ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Ние, от **„Кемплайт“ ЕООД**, ЕИК: 201875626, седалище и адрес на управление: гр. Плевен, 5800, ул."Десети Декември" № 150, ет. 2 и от **Кооперация "Кемплайт Кооп"**, ЕИК: 207352038, седалище и адрес на управление: гр. Плевен, 5800, ул."Десети Декември" № 150, ет. 2, данни за контакт: team@camplight.net (наричани по-долу с общото наименование “ Група от свързани юридически лица Кемплайт ” или накратко „ **Групата на Кемплайт или Ние** “) разбираме важността на конфиденциалността и защитата на Вашите лични данни.

„Кемплайт“ ЕООД и Кооперация "Кемплайт Кооп" са свързани юридически лица, които развиват еднородна и свързана помежду си търговска дейност, поради което в определени случаи може да наложи да обработват лични данни на едни и същи лица за едни и същи цели. Именно заради това двете организации приемат да прилагат настоящата обща политика за защита на личните данни. Настоящата политика е приложима в случаите, в които двете организации съвместно обработват лични данни на едни и същи лица за едни и същи цели, както и в случаите, в които всяка от организациите обработва самостоятелно лични данни.

I. Декларация относно политиката за защита на личните данни и дефиниции

1. Декларация

Считано от 25 май 2018 г. влезе в сила 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 („Общият регламент на ЕС относно защитата на данните“ или „ОРЗД“), с който се променя съществуващият правен режим по защита на данните и свободното движение на същите.

Като организации, установени на територията на Република България и обработващи данни на граждани на ЕС, за Групата на Кемплайт възникват редица задължения, свързани с обработването на личните данни и тяхното свободно движение в съответствие ОРЗД, актовете по неговото прилагане и действащото национално законодателство.

С оглед на това, Групата ще прилага настоящата Политика за защита на личните данни („**Политиката**“), която ще бъде минимален стандарт при обработването на данни на физическите лица и осигуряването на тяхното свободно движение.

Настоящата политика има за цел да Ви запознае с начина, по който събираме, обработваме и съхраняваме Вашите лични данни, когато Вие взаимодействате с нас във връзка с предлаганите от нас стоки / услуги.

Контрагентите и всички трети страни, които работят с или за Групата и които имат или могат да имат достъп до лични данни, трябва да са прочели, разбрали и да са се задължили да спазват настоящата политика. Под контрагенти следва да се разбира всички лица, които по един или друг начин са или могат да бъдат в делови отношения с Групата, като например, но без да се ограничава до – клиенти, доставчици, партньори,

изпълнители, подизпълнители, възложители и други.

Тази Политика се прилага за всички контрагенти, както и за всички служители / работници и лица, които имат сключени граждански договори с Групата (наричани с общото наименование „Персонал“), както и за член - кооператори и за други трети лица, на които Групата я е предоставила във връзка с обработка на лични данни на субекти на данни.

Групата на Кемплайт си запазва правото периодично да актуализира и изменя настоящата Политика за поверителност с цел отразяване актуалния начин, по който се обработват Вашите лични данни.

Настоящата Политика за защита на личните данни е публикувана на уебсайта на Групата и е общодостъпна за всички лица, с които Групата влиза в правоотношения.

2. Дефиниции

Лични данни – всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано; физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано пряко или непряко, по - специално чрез идентификатор като име, ЕГН, постоянен или настоящ адрес, IP адрес или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

Администратор – съгласно настоящата политика, администратор на лични данни е всяко дружество, което само или съвместно с други определя целите и средствата за обработването на лични данни.

Субект на данни – всяко живо същество, което е обект на лични данни, съхранявани от Групата. Такива са клиентите, съконтрагентите на Групата, когато то обработва техни лични данни.

Обработване – 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.

Нарушение на сигурността на лични данни – 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. Администраторът има задължението да докладва на надзорния орган за нарушения на сигурността на личните данни и тогава, когато има вероятност нарушението да има неблагоприятни последици върху личните данни или неприкосновеността на личния живот на субекта на данните.

Съгласие на субекта на данните - означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субектите на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му личните му данни да бъдат обработени.

Трета страна – физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните и администратора.

II. Задължения и роли по Регламента

1. Групата може да обработва лични данни както в качеството на администратор на лични данни (като само определя целите и средствата на обработването), така и като обработващ лични данни, действащ от името на трети лица – администратори на лични данни.

2. Ръководството на Групата на Кемплайт е отговорно за разработване и насърчаване на добри практики в областта на обработване на информация в Групата.

3. Спазването на законодателството за защита на данните е отговорност на всички лица от Групата на Кемплайт, които обработват лични данни.

