Политика за защита на личните данни на администратор БИСЕИ ЕООД

I. Въведение и представяне

1. БИСЕИ ЕООД ЕИК 203612428 е администратор по смисъла на член 26 параграф 1 от Регламент (ЕС) 2016/679. За целите на настоящия документ те ще бъде наричан за краткост Администратор.

2. Контактна информация:
   - Адрес: ул. Проф. Д-р Д. Атанасов 22, ап. 11 София 1680
   - Интернет адрес: www.bi-sei.com
   - Телефон:+359 877377505

3. За Отговорник по защита на данните Администраторът определя Павлина Клисурска-Фистолера по съвместяване с другата й длъжност. Задължения:
   - разработва и внедрява изискванията на РЕГЛАМЕНТ (ЕС) 2016/679 както се изисква от настоящата политика;
   - пряко отговорно е да гарантира, че като цяло Администратора, съответства на изискванията на Регламент (ЕС) 2016/679;
   - отговаря за управлението на сигурността и риска по отношение на съответствието с политиката;
   - представлява Администратора по всички въпроси, свързани с обработването на данни.

II. Дефиниции

1. Всички термини, използвани в този документ, са в смисъла на дефинирането им в член 4 на Регламент (ЕС) 2016/679 на Европейския Парламент (Общ регламент относно защитата на данните – ОРЗД).

III. Категории субекти на данни

В бизнес дейността си Администратора има взаимодействие със следните категории субекти на данни:

1. Представители на юридически лица, информацията за които е публично достъпна в регистрите на Агенцията по вписванията
2. Физически лица – потребители на услугите на Администратора или потенциални такива

Настоящата политика има за цел да осигури защитата на данните на физическите лица от страна на Администратора.

IV. Категории лични данни

Съобразно нуждите на дейността си Администратора събира и обработва следните категории лични данни:

1. Обикновени лични данни – имена, адрес, електронна поща, IP адрес
2. Единен граждански номер, когато това се изисква за сключване на различни договорни отношения и издаване на фактури.

Администратора не събира и не обработва чувствителни лични данни.

Всички категории лични данни са описани подробно в Регистъра на дейностите по обработването на лични данни

V. Правни основания за обработване на данните

1. Съгласие:
    - Администраторът поддържа информация за данните, събрани въз основа на съгласие на субекта, като за всеки един случай може да докаже, че даденото съгласие е:
        - свободно изразено – не дадено под натиск или заплаха от неблагоприятни последици;
        - конкретно – отделно съгласие за всяка конкретно определена цел, а когато е относимо – и за конкретна категория лични данни;
        - информирано – дадено на основата на пълна, точна и лесно разбираема информация;
        - недвусмислено – не се извлича или предполага на основата на други изявления или действия на лицето;

        - изрично изявление или ясно потвърждаващо действие – не се приема за съгласие мълчанието на даден субект на данни.
    - Администраторът поддържа документация (в електронен вид) за изразеното съгласие с цел доказване пред компетентните органи.
    - Администраторът е подсигурил възможност за оттегляне на даденото съгласие по всяко време толкова лесно, колкото е дадено.
2. Сключване или изпълнение на договор
3. Законово задължение

Всички категории лични данни със съответното основание за обработване са описани подробно в Регистъра на дейностите по обработването на лични данни

VI. Цели на обработването на данни

1. Счетоводно отчитане
2. Търговска и маркетингова дейност
3. Съгласно договорни отношения с контрагенти

Всички цели на обработването на данни са описани подробно в Регистъра на дейностите по обработването на лични данни.

VII. Предоставяне на личните данни

Администраторът 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.

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 Длъжностното лице за защита на данните.

Извън организацията Администраторът предоставя данни на следните контрагенти:

1. Публични органи – НАП, НОИ
2. На други обработващи лични данни съобразно нуждите на бизнес дейността:
    - Счетоводна кантора
    - IT компании, поддържащи интернет сайтовете на Администратора, имейл платформата и информационната система

Всички получатели на данни са описани подробно в Регистъра на дейностите по обработването на лични данни.

VIII. Трансфер на данните

1. Администраторът събира и обработва електронни адреси на потенциални и настоящи клиенти мануално.
2. Извън т.1 Администраторът третира всеки износ на данни от рамките на ЕС към страни извън ЕС (посочени в Общия регламент като “трети страни”) като незаконен, освен ако няма подходящо ниво на защита на основните права на субектите на данни.
3. Изключения: прехвърляне на лични данни в трета страна или международна организация се извършва само при едно от следните условия:
    - предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
    - предаването е необходимо поради важни причини от обществен интерес;
    - предаването е необходимо за установяването, упражняването или защитата на правни претенции;
    - предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;
    - предаването се извършва от регистър, който съгласно правото на ЕС или правото на държавите членки е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

IX. Съхранение и унищожение на данните

1. Администраторът не съхраняват 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. Администраторът може да съхраняват данни за по-дълги периоди единствено ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, 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. Процедура за съхраняване и унищожаване на данните, приета от Администраторът се прилага във всички случаи.
4. Личните данни ще бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност (чл. 5, пар. 1 б. е) от Общия регламент) – включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

X. Оценка на риска

1. Администраторът е наясно с рисковете, свързани с обработването на определени видове лични данни.
2. Администраторът 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 и във връзка с обработването, предприето от други организации от името на Администраторът.
3. Администраторът управлява всички рискове, идентифицирани от оценката на въздействието, с цел да се намали вероятността от несъответствие с тези правила.
4. Когато в резултат на Оценката на въздействието е ясно, че Администраторът ще започне да обработва лични данни, които поради висок риск биха могли да причинят вреди на субектите на данни, решението дали обработването да продължи или не, трябва да бъде предадено за преглед от страна на Отговорника за защита на данните.

5. Ако ДЛЗД има сериозни опасения или относно потенциалната вреда или опасност, или относно количеството на съответните данни, то следва да ескалира въпроса пред надзорния орган.
6. Отговорникът по защита на данните прави периодичен (ежегоден) преглед на първоначално инвентаризираните данни, преразглежда вписаната информация в Регистъра на дейностите по обработване в светлината на всякакви промени в дейностите на АДМИНИСТРАТОРА.

XI. Мерки за сигурност

1. Администраторът е осигурил съответните технически и организационни мерки за сигурност на обработваните данни, подробно описани в Регистъра на дейностите по обработването на данни.

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.

XII. Принципи при защита на данните

Администраторът извършва цялата обработка на лични данни в съответствие с принципите за защита на данните, посочени в член 5 от Регламент (ЕС) 2016/679. Политиката и процедурите на Администратора имат за цел да гарантират спазването на тези принципи.

1. **Законосъобразност, добросъвестност и прозрачност:** Личните данни се обработват законосъобразно, добросъвестно и прозрачно
    - Законосъобразно – с идентифицирана законна основа/правно основание.
    - Добросъвестно – Администраторът предоставя необходимата 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.
        - Всички формуляри за събиране на данни (електронни или на хартиен носител), включително изискванията за събиране на данни в новите информационни системи, трябва да включват декларация за добросъвестно обработване или да бъдат одобрени от ДЛЗД.

- Прозрачно – във всеки един момент Администраторът може да предоставя обобщена, кратка и разбираема информация чрез интернет сайта си или по друг достъпен за субектите на данни начин относно:
  - идентифициране на дружеството или организацията – наименование и начин за контакт, включително с Отговорника по защита на данните, ако има такова (адрес, електронна поща, телефон и т.н.);
  - какви категории лични данни се събират и за какви цели се обработват;
  - категориите получатели на лични данни извън дружеството или организацията, както и дали ще се предават (трансферират) данни в трети страни извън ЕС;
  - срока за съхранение на данните;
  - съществуването на конкретни права на субектите на данните (право на достъп, коригиране или изтриване на лични данни, ограничаване на обработването, възражение срещу обработването, преносимост на данните) и реда за упражняването им;
  - правото на субектите на данни да подадат жалба до КЗЛД или до съда;
  - дали предоставянето на лични данни е задължително по закон или договорно изискване