ВЪТРЕШНИ ПРАВИЛА

на СДРУЖЕНИЕ „СИП БЪЛГАРИЯ “

за защита на личните данни съгласно Регламент 2016/679

(приети с Решение на Общото събрание от 14.04.2021 г.)

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите Вътрешни правила уреждат организацията на обработване и защитата на личните данни на учредителите, служителите и членовете на органите на Сдружение “СИП България“, на потребителите на предоставяните от него социални услуги, на неговите дарители и партньори, както и на всички други групи физически лица, с които сдружението влиза в отношения при осъществяването на дейността си.

Чл. 2. Сдружение “СИП България” (по-нататък „сдружението“ или „администратора“) събира и обработва лични данни в съответствие с действащите разпоредби за защита на личните данни – 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 – ОРЗД) и др. – и предприема всички необходими действия за осигуряване на съответствие със законовите и нормативни изисквания.

Чл. 3. Сдружението спазва следните нормативно установени принципи, свързани с обработването на лични данни:

- **законосъобразност, добросъвестност и прозрачност** – обработване на личните данни законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните;
- **ограничение на целите** – събиране на личните данни за конкретни, изрично указани и легитимни цели, без да се обработват по-нататък по начин, несъвместим с тези цели;
- **свеждане на данните до минимум** – подходящи лични данни, свързани със и ограничени до необходимото във връзка с целите, за които се обработват;
- **точност** – поддържаане на данните в актуален вид и предприемане на всички разумни мерки за гарантиране своевременното изтриване или коригиране на неточни данни, при отчитане на целите на обработването**;**
- **ограничение на съхранението** – съхраняване на данните за период, не по-дълъг от необходимия за целите на обработването;
- **цялостност и поверителност** – обработване по начин, гарантиращ подходящо ниво на сигурност, като се прилагат подходящи технически или организационни мерки.

Чл. 4 При събиране, обработване и съхраняване на личните данни на субектите на данни сдружението съблюдава още:

1. необходимостта от гарантиране неприкосновеността на личността и личния живот на субекта на данни;

2. правилото „необходимост да се знае“ – обработване на данните само от лица, чиито служебни задължения изискват обработване на съответните данни.

Чл. 5. (1) Лични данни, отнасящи се до здравословното състояние, се обработват за служителите на сдружението, с оглед изпълнение на задълженията на сдружението в областта на трудово-осигурителното законодателство, както и за участниците, помощниците и ръководителите на мероприятията организирани от сдружение "СИП България" с оглед адекватната грижа за тяхното здраве по време на конкретното мероприятие и изпълнението на законови задължения на администратора.

(2) Обработването на лични данни въз основа на съгласие по смисъла на чл. 4, т. 11 от ОРЗД става след подписване на писмена декларация от субекта на данните.

(3) Сдружението не извършва автоматизирано вземане на индивидуални решения по смисъла на чл. 22 от ОРЗД и субектите, чиито данни обработва, не са обект на такива решения.

Чл. 6. (1) Сдружението може да обработва лични данни самостоятелно или чрез трети лица, в качеството им на обработващи лични данни, на основание сключен с тях договор.

(2) Дейностите по осигуряване на здравословни и безопасни условия на труд се уреждат по договор със служба по трудова медицина по реда на Наредба № 3 от 25 януари 2008 г. за условията и реда за осъществяване дейността на службите по трудова медицина.

II. РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 7. (1) Като администратор на лични данни, Сдружение „СИП Бълария" води регистър на дейностите по обработване на лични данни (РДОЛД) – Приложение № 1, представляващо неразделна част от настоящите Вътрешни правила.

(2) РДОЛД съдържа следната информация:

- името и координатите за връзка на администратора и на представителя на администратора;
- 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;
- предвидените срокове за изтриване на различните категории данни;
- общо описание на техническите и организационни мерки за сигурност.

III. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА СИГУРНОСТ

Чл. 8. (1) Сдружение „СИП България" прилага следните технически и организационни мерки за осигуряване ниво на сигурност на личните данни, съобразено с естеството, обхвата, контекста и целите на обработването, както и с рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни, а именно:

1. Съхраняване на носителите на лични данни – хартиени и технически – в работни помещения – офиси – без достъп за външни лица и с ограничен достъп само на служители, действащи под ръководството на администратора, на които достъпът е необходим за изпълнение на служебните им задължения;
2. Осигуряване на физическа защита чрез видеонаблюдение, пожароизвестителни и пожарогасителни средства, заключващи системи – механични или електронни, вкл. чип карти, заключващи се шкафове и др.;

3. Осъществяване на достъп до личните данни на хартиен носител по възможност без изнасяне на оригиналните носители извън офисите, в които се обработват и съхраняват данните;
4. По отношение на данните, поддържани на технически носител в електронен вид:
   - ограничен достъп само за оторизирани служители на сдружението до твърдия диск, на който се съхраняват личните данни;
   - използване на лицензиран софтуер, на антивирусна програма и „защитна стена“;
   - използване на уникални потребителски акаунти и на текстово-цифрови пароли за достъп до компютрите и работните програми в локалната компютърна мрежа;
   - архивиране на личните данни в криптиран вид;
   - предоставяне на компютърната техника, на която се съхраняват лични данни, за ремонт без устройствата, на които се съхраняват данните;