III. Принципи за защита на данните

Обработването на лични данни трябва да се извършва в съответствие с принципите за защита на данните, посочени в член 5 от Регламента. Политиките и процедурите на Групата на Кемплайт имат за цел да гарантират спазването на тези принципи.

1. **Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно**

Законосъобразно – Групата следва да идентифицира законова основа, преди да обработва съответните лични данни. Такава законова основа често се посочва като "основание за обработване", например „съгласие“.

Добросъвестно - за да може обработването да бъде добросъвестно администраторът на данни трябва да предостави определена информация на субектите на данни, доколкото това е практически възможно. Това важи, независимо дали личните данни са получени директно от субектите на данни или от други източници.

Регламентът увеличава изискванията за това каква информация трябва да бъде на разположение на субектите на данни, която е обхваната от изискването за "прозрачност".

Прозрачно – Регламентът включва правила относно предоставяне на поверителна информация на субектите на данни в членове 12, 13 и 14 от Регламента. Те са подробни и конкретни, поставяйки акцента върху това, че известията за поверителност са разбираеми и достъпни. Информацията трябва да бъде съобщена на субекта на данните в разбираема форма, като се използва ясен и разбираем език.

Специфичната информация, която трябва да бъде предоставена на субекта на данните, трябва да включва като минимум:

i. данни, които идентифицират администратора и данните за контакт на администратора и, ако има такъв, на представителя на администратора;

ii. контактите на ДЛЗД/отговорника по защита на личните данни, ако администраторът прецени, че попада в обхвата на задължителното назначаване на такова лице;

iii. целите на обработването, за което личните данни са предназначени, както и правното основание за обработването; периода, за който ще се съхраняват личните данни;

iv. съществуването на следните права - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както право на възражение срещу условията (или липсата на такива) във връзка с упражняването на тези права;

v. категориите лични данни;

vi. получателите или категориите получатели на лични данни, където това е приложимо;

vii. където е приложимо, дали администраторът възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на данните;

viii. правото на жалба;

ix. източника на личните данни и, ако е приложимо, дали данните са от публично достъпен източник; съществуването на автоматизирано вземане на решения, включително профилиране;

x. всякаква допълнителна информация, необходима да се гарантира добросъвестно обработване.

2. Лични данни могат да се събират само за конкретни, изрично указани и законни цели

Данните, получени за конкретни цели, не трябва да се използват за цел, която се различава от тези, за които предварително са събрани данните (чл. 30 Регламента).

3. Личните данни трябва да бъдат адекватни, релевантни, ограничени до това, което е необходимо за обработването им със съответната цел.

4. Личните данни трябва да бъдат точни и актуализирани във всеки един момент, и да са положени необходими усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.

i. Данните, които се съхраняват от администратора на данни, трябва да бъдат прегледани и актуализирани при необходимост. Не трябва да се съхраняват данни, в случаите, когато има вероятност да не са точни.

ii. Ръководството гарантира, че при наемането на персонал, целият персонал ще

бъде обучен в значението на събирането на точни данни и поддържането им.

iii. Също така, задължение на субекта на данните, респективно администраторът - в случаите, в които Групата действа като обработващ лични данни, е да декларира, че данните, които предава за съхраняване от Групата на Кемплайт са точни и актуални. Попълването на формуляр от субекта на данни/администратора, предназначени за Групата, ще включва изявление, че съдържащите се в него данни са точни към датата на подаване.

iv. От служителите / работниците и контрагентите трябва да се изисква да уведомяват Групата на Кемплайт за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Отговорността на Групата на Кемплайт е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия.

v. Ръководството на Групата декларира, че са налице подходящи процедури и политики за поддържане на точност и актуалност на личните данни, като се отчита обемът на събраните данни, скоростта, с която може да се промени и други относими фактори.

vi. Най-малко на годишна база Ръководството на Групата ще преглежда сроковете на съхранение на всички лични данни, обработвани от Групата на Кемплайт, като се позовава на инвентаризацията на данните и ще идентифицира всички данни, които вече не се изискват в контекста на регистрираната цел. Тези данни ще бъдат надеждно унищожени в съответствие с процедурите и правилата на администратора.

vii. Ръководството на Групата привежда съответните лични данни в съответствие с постъпили надлежни искания за корекция на данни в рамките на един месец от датата на постъпване на искането съобразно вътрешните правила за управление на исканията от субектите. Този срок може да бъде удължен с още два месеца за сложни заявки. Ако Групата на Кемплайт реши да не се съобрази с искането, Групата ще отговори на субекта на данните, за да обясни мотивите си и да го информира за правото му да подаде жалба пред надзорния орган и да потърси правна защита.

viii. Ръководството на Групата взема подходящи мерки, в случаите когато организациите на трети лица имат неточни или остарели лични данни, информира ги, че информацията е неточна или остаряла и не се използва за вземане на решения относно лицата, информира съответните лица; и препраща всяка корекция на лични данни към третите лица, където това е необходимо.

