СДРУЖЕНИЕ „КИБЕЛА“ – ХАСКОВО

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Вътрешни правила за обработване и защита на личните данни

I. Общи положения

1. Настоящата политика урежда правилата, по които Сдружение „Кибела“ – Хасково („Сдружението“) събира, използва, съхранява, предоставя и защитава лични данни при осъществяване на дейността си.

2. Политиката се прилага при работа по проекти, обучения, събития, инициативи, доброволчество, членство, комуникация с участници, родители, партньори и дарители, както и при използване на сайта www.kibela.one, социалните мрежи, онлайн формуляри, електронна поща, облачни услуги, хартиени документи и други средства за обработване.

3. Политиката се прилага за председателя, членовете на органите на Сдружението, лицата, които изпълняват задачи за него и имат достъп до лични данни, както и в относимата част към външните доставчици, които обработват данни от името на Сдружението.

4. Политиката се прилага съгласно Регламент (ЕС) 2016/679 (GDPR), Закона за защита на личните данни и другите приложими нормативни актове.

5. Политиката е вътрешен организационен документ. Тя не заменя уведомленията към физическите лица, декларациите за съгласие, договорните клаузи с обработващи лични данни или политиката за бисквитките на сайта.

II. Администратор и контакт

6. Администратор на личните данни е Сдружение „Кибела“ – Хасково.

Адрес на управление: гр. Хасково, ул. „Добруджа“ № 44.

Адрес за кореспонденция: гр. Хасково, площад „Спартак“ № 14, партер.

Сайт: www.kibela.one. Имейл за въпроси и искания, свързани с личните данни: office@kibela.one.

7. Председателят отговаря вътрешно за прилагането на политиката, координира разглеждането на исканията, организира реакцията при инциденти и следи за изпълнението на мерките. Това не означава само по себе си, че е назначено длъжностно лице по защита на данните по смисъла на GDPR.

8. Ролята на Сдружението, партньорите и доставчиците (администратор, съвместен администратор или обработващ) се определя според действителните функции и договорености.

III. Основни принципи

9. Данните се обработват законосъобразно, добросъвестно и прозрачно; за конкретни и легитимни цели; в необходимия обем; с грижа за точността им; за срок, който не надвишава необходимото, освен когато закон или обвързващо изискване налага по-дълго съхранение; и при подходяща сигурност и поверителност.

10. Не се събират данни „за всеки случай“, не се използват за несъвместими цели и не се предоставя достъп на лица без служебна необходимост.

IV. Категории лица, данни и цели

11. В зависимост от конкретната дейност данни могат да се обработват за участници в събития, обучения и проекти, включително деца и младежи; родители и законни представители; доброволци и кандидати; членове и лица, участващи в управлението; партньори и техни представители; дарители; абонати за известия от сайта; лица, които се свързват със Сдружението.

12. Категориите данни могат да включват имена и контакти; възраст или дата на раждане, когато е необходима; участие и присъствие; данни в декларации и документи за отчетност; снимки и видеозаписи; обратна връзка; данни, изисквани от приложимите правила на програма или донор.

13. Само когато е необходимо и има приложимо правно основание, може да се обработват данни за здравословно състояние, увреждания или други обстоятелства, свързани с участието, както и информация за участници с по-малко възможности по конкретна програма. Медицински документи или други удостоверения не се изискват, когато не са необходими и не се изискват от приложимите правила.

14. Информацията за „по-малко възможности“ не се приема автоматично за специална категория лични данни. Преценява се какво разкрива конкретната информация, дали е необходима и на какво основание може да се обработва.

15. Целите включват организация и провеждане на дейности; комуникация с участници и родители; управление на доброволци и членство; безопасно участие и достъпност; изпълнение и отчитане на проекти; изпълнение на законови задължения; отношения с партньори и дарители; публичност на дейността; изпращане на заявени известия; разглеждане на запитвания и защита на правни права.

16. Не всички данни се събират във всеки проект. Всеки формуляр трябва да изисква само данните, необходими за конкретната дейност.

V. Правни основания

17. За всяка дейност се определя приложимото основание по чл. 6 GDPR: съгласие; изпълнение на договор или действия по искане на лицето преди договор; спазване на законово задължение; или легитимен интерес след преценка на интересите и правата на лицето.

18. За специални категории данни се изискват както основание по чл. 6, така и приложимо изключение по чл. 9, параграф 2 GDPR. Попълването на формуляр или участието в проект само по себе си не е достатъчно основание за обработване на здравни данни.

