2026 г.) и влиза в сила от датата на приемането си.

Чл. 31. Политиката подлежи на преглед и актуализация при необходимост, но най-малко веднъж на всеки две години, както и при промени в законодателството или в дейността на Организацията.

Чл. 32. Всички лица, обработващи лични данни от името на Организацията, са длъжни да се запознаят с настоящата политика и да я спазват стриктно. Приложения: Декларация за информирано съгласие (за снимков материал/допълнителни данни) Формуляр за упражняване на права от субекти на данни Регистър на дейностите по обработване (вътрешен) Регистър на инциденти със сигурността