5. Личните данни трябва да се съхраняват в такава форма, че субектът на данните може да бъде идентифициран само толкова дълго, колкото е необходимо за обработването.

i. Когато личните данни се запазват след датата на обработването, те ще бъдат съхранявани по подходящ начин (минимизирани, криптирани, псевдонимизирани), за да се защити самоличността на субекта на данните в случай на нарушение на данните.

ii. Лични данни ще бъдат пазени в съответствие с вътрешните правила за съхранение и унищожаване на данните, описани в Раздел IX от Политиката и след като е преминал срокът им на съхранение те трябва да бъдат надеждно унищожени по указания в тази процедура ред.

iii. Ръководството одобрява всяко запазване на данни, което надхвърля срока на съхранение, съгласно настоящата Политика и трябва да гарантира, че обосновката е ясно определена и е в съответствие с изискванията на законодателството за защита на данните. Това одобрение трябва да бъде писмено.

6. Личните данни трябва да бъдат обработвани по начин, който гарантира подходяща сигурност (чл. 24, чл. 32 от Регламента)

Ръководството на Групата ще извърши оценка на въздействието (оценка на риска), когато това е приложимо и необходимо, като вземе предвид всички обстоятелства, свързани с операциите по управление или обработване на данни от Групата на Кемплайт.

При определянето на това доколко уместно е обработването, Ръководството на Групата разглежда степента на евентуална вреда или загуба, която може да бъде причинена на физически лица, ако възникне нарушение на сигурността, както и всяка вероятна вреда за репутацията на администратора, включително евентуална загуба на доверие.

При оценяването на подходящи технически мерки, Ръководството на Групата ще разгледа следните възможности:

i. Защита с парола;

ii. Автоматично заключване на бездействащи работни станции в мрежата;

iii. Премахване на права на достъп за USB и други преносими носители с памет;

iv. Антивирусен софтуер и защитни стени;

v. Правата за достъп основани на роли, включително тези на назначен временно персонал;

vi. Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;

vii. Сигурност на локални и широкообхватни мрежи;

viii. Технологии за подобряване на поверителността, като например псевдонимизиране и анонимизиране.

При оценяването на подходящите организационни мерки Ръководството на Групата ще вземе предвид следното:

i. Нивата на подходящо обучение в Групата на Кемплайт ;

ii. Мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);

iii. Включването на защитата на данните в трудовите договори;

iv. Идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;

v. Редовна проверка на персонала за спазване на съответните стандарти за сигурност;

vi. Контрол на физическия достъп до електронни и хартиено базирани записи;

vii. Приемането на политика на „чисто работно място“;

viii. Съхраняване на хартия на базата данни в заключващи се стенни шкафове;

ix. Ограничаване на използването на портативни електронни устройства за работни цели извън работното място;

x. Ограничаване на използването от служителите на лични устройства на работното място;

xi. Приемане на ясни правила за създаване и ползване на пароли;

xii. Редовно създаване на резервни копия на личните данни и физическо съхраняване на носителите с копия извън офиса;

xiii. Налагане на договорни задължения на организации контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни извън ЕС.

Тези контроли са избрани въз основа на идентифицираните рискове за лични данни, както и потенциала за нанасяне на вреди на лицата, чиито данни се обработват.

7. Спазване на принципа на отчетност

Групата на Кемплайт ще доказва спазването на принципите за защита на данните чрез прилагане на политики по защита на данните, като се присъединява към кодекси, политики и договори, внедрява подходящи технически и организационни мерки, както и чрез защита на данните по подразбиране, оценка на въздействието върху защитата на личните данни, процедура за уведомяване за нарушаване на лични данни и т.н.

