ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

НА

КАММАРТОН БЪЛГАРИЯ ЕООД

I. Общи положения

Каммартон България ЕИК: 040201751, със седалище и адрес на управление в гр. София, 1220, ул. „Илиенско шосе“ № 8, наричано по-нататък „Организацията“, е администратор на лични данни.

Тази политика определя основните принципи, чрез които Организацията обработва личните данни на своите клиенти, посетители, потребители на сайтове, служители, изпълнители по договори, доставчици, бизнес партньори и други физически лица.

Тя се прилага от всички служители и всички изпълнители, които работят от името на Организацията.

Организацията декларира, че сигурността на личните данни е от изключителна важност за нея и има голямо значение за успеха на бизнеса й и за имиджа й в обществото.

Организацията гарантира, че събирането на лични данни се осъществява в съответствие с действащото законодателство, добрите практики и бизнес стандарти.

При събирането и обработването на лични данни Организацията се подчинява на редица закони и нормативни правила, които разпореждат как да бъдат извършвани тези действия и какви гаранции за защита на личните данни да бъдат приложени. Относимата нормативна уредба включва, но не се ограничава до Общия регламент за защита на личните данни (Регламент (ЕС) 679/2016), Кодекса на труда, Кодекса за социално осигуряване, Закона за защита на личните данни, Закона за здравословни и безопасни условия на труд, Закона за счетоводството, Търговски закон, Закон за задълженията и договорите, Закон за защита на потребителите, както и издадените въз основа на тях подзаконови нормативни актове.

Организацията защитава личните данни, като прилага всички подходящи технически и организационни мерки, с които разполага, за да не допуска неразрешен достъп, неразрешено или злонамерено ползване, загуба или преждевременно заличаване на информация.

Тази политика се прилага за всички системи, хора и процеси, които изграждат информационната система на Организацията, включително спрямо лицата, заемащи управленски длъжности, служителите, доставчиците и всички други трети лица, които имат достъп до системите с лични данни на Организацията.

II. Защита на личните данни

1. Общ регламент за защита на данните (Регламент (ЕС) 2016/679)

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. 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, наричан по-нататък “Общ регламент за защита на данните” или “Регламента”, е един от най-важните законодателни актове, който засяга начина, по който Организацията извършва своите дейности по обработване на информация.

Политиката на Организацията е да гарантира, че спазва Регламента и другите приложими нормативни актове и може по всяко време да демонстрира съответствието на дейността си с тях.

2. Основни понятия

а) *Лични данни* са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано (*„субект на данни“*);

б) С*убект на данни* е физическо лице, което е идентифицирано или 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;

в) *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;

г) *Администратор на лични данни* 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;

д) *Обработващ лични данни* означава *физическо* или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

е) *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. 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;

ж) Съ*гласие на субекта на данните* означава 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;

з) *Нарушение на сигурността* на *лични данни* означава 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;

и) *Надзорен орган* означава независим публичен орган, създаден от държава членка съгласно член 51 от Регламента, който е отговорен за наблюдението на прилагането на Регламента, за да се защитят основните права и свободи на физическите лица във връзка с обработването и да се улесни свободното движение на личните данни в рамките на Съюза. В Република България този надзорен орган е Комисия за защита на личните данни.

3. Принципи, свързани с обработването на лични данни

Организацията се стреми да спазва основните принципи по Регламента във връзка с обработването на лични данни, като поема конкретни отговорности във връзка с всеки един от тях.

а) Законосъобразност, добросъвестност и прозрачност
Организацията обработва личните данни законосъобразно, добросъвестно и по прозрачен начин по отношение на субектите на данни.

б) Ограничение на целите
Организацията събира личните данни за конкретни, изрично указани и легитимни цели и не ги обработва по-нататък по начин, несъвместим с тези цели.

в) Свеждане на данните до минимум
Организацията се стреми личните данни, които обработва, да бъдат подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват.

г) Точност
Организацията се стреми личните данни, които обработва да са точни и при необходимост да бъдат поддържани в актуален вид. Организацията предприема всички разумни мерки, за да гарантира

своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.

д) Ограничение на съхранението
Организацията съхранява личните данни във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни.

е) Цялостност и поверителност
Организацията обработва личните данни по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки. По възможност Организацията прилага анонимизация или псевдонимизация на личните данни, за да ограничи рисковете за субектите на данни.

ж) Отчетност
Организацията носи отговорност и е в състояние да докаже спазването на всички принципи на Регламента, изброени дотук.