5. Поддържане на резервно копие на електронната база с лични данни в ел. вид или на хартиен носител;

6. Унищожаване на документи с лични данни след отпадане на основанието за обработване и при изтичане на срока за съхранение, по начин, предотвратяващ всякаква възможност за бъдещо разчитане на данните: унищожаване на подлежащите на унищожаване докумети на хартиен носител чрез нарязване; унищожаване на лични данни, съхранявани на електронен носител, чрез трайно изтриване или физическо унищожаване на носителите;

7. Изискване към служителите на сдружението да спазват определените в раздел V задължения относно защитата на личните данни.

IV. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 9. Относно личните данни, които сдружение „СИП България “ обработва, всеки субект на данни има право да упражни правата си по чл. 15 – 22 на Регламент (ЕС) 2016/679 пред сдружението, а именно:

1. Право на достъп;
2. Право на коригиране;
3. Право на изтриване (право „да бъдеш забравен“);
4. Право на ограничаване на обработването;
5. Право на информиране по чл. 19 от ОРЗД;
6. Право на преносимост на данните;
7. Право на възражение;
8. Право да не бъде обект на автоматизирано вземане на решение.

(2) При подаване на искания за упражняване на горепосочените права субектът на данни следва да се идентифицира чрез предоставяне на документ за самоличност или по друг надлежен начин.

(3) В случай че упражняването на горните права, от лицето (участник, помощник или ръководител) по време на мероприятиятие проведено от сдружение “СИП България”, е несъвместимо с изпълнението на задълженията на администратора, на лицето не се позволява да присъства повече на конкретното мероприятие за което лицето (участник, помощник или ръководител) бива уведомено.

Чл. 10. Всеки субект, чиито лични данни се обработват от сдружението, има право да подаде жалба до компетентния надзорен орган – Комисия за защита на личните данни, ако счита, че обработването нарушава разпоредбите на ОРЗД.

Чл. 11. (1) Заявленията и исканията, постъпили от субекти на данни по повод техните права се завеждат във входящия регистър.

(2) Администраторът отговаря на всяко подадено искане във връзка с правата по чл. 9 в едномесечен срок от получаването му, за което не се дължи такса. При необходимост този срок може да бъде удължен с още два месеца предвид сложността и броя на исканията, за което субектът на данните следва да бъде уведомен до един месец от получаване на искането.

(3) При отказ да предприеме действия по дадено искане, администраторът информира субекта на данните за причината в срок от един месец от получаване на искането.

Чл. 12. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може:

- да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия, или
- да откаже да предприеме действия по искането.

V. ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ НА СДРУЖЕНИЕТО

Чл. 13. За целите на настоящите Вътрешни правила, под „служители на сдружението“ следва да се разбира не само тези, работещи по трудов договор, но и учредителите и членовете на органите на сдружението, доколкото техните правомощия съгласно Учредителния акт на сдружението или настоящите Вътрешни правила предполагат обработване на лични данни и/или носене на отговорност във връзка с обработването на лични данни.

Чл. 14. Служителите на сдружението, обработващи лични данни, са длъжни:

а) да се запознаят с нормативната уредба в областта на защитата на лични данни и с настоящите Вътрешни правила, за което подписват декларация;

б) да обработват личните данни в съответствие с принципите по чл. 3 от настоящите Вътрешни правила и да прилагат Вътрешните правила и всички останали относими към защитата на данните нормативни изисквания;

в) да спазват указанията на администратора относно обработването на личните данни, до които имат достъп;

г) да не споделят критична информация относно идентификатори, пароли за достъп и др. средства за защита с неоторизирани служители и лица;

д) да не прехвърлят на преносими лични носители на данни каквито и да е лични данни от базата с данни, които обработва администраторът;

е) да уведомяват незабавно прекия си ръководител в случай на установяване на неправомерен достъп или ползване на съответната информация, включваща лични данни, или на неправомерно проникване в помещение, в което тази информация се съхранява.

VI. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 15. За целите на настоящите Вътрешни правила се прилагат определенията в чл. 4 от Регламент (ЕС) 2016/679, в това число следните 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;
- „**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 комбиниране, ограничаване, изтриване или унищожаване;
- „**администратор**“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;
- „**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.

Чл. 16. Управителят на сдружение „СИП България “ следи за спазването на нормативните изисквания за защита на личните данни и настоящите Вътрешни правила и предприема нужните действия за съобразяване с тях на дейностите по обработване на лични данни от сдружението като администратор.

Чл. 17. За всички неуредени в настоящите Вътрешни правила въпроси са приложими разпоредбите на Общия регламент относно защитата на данните – (ЕС) 2016/679 – и законодателството на Република България относно защитата на личните данни.

Настоящите Вътрешни правила за защита на личните данни са приети с Решение на Управителния съвет на сдружението от 14.04.2021 г.