IV. Лични данни, обработвани от Групата на Кемплайт

Групата на Кемплайт обработва лични данни на субекта на данните, когато е дал съгласие за обработване на личните му данни, за една или повече конкретни цели, или когато следва да обработва данните им по закон или правно защитими интереси на Групата налагат това, както следва (**Регистри**):

1. **Обработване на лични данни на персонала на Групата:**

Процес (описание)	Обработвани лични данни	Трети лица – получатели на личните данни	Срок на съхранение на лични данни	Начин на обработване

1. Подбор на служители/работници	Данни за контакт (имена, телефон, електронна поща), данни за образование и професионален стаж и друга информация, предоставена от кандидата. Всякакви данни, предоставени по време на процеса на подбор, включително, но не само, резултати от тестове, код, задачи и видео/аудио записи.	Бюро по труда, Доставчици на услуги по подбор/наем на персонал, Клиенти	5 години от получаването на данните	чрез неавтоматични средства – на хартиен носител чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни.
2. Сключване на трудови договори	Имена, ЕГН, постоянен адрес, IBAN, телефон, електронна поща и необходимите по закон данни (съдимост, медицинско състояние)	Доставчици на услуги по външно счетоводство, НАП, НОИ, Трудова медицина	До по-ранното от двете 1) прекратяване дейността на Групата и предаване на ведомостите в НОИ или 2) изтичане на 50 години.	чрез неавтоматични средства – на хартиен носител чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни.
3. Сключване на граждански договори	Имена, ЕГН, постоянен адрес, IBAN, телефон, електронна поща	Доставчици на услуги по външно счетоводство, НАП, НОИ	Граждански договори и протоколи за предадена работа – до 5 години, считано от 1 януари на годината, следваща годината, в която са издадени (за целите на данъчния и осигурителен контрол)	чрез неавтоматични средства – на хартиен носител чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни.
4. Администриране на трудовит	Имена, IBAN, трудов стаж, данни за	Доставчици на услуги по външно	До по-ранното от двете	чрез неавтоматични средства – на хартиен носител

е правоотношения – изплащане на заплати	доходи от други правоотношения	счетоводство, НАП, НОИ	1) прекратяване дейността на Групата и предаване на ведомостите в НОИ или 2) изтичане на 50 години.	чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни.
5. Администриране на трудовите правоотношения – болнични и трудова медицина	Имена, информация за здравословно състояние от болнични листове при ползване на отпуск поради общо заболяване/майчинство	Служба по трудова медицина, НОИ, НАП	Болнични – 3 години, считано от 1 януари на годината, следващата годината на издаване на болничния лист	чрез неавтоматични средства – на хартиен носител чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни.
6. Администриране на трудовите правоотношения – водене на трудово досие	Документи във връзка с трудовото правоотношение – заповеди за назначаване, за прекратяване на трудов договор, за ползване на отпуск и пр. Копие от диплома – само когато в щатното разписание е записано, че длъжността изисква определено образование или степен на квалификация Свидетелство за съдимост – само ако в закон се изисква удостоверяване на съдебно минало за заемане на длъжността	Доставчици на услуги по външно счетоводство, НАП, НОИ, Агенция по заетостта и други структури към МТСП, банки и платежни институции.	Трудови договори и допълнителни споразумения заповеди за назначаване, заповеди за преназначаване, заповеди за ползван неплатен отпуск над 30 работни дни, заповеди за прекратяване на трудови правоотношения - до прекратяване дейността на Групата и предаване в НОИ. Непотърсени трудови книжки, дневник за издадени	чрез неавтоматични средства – на хартиен носител чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни.

	Медицинско удостоверение –само ако в закон се изисква такова Снимка (на CV и/ли диплома)		трудови книжки, удостоверения – 50 години. Всички останали документи и лични данни от досието (копие от диплома, снимка, медицинско при постъпване, телефонен номер, заповеди различни от посочените по-горе и др.) – до по-късното от: 1)прекратяването на трудовото правоотношение или 2)уреждане на отношенията с бившия служител.	
7. Представяне на екипа, маркетинг и брандинг активности	Имена, професионален опит, роля по проекти, цитати/отговори на въпроси и снимки	Могат да бъдат достъпни чрез интернет, публични канали и социалните мрежи, както и страниците на Групата.	До оттегляне на съгласието от страна на лицето	чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни
8. Събития	Имена, снимки, видеа от събитията	Могат да бъдат достъпни чрез интернет и социалните мрежи, както и	До оттегляне на съгласието от страна на лицето	чрез автоматични средства – компютър, на хард диск, облачно

		страниците на Групата		съхранение на данни

При възникване на делови взаимоотношения от трудовоправен или гражданскоправен характер на лицата се връчват подробни уведомления във връзка с личните им данни и/или се сключват анекси към съответните договори във връзка с личните им данни.

2. Обработване на лични данни на контрагенти на Групата:

Процес (описание)	**Обработвани лични данни**	**Трети лица – получатели на личните данни**	**Срок на съхранение на лични данни**	**Начин на обработване**
1.Сключване на договори с клиенти / възложители, както и изпълнение по такива договори	За юридически лица: ЕИК, име, МОЛ, данни за контакт, ЕГН на МОЛ, адрес, IBAN; данни от Годишен финансов отчет; ГДО; Годишен доклад за дейността, За физически лица: Имена, данни за контакт, ЕГН, адрес, IBAN. При необходимост с оглед изпълнение на предмета на договора: информация за фактури, договори, персонал, членове (информацията може да варира и да съдържа три имена, електронна поща, телефон, адрес, образование, професия и ЕГН) Други данни свързани с изпълнение на договора: бази данни за трети	външен счетоводител; системи за платежни операции; банки; при необходимост – компетентни държавни органи.	10 години, считано от 1 януари на годината, следваща годината, през която данните са предоставени.	чрез неавтоматични средства – на хартиен носител чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни.

	лица, отчети, регистри и други.			
2. Сключване на договори за комисионни с партньори, както и изпълнение по такива договори	За юридически лица: ЕИК, име, МОЛ, данни за контакт, ЕГН на МОЛ, адрес, IBAN; данни от Годишен финансов отчет; ГДО; Годишен доклад за дейността, За физически лица: Имена, данни за контакт, ЕГН, адрес, IBAN. При необходимост с оглед изпълнение на предмета на договора: информация за фактури, договори, персонал, членове (информацията може да варира и да съдържа три имена, електронна поща, телефон, адрес, образование, професия и ЕГН) Други данни свързани с изпълнение на договора: бази данни за трети лица, отчети, регистри и други.	външен счетоводител; системи за платежни операции; банки; при необходимост – компетентни държавни органи.	10 години, считано от 1 януари на годината, следваща годината, през която данните са предоставени.	чрез неавтоматични средства – на хартиен носител чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни.
3.Сключване на договор с изпълнители / подизпълнители, както и изпълнение	За юридически лица: ЕИК, име, МОЛ, данни за контакт, ЕГН на МОЛ, адрес, IBAN; данни от Годишен финансов отчет; ГДО; Годишен доклад за дейността,	външен счетоводител; системи за платежни операции; банки; при необходимост – компетентни държавни органи.	10 години, считано от 1 януари на годината, следваща годината, през която данните са предоставени.	чрез неавтоматични средства – на хартиен носител чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни.

по такива договори	За физически лица: Имена, данни за контакт, ЕГН, адрес, IBAN. При необходимост с оглед изпълнение на предмета на договора: информация за фактури, договори, персонал, членове (информацията може да варира и да съдържа три имена, електронна поща, телефон, адрес, образование, професия и ЕГН) Други данни свързани с изпълнение на договора: бази данни за трети лица, отчети, регистри и други.			
4. Отговаряне на запитвания, въпроси и коментари чрез Контактна форма на уебсайт, социални мрежи, електронна поща, телефонен разговор	Обемът на споделяне на лични данни е по преценка на потребителя/клиента - Имена, телефонен номер, електронна поща и други	Не се предоставят на трети лица освен ако Групата не е задължена по закон	До 6 месеца	чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни
5. Представяне на екипа, маркетинг и брандинг активности	Имена, професионален опит, роля по проекти, цитати/отговори на въпроси и снимки	Могат да бъдат достъпни чрез интернет, публични канали и социалните мрежи, както и	До оттегляне на съгласието от страна на лицето	чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни.

		страниците на Групата		
6. Събития	Имена, снимки, видео от събитията	Могат да бъдат достъпни чрез интернет и социалните мрежи, както и страниците на Групата	До оттегляне на съгласието от страна на лицето	чрез автоматични средства – компютър, на хард диск, облачно съхранение на данни

3. Обработване на лични данни член – кооператори:

Процес (описание)	**Обработвани лични данни**	**Трети лица – получатели на личните данни**	**Срок на съхранение на лични данни**	**Начин на обработване**
1. Приемане на нов член - попълване на онлайн формуляр / молба и одобрение от УС	Данни за контакт (имена, телефон, електронна поща), данни за образование и професионален стаж и друга информация, предоставена от кандидата.	Не се предоставят на трети лица освен ако кооперацията е задължена по закон.	До прекратяване на членството	чрез автоматични средства – компютър, на хард диск, в cloud сървър
2. Провеждане на Общи събрания и събрания на управителните органи на Кооперацията – изготвяне на покани и протоколи.	Имена, подпис, ЕГН при упълномощаване, имейли, направени изказвания/предложения	ТРРЮЛНЦ (при промяна на обстоятелствата и обявяване на актове, гласувани на ОС)	Съхраняване на покани и протоколи от ОС и УС - до прекратяване на Кооперацията	чрез неавтоматични средства – на хартиен носител чрез автоматични средства – компютър, на хард диск, в cloud сървър
3. Събития	Имена, снимки, видео от събитията	Могат да бъдат достъпни чрез интернет и социалните мрежи, както и страниците на Кооперацията	До прекратяване на Кооперацията	чрез автоматични средства – компютър, на хард диск, в cloud сървър

Процес (описание)	Обработвани лични данни	Трети лица – получатели на личните данни	Срок на съхранение на лични данни	Начин на обработване
4. Избор на членове на УС и Контролен съвет	Имена, ЕГН, контактна информация, снимки	ТРРЮЛНЦ, НАП (само л.д. на председателя), банки (само л.д. на председателя)	Протоколи - до прекратяване на Кооперацията, Контактна информация и снимки – до прекратяване на мандата в УС/Контролния съвет или на членството	чрез неавтоматични средства – на хартиен носител чрез автоматични средства – компютър, на хард диск, в cloud сървър
5. Поддържане на база данни с членовете	Имена, имейл, телефон, рождена дата, рожден град и настоящ град, пол, снимки, гимназия, университет, специалност, други обучения, езици, настоящ работодател, настояща позиция в работата, предишни работи, професионални интереси, лични интереси, дати на плащане и/или получаване на вноски	Не се предоставят на трети лица освен ако Кооперацията е задължено по закон.	До прекратяване на членството	чрез автоматични средства – компютър, на хард диск, в cloud сървър
6. Представяне на екипа, маркетинг и брандинг активности	Имена, професионален опит, роля по проекти, цитати/отговори на въпроси и снимки	Могат да бъдат достъпни чрез интернет, публични канали и социалните мрежи, както и страниците на Кооперацията	До оттегляне на съгласието от страна на лицето	чрез автоматични средства – компютър, на хард диск, в cloud сървър

3. Основания и цели на обработката на лични данни

Обработването на Вашите лични данни за тези цели в повечето случаи е необходимо за сключването и изпълнението на договор между Вас и Групата (вкл. договори, сключени от разстояние, както и за приложими ненаименувани договори, договор за поръчка, договор за изработка, договор за доставка, договор за посредничество, договор за покупко-продажба и други). Освен това, за изпълнението на тези цели се изисква обработване съгласно приложимите законови разпоредби на територията на Република България, включително данъчното и счетоводното законодателство.

- **Маркетинг**

Нашето желание е Вие винаги да сте осведомен/а за всички предстоящи събития, както и за най-добрите предложения относно услугите, организирани или предлагани от страна на Групата. В тази връзка, можем да Ви изпращаме всякакви видове съобщения, посредством канали за електронни съобщения, които съдържат обща и тематична информация. Ние винаги гарантираме, че това обработване се извършва при строго спазване на Вашите права и свободи, и че решенията, взети във връзка с тях, не пораждат никакви правни последици за Вас.

- **Защита на нашите законни интереси**

Възможно е да има случаи, в които има необходимост ние да използваме или да предаваме информация, за да защитим правата на Групата. Те могат да включват:

i. мерки за защита на уеб сайта на Групата срещу кибератаки;
ii. мерки за своевременно предотвратяване и откриване на опити за измама, включително предаване на информация на компетентни публични органи;
iii. мерки за управление на различни други рискове.

Главната причина за тези видове обработване са законните интереси на Групата, свързани със защитата на дейността ѝ, като ние гарантираме, че всички предприемани от нас мерки се съобразяват едновременно както с нашите интереси, така и с Вашите основни права и свободи.

Понастоящем ние съхраняваме и обработваме личните Ви данни на територията на Република България. Въпреки това, съществува възможност някои от Вашите данни да бъдат предадени на субекти, намиращи се в Европейския съюз или извън него.

V. Права на субектите на данни

1. Всеки от субектите на данни има следните права по отношение на обработването на данни, както и на данните, които се записват за него:

i. Да отправя искания за потвърждаване дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните, както и информация кои са получателите на тези данни;
ii. Да поиска копие от своите лични данни от администратора;
iii. Да иска от администратора коригиране на лични данни когато те са неточни,

както и когато не са вече актуални;

iv. Да изиска от администратора изтриване на лични данни (право „да бъдеш забравен");

v. Да иска от администратора ограничаване на обработването на лични данни, като в този случай данните ще бъдат само съхранявани, но не и обработвани по друг начин;

vi. Да направи възражение срещу обработване на негови лични данни;

vii. Да направи възражение срещу обработване на лични данни, отнасящи се до него за целите на директния маркетинг.

viii. Да се обърне с жалба до надзорен орган ако смята, че някоя от разпоредбите на Регламента е нарушена;

ix. Да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;

x. Да оттегли съгласието си за обработване на личните данни по всяко време с отделно искане, отправено до администратора;

xi. Да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;

xii. Да се противопостави на автоматизирано профилиране, което се случва без негово съгласие;

2. Групата на Кемплайт осигурява условия, които да гарантират упражняването на тези права от субекта на данни:

i. Субектите на данни могат да направят искания за достъп до данни;

ii. Субектите на данни имат право да подават жалби до Групата на Кемплайт, свързани с обработването на личните им данни.

VI. Съгласие

1. Под „съгласие“ Групата на Кемплайт ще разбира 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. Субектът на данните може да оттегли своето съгласие по всяко време.

2. Групата на Кемплайт разбира под „съгласие“ само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху него да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

3. Съгласието не може да бъде изведено от липсата на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. Администраторът трябва да може да докаже, че е получено съгласие за дейностите по обработване.

4. В повечето случаи съгласието за обработване на лични данни и специални категории данни се получава рутинно от Групата на Кемплайт, като се използват стандартни документи за съгласие, напр. когато нов клиент подписва договор или по време на набиране на нов персонал и т.н.

VII. Сигурност на данните

1. Всички служители / работници са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които Групата на Кемплайт държи, както и, че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако Групата на Кемплайт не е дал такива права на тази трета страна, като са сключили договор/клауза за поверителност.

2. Всички лични данни трябва да бъдат достъпни само за тези, които се нуждаят от тях, а достъпът може да бъде предоставен само в съответствие с изградените правила за контрол на достъпа. Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:

i. в самостоятелна стая с контролиран достъп; и/или в заключен шкаф или в картотека; и/или

ii. ако е компютъризирана, защитена с парола в съответствие с вътрешните изисквания посочени в организационните и технически мерки за контролиране на достъпа до информация (например правила за контрол на достъпа); и / или

iii. съхранявани на преносими компютърни носители, които са защитени в съответствие с организационните и технически мерки за контролиране на достъпа до информация.

3. Да се създаде организация, която да гарантира, че компютърните екрани и терминалите не могат да бъдат гледани от друг, освен от оторизираните служители / работници на Групата на Кемплайт. От всички служители / работници се изисква да бъдат обучени и да приемат съответните договорни клаузи/декларация/уведомление относно събирането, обработването и съхранението на лични данни.

4. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат изваждани от определените офисни помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за текущата работа, те трябва да бъдат унищожени в съответствие със създадени за това вътрешни правила в Раздел IX от настоящата политика.

VIII. Разкриване на данни

1. Групата на Кемплайт осигурява условия, при които личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички служители / работници трябва да бъдат предпазливи, когато им поискат да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността извършвана от организацията.

На служителите се извършва специално обучение и периодични инструктажи с цел да

се избегне рискът от такова нарушение.

2. Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат специално разрешени от Управителя на Групата.

Получатели на Вашите лични данни

Групата се ангажира да прилага най-високите стандарти на етични и юридически практики във всички свои дейности, включително защитата на личните данни на всички потребители на уебсайта. С изключение на случаите, посочени по-долу, няма да разкриваме, нито ще позволим на никое лице извън Групата да има достъп до личната ви информация или да я използва.

В зависимост от спецификата на всеки конкретен случай, можем да предаваме или да предоставяме достъп до някои от Вашите лични данни на следните категории получатели:

i. доставчици на платежни/банкови услуги;
ii. доставчици на куриерски услуги;
iii. външни счетоводни дружества;
iv. подизпълнители на услуги предлагани от Групата;
v. и на други категории лица във връзка със сключването и изпълнението на договорите (вкл. устни и неформални такива) между Вас и Групата.

Гарантираме, че достъпът до Вашите данни от частноправни субекти - трети страни се осъществява съгласно законовите разпоредби в областта на защитата на личните данни и конфиденциалността на информацията въз основа на договори, сключени с тях, и са задължени да защитават поверителността и сигурността на Вашата лична информация и данни. Те не са упълномощени да използват, разкриват или променят тази информация по никакъв начин, освен за целите на извършване на услугите, възложени от Групата.

Ако сме задължени по закон или ако това е необходимо за защита на законните ни интереси, имаме право да разкриваме определени лични данни и на публични органи.

IX. Съхраняване и унищожаване на данните

1. Групата на Кемплайт не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходимо, по отношение на целите, за които са били събрани данните.

2. Групата на Кемплайт може да съхранява данни за по-дълги периоди единствено ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и организационни мерки за гарантиране на правата и свободите на субекта на данните.

3. Периодът на съхранение за всяка категория на лични данни се определят в

настоящата Политика.