Организацията гарантира, че отговаря на всички тези принципи както при обработването на лични данни, което извършва в момента, така и като част от въвеждането на нови средства за обработване, като например нови информационни системи.

4. Права на субектите на данни

Правата на субектите на данни по Регламента са:
а) право на информираност;
б) право на достъп;
в) право на коригиране;
г) право на изтриване (право “да бъдеш забравен”);
д) право на ограничаване на обработването;
е) право на преносимост на данните;
ж) право на възражение;
з) права при автоматизирано вземане на индивидуални решения и профилиране;
и) право на жалба.
Организацията съдейства на субектите на данни при упражняването на техните права, като ги информира за тях и се стреми да удовлетвори исканията им и да им даде отговор в законоустановения срок, когато тези искания са основателни.

Когато са подадени искания за упражняване на права от субекти на данни, Организацията гарантира, че тези искания се обработват в разумен срок и води дневник за тях.

Организацията приема процедура, по която субектите на данни могат да упражнят своите права по отношение на личните си данни, и техните искания се обработват своевременно и ефективно.

5. Съгласие

Организацията спазва всички изисквания на Регламента за личните данни, събирани и обработвани на правно основание съгласие на субекта на данни. По-конкретно за случаите, в които съгласието е необходимо, Организацията спазва изискванията и условията за неговото изрично получаване. В такива случаи Организацията предоставя на субектите на данни прозрачна информация за използването на личните данни в момента на получаване на съгласието и разяснява правата им по отношение на техните данни, като например правото да се оттегли съгласието. Организацията предоставя тази информация в достъпна форма, безплатно и на ясен език. Ако личните данни не са получени директно от субекта на данните, то Организацията предоставя тази информация в разумен срок след получаване на данните и не по-късно от един месец от получаване на данните, а ако данните се използват за връзка със субекта на данните – най-късно в момента на осъществяване на първия контакт с него.

Когато обработването на лични данни се основава на съгласието на субекта на данните, Организацията е отговорна за запазването на това съгласие. Организацията отговаря за предоставянето на съгласието на субектите на данни, които трябва да дадат съгласието си, и ги информира и гарантира, че тяхното съгласие може да бъде оттеглено по всяко време.

6. Използване на личните данни за друга цел (освен първоначалната)

Организацията обработва личните данни само за целите, за които първоначално са били събрани. В случай че възникне необходимост събраните данни да се обработват за друга цел, Организацията прави индивидуална преценка за съвместимостта на целите за всеки конкретен случай, както и ако е необходимо, ще поиска съгласието на своите субекти на данни в ясна и кратка форма.

Организацията включва във всяко такова искане първоначалната цел, за която са събрани данните, както и новата или допълнителната/ите цел/и. Искането включва и причината за промяната на целта/целите. Длъжностното лице по защита на данните отговаря за спазването на правилата в този параграф.

7. Защита на личните данни на етапа на проектирането

Организацията приема принципа за защита на личните данни на етапа на проектирането и гарантира, че определянето, планирането и изграждането на всички нови или значителната промяна на вече съществуващи системи, които събират или обработват лични данни, ще бъдат обект на надлежна преценка, свързана със защитата на личните данни, включително ако е необходимо, извършването на една или повече оценки на въздействието върху защитата на данните.

8. Оценка на риска и оценка на въздействието.

Организацията оценява риска за правата и свободите на субектите на данни за дейностите по обработване и при установяване на висок риск за някоя дейност, извършва оценка на въздействието върху защитата на данните.

При извършването на оценката на въздействие върху защитата на личните данни Организацията включва най-малко следната информация/оценки:

- Системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;
- Оценка дали предложеното обработване на лични данни е едновременно необходимо и пропорционално за целите, за които се извършва;
- Оценка на рисковете за правата на субектите на данни във връзка с планираните операции по обработване;
- Мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

Организацията се ангажира да използва технически мерки като псевдонимизиране, криптиране и други подходящи технически мерки за защита на личните данни, когато е осъществимо и приложимо.

9. Трансфер на лични данни

Организацията се задължава предаването на лични данни, които се обработват или са предназначени за обработване след предаването на трета държава или на международна организация, да се осъществява само при условие, че са спазени разпоредбите на Регламента, включително във връзка с последващи предавания на лични данни от третата държава или от международната организация на друга трета държава или на друга международна организация, за да се осигури необходимото ниво на защита на физическите лица по Регламента и те да не бъдат изложени на риск.