19. Съгласието, когато се използва, трябва да е свободно, конкретно, информирано и недвусмислено, да може да бъде доказано и оттеглено толкова лесно, колкото е дадено. Оттеглянето не засяга законосъобразността на обработването преди него.

20. Съгласието за заснемане или публикуване се разглежда отделно от другите основания за участие. Отказът от публикуване не следва автоматично да лишава лицето от участие, когато публикуването не е необходимо за дейността.

21. Преди стартиране на нова форма или дейност се определят целите, категориите данни, основанието, получателите и срокът за съхранение. Когато е приложимо, те се посочват в уведомлението за поверителност.

VI. Деца, снимки и видеозаписи

22. При дейности с деца се прилагат и вътрешните политики на Сдружението за закрила на детето и поведение при работа с деца.

23. Информацията към деца се предоставя ясно и разбираемо, съобразно възрастта. Когато законът изисква съгласие или действие от родител/законен представител, това се осигурява и документира.

24. При снимки и видеозаписи се определят целта и начинът на използване — вътрешна документация, отчетност по проект или публичност в сайта и социалните мрежи. Когато основанието е съгласие, то е конкретно за съответните цели и се получава от родител/законен представител, когато това е необходимо.

25. Декларациите могат да се изготвят за отделен проект, но трябва да посочват целите, каналите на публикуване и начина за оттегляне на съгласието. Разрешение за заснемане не означава автоматично разрешение за всякакво последващо публикуване.

26. При публикуване се избягват ненужни идентифициращи подробности за деца. Не се публикуват чувствителни данни или информация за здраве и уязвими обстоятелства заедно с изображение, освен ако това е необходимо, законосъобразно и надлежно обезпечено.

VII. Достъп и предоставяне на данни

27. Достъп получават само лицата, за които той е необходим за изпълнение на конкретни задачи. Членовете на органите, проектните екипи и доброволците нямат автоматично право на достъп до всички данни.

28. Счетоводната фирма може да получава данните, необходими за счетоводно обслужване и законови задължения. Отношенията трябва да бъдат уредени с подходящи договорни условия за поверителност, сигурност и обработване, когато фирмата действа като обработващ. Ролята ѝ се определя според действителните функции.

29. Други външни изпълнители по правило нямат достъп до лични данни, освен когато това е необходимо за конкретна задача и са осигурени подходящи правни и договорни гаранции.

30. Данни се предоставят на донори, финансиращи органи, партньори или контролни органи само когато това е необходимо за проект, отчетност или законово задължение и има приложимо основание. Предоставя се минимално необходимият обем; когато е възможно, се използват обобщени или псевдонимизирани данни.

31. Самото искане на донор не е достатъчно основание за предоставяне на всякакви данни. Преди предоставяне се проверяват целта, обемът, получателят и правното основание.

32. При използване на Google Forms, Google Drive, електронна поща, сайт, социални мрежи и други онлайн услуги се проверяват условията на услугата, настройките за споделяне, достъпът на доставчика и евентуалното предаване на данни извън Европейското икономическо пространство.

33. Предаване на данни извън Европейското икономическо пространство се допуска само при спазване на глава V GDPR.

VIII. Срокове за съхранение и унищожаване

34. Данните се съхраняват за срока, необходим за целта, освен когато закон, договор за финансиране, правила на програма или необходимост от защита на правни претенции налагат друг срок.

35. Документите по проекти се съхраняват според приложимото законодателство, договора и правилата на съответната програма или донор. Срокът обичайно е най-малко пет години, когато това се изисква от приложимите условия. Това не е автоматичен срок за всички лични данни.

36. Данните за абонамент за известия се съхраняват, докато абонаментът е активен или докато са необходими за управление и доказване на заявката, след което се изтриват или свеждат до минималния необходим обем.

37. Когато целта отпадне и няма друго основание, данните се изтриват, унищожават или анонимизират. Хартиените документи се унищожават така, че информацията да не може да бъде възстановена. Електронните копия се изтриват от местата под контрола на Сдружението, доколкото е технически възможно и законосъобразно.

38. Когато изтриването е ограничено от закон или задължителен срок, данните се ограничават до необходимото и не се използват за несъвместими цели.