4. Личните данни се унищожават по сигурен начин, съобразно изискванията на чл. 5, пар. 1 б. е) от Регламента, като се прилагат подходящи технически или организационни мерки срещу случайна загуба, унищожаване или повреждане („цялостност и поверителност“);

5. След отпадане на необходимостта от обработване на съответната категория лични данни Групата на Кемплайт предприема стъпки за унищожаването на данните съгласно настоящите правила.

6. Всички лични данни, съхранявани на хартиен носител, се унищожават в офиса на Групата на Кемплайт посредством устройство за нарязване (шредер). В случай че такова устройство не е налично към момента на възникване на задължението за унищожаване, данните се унищожават чрез нарязване с ножица, като лицето, отговорно за унищожаването следва да се увери, че след нарязването данните не могат да бъдат възстановени. Когато на съответния хартиен носител се съдържат и други данни, които все още се обработват от Групата на определено законово основание, ненужните данни се заличават от хартиения носител със средства, непозволяващи тяхното възстановяване;

7. Данните, които се съхраняват под формата на електронни съобщения (електронна поща) се унищожават чрез постоянно изтриване.

8. Личните данни, съхранявани в електронна форма се изтриват по начин, който не позволява тяхното възстановяване.

9. След извършване на унищожаване на лични данни лицето, осъществило унищожаването, издава нарочен протокол, който следва да съдържа информация относно категорията лични данни, формата, под която данните са били съхранявани, основанието за предприетото унищожаване, метода на сигурно унищожаване, дата на унищожаване, имена и подпис на лицето, осъществило унищожаването.

X. Регистър на обработванията на данни (инвентаризация на данните)

1. Групата на Кемплайт използва процес на инвентаризация на данните като част от своя подход за справяне с рисковете и възможностите в процеса на спазване на политиката за съответствие с Регламента в случаите, в които това е приложимо. При инвентаризацията на данните в Групата на Кемплайт и в работния поток от данни се установяват:

- бизнес процесите, които използват лични данни;
- източниците на лични данни;
- броя на субектите на данни;
- описание на категориите лични данни и елементите на във всяка категория;
- дейностите по обработване;
- целите на обработването, за което личните данни са предназначени;
- правното основание за обработването;

- получателите или категориите получатели на личните данни;
- основните системи и места за съхранение;
- всички лични данни, които подлежат на трансфери извън ЕС;
- сроковете за съхранение и заличаване.

2. Групата на Кемплайт е наясно с рисковете, свързани с обработването на определени видове лични данни.

3. Групата на Кемплайт оценява нивото на риска за лицата, свързани с обработването на личните им данни. Извършват се оценки на въздействието върху защитата на данните във връзка с обработването на лични данни от Групата и във връзка с обработването, предприето от други организации от името на Групата.

4. Групата на Кемплайт управлява всички рискове, идентифицирани от оценката на въздействието, с цел да се намали вероятността от несъответствие с тези правила.

Когато вид обработване може да доведе до висок риск за правата и свободите на физическите лица, по-специално с използване на нови технологии и като се вземат предвид естеството, обхвата, контекста и целите на обработването, преди да пристъпи към обработване Групата на Кемплайт следва да извърши оценка на въздействието на предвидените операции по обработване върху защитата на личните данни. Една обща оценка на въздействието може да разглежда набор от подобни операции по обработване, които представляват подобни високи рискове.

XI. Жалби

Разполагате със законовото право да депозирате жалба пред местния надзорен орган относно обработването на Вашите лични данни. На територията на Република България данните за контакт с надзорния орган за защита на данните са следните:

Комисия за защита на лични данни
Адрес: гр. София, бул. „Цветан Лазаров” № 2
Тел. +359 2 915 3580; факс: +359 2 915 3525
E-mail: kzld@cpdp.bg
Интернет страница: http://www.cpdp.bg/

Без да ограничаваме по какъвто и да било начин Вашето законово право да се свързвате с надзорния орган по всяко време, Ви молим да се свържете с нас предварително и обещаваме, че ще положим максимални усилия, за да разрешим възникналите проблеми по взаимно съгласие чрез следните начини за контакт:

Адрес: гр. Плевен, 5800, ул."Десети Декември" № 150, ет. 2
Електронна поща: margarita@camplight.net
Лице за контакт: Маргарита Христова

Настоящата Политика за защита на личните данни е утвърдена от Управителя на „Кемплайт“ ЕООД на 25.05.2018 година.

Политиката е актуализирана на 45.03.2026 г. и е утвърдена от Управителя на „Кемплайт“ ЕООД и от председателя на Кооперация "Кемплайт Кооп".