10. Ключови длъжности и отговорности във връзка със защитата на личните данни

Всеки, който работи за Организацията и има достъп до личните данни, които тя обработва, отговаря за тяхната защита.

Ключовите длъжности и отговорности за защитата на личните данни в Организацията са:

а) Управителните органи на Организацията

Управителните органи взимат решения и одобряват стратегиите, политиките и правилата на Организацията във връзка със защитата на личните данни;

б) Длъжностното лице по защита на личните данни

Длъжностното лице по защита на личните данни е отговорно за управлението на програмата за защита на личните данни в Организацията и за разработването, въвеждането и популяризирането на политиките и процедурите за защита на личните данни и участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни;

в) Лицата, осъществяващи правното обслужване на Организацията

Лицата, осъществяващи правното обслужване на Организацията, съвместно с Длъжностното лице по защита на данните, наблюдават и анализират законодателството в областта на защитата на личните данни и промените в него, разработват и актуализират необходимите правни документи и оказват правна помощ на Организацията за постигане на неговите цели, свързани с личните данни;

г) Специалистите по информационни технологии

Специалистите по информационни технологии отговарят за това всички системи, оборудване и услуги, използвани за съхранение на данни, да съответстват на стандартите за сигурност и извършват периодични проверки и сканирания, за да гарантират, че хардуера и софтуера функционират правилно;

д) Лицата, заети с управлението на човешките ресурси

Лицата, заети с управлението на човешките ресурси отговарят съместно с Длъжностното лице по защита на данните за провеждането на редовни обучения на служителите във връзка със защитата на личните данни, както и самостоятелно за това личните данни на служителите и изпълнителите по договори с Организацията да бъдат обработвани законосъобразно;

е) Лицата, натоварени с маркетинга и връзката с клиентите и външните лица

Лицата, натоварени с маркетинга и връзката с клиентите и външните лица, подпомагани от Длъжностното лице по защита на данните, отговарят за това всички маркетинг инициативи и комуникации до клиентите и външните лица да съответстват на принципите за защита на личните данни, в това число и комуникацията с медиите;

ж) Лицата, натоварени с организирането на работата с външни лица – доставчици на продукти и услуги

Лицата, натоварени с организирането на работата на Организацията с външни лица – доставчици на продукти и услуги, отговарят за осигуряването в отношенията с доставчиците на адекватно ниво на защита на личните данни, включително чрез подбор на доставчици, които предоставят достатъчни гаранции, че са предприели подходящи технически и организационни мерки за защита на личните данни, които им стават известни или биха могли да им станат известни във връзка с предоставяне на продукти и услуги на Организацията.

11. Уведомления и съобщения при нарушение на сигурността на личните данни

Политиката на Организацията е да се спазват принципите на добросъвестност и пропорционалност, когато се обсъжда какви действия да бъдат предприети, за да се информират засегнатите страни при нарушение на сигурността на личните данни. В съответствие с Регламента, когато е налице нарушение, което може да доведе до риск за правата и свободите на физическите лица, Организацията ще информира надзорния орган в рамките на 72 часа от узнаване на нарушението от страна на Организацията, съгласно приетата и одобрена от Организацията Процедура по уведомяване и съобщаване на нарушения на сигурността на личните данни.

12. Обучения, тренинги и инструктажи

Организацията осигурява на служителите си възможността за периодични обучения и тренинги във връзка със защитата на личните данни и провежда инструктажи, за да гарантира, че всички служители, които под една или друга форма оперират с лични данни, разбират своята отговорност за спазване на добрите правила и практики за тяхната защита.

13. Преглед и актуализиране

Организацията извършва преглед и актуализация на всички политики и процедури, свързани със защитата на личните данни най-малко веднъж годишно, както и при промени в действащото законодателство, структурата и дейностите на Организацията.

14. Информация

Организацията поддържа следната информация в актуален вид:

- Наименование на организацията и координати за връзка, включително с длъжностното лице по защита на данните;
- Цели на обработването на лични данни;
- Категории лица и лични данни, които се обработват;
- Категории получатели, на които личните данни се разкриват;
- Срокове за съхранение на личните данни;
- Прилагани технически и организационни мерки за защита на данните.

Настоящата политика е приета от Управителя на 23.05.2018 г. Тя подлежи на преглед и актуализация най-малко веднъж годишно, както и при промени в приложимото законодателство.