IX. Мерки за сигурност

39. Мерките се съобразяват с характера на данните и риска и включват според приложимостта:

• достъп до документи и файлове само за лица с необходимост от тях;

• защита на устройства и акаунти с пароли и, когато е налична, многофакторна автентикация;

• ограничаване на споделянето в облачни услуги и проверка на получателите преди изпращане;

• избягване на публични линкове към файлове с лични данни и изпращане само на необходимите документи;

• съхраняване на хартиени документи на място с ограничен достъп;

• предпазливост при използване на лични устройства и имейли, когато това е необходимо за дейността;

• своевременно прекратяване на достъпа на лица, които вече не изпълняват съответната задача;

• резервни копия, когато са приложими и пропорционални;

• проверка на получателите и приложенията преди изпращане;

• поверителност и забрана за копиране, публикуване или използване извън определената цел.

40. Лицата с достъп са длъжни да пазят поверителност, да използват данните само за възложените задачи и незабавно да съобщават за съмнение за загуба, неправомерен достъп или разкриване.

X. Права на физическите лица

41. При условията на GDPR лицата могат да поискат достъп, коригиране, изтриване или ограничаване на обработването, да възразят срещу обработване, основано на легитимен интерес, и да упражнят право на преносимост, когато е приложимо. Съгласието може да бъде оттеглено, когато обработването се основава на него.

42. Искания се изпращат на office@kibela.one или на адреса за кореспонденция на Сдружението. Председателят преценява искането и при необходимост потвърждава самоличността пропорционално. Отговор се предоставя в сроковете по GDPR, обичайно до един месец. При законовите условия срокът може да бъде удължен, като лицето се уведомява.

43. Ако Сдружението не предприеме действия по искането, лицето се уведомява за причините и за възможността да подаде жалба до надзорния орган и да потърси съдебна защита.

44. Правото на изтриване може да бъде ограничено, когато данните трябва да се съхраняват по закон или по приложими задължения за отчетност. Преценява се всеки конкретен случай.

45. Лицето може да подаде жалба до Комисията за защита на личните данни (КЗЛД). Актуалните контакти се проверяват на официалния сайт на Комисията.

XI. Инциденти и нарушения на сигурността

46. При загуба на документ или устройство, изпращане до неправилен получател, неразрешен достъп, публично разкриване или друг инцидент всеки, който узнае за него, уведомява незабавно председателя.

47. Председателят организира ограничаване на инцидента, запазване на наличната информация, установяване на засегнатите данни и лица, оценка на риска и документиране на предприетите действия.

48. Когато нарушението може да доведе до риск за правата и свободите на лицата, Сдружението уведомява КЗЛД без неоправдано забавяне и, когато е възможно, не по-късно от 72 часа след узнаването. При вероятен висок риск засегнатите лица се уведомяват без неоправдано забавяне, освен ако е приложимо законово изключение.

49. Всяко нарушение се документира, включително когато след оценка не се налага уведомяване на КЗЛД. Записват се фактите, последиците, оценката на риска и коригиращите мерки.

XII. Регистър и отчетност

50. Сдружението поддържа подходяща информация за дейностите по обработване: цели, категории лица и данни, получатели, срокове за съхранение и общо описание на мерките за сигурност. Формата се съобразява с приложимите изисквания на GDPR.

51. Председателят организира преглед на формулярите, уведомленията, декларациите, достъпите и сроковете, така че практиките да съответстват на настоящата политика.

52. Когато дейността може да породи висок риск за правата и свободите на лицата, преди започването ѝ се преценява необходимостта от оценка на въздействието по чл. 35 GDPR.

XIII. Сайт, социални мрежи и известия

53. При използване на сайта www.kibela.one, Facebook, Instagram и други онлайн канали Сдружението обработва само данните, необходими за съответната комуникация или дейност. Платформите могат да обработват данни и за собствени цели съгласно своите условия и политики.

54. При абонамент за известия за нови публикации се обработват данните, необходими за управление на абонамента и изпращане на заявените съобщения. Трябва да има лесен начин за прекратяване на абонамента. Данните не се използват автоматично за други маркетингови цели.

55. Политиката за бисквитките е отделен документ. Конкретните бисквитки, аналитични инструменти, вградени услуги и настройки за съгласие се описват след проверка на окончателната конфигурация на сайта. Настоящата политика не твърди, че конкретен инструмент за статистика се използва или не се използва.

XIV. Преглед и заключителни разпоредби

56. Политиката се преглежда при промяна в законодателството, дейността, използваните технологии, категориите данни, изискванията на програмите или организацията на достъпа.

57. Политиката се прилага от датата на приемането ѝ с решение на компетентния орган на Сдружението.

Приета с решение на:	.....
Дата:	.....
Подпис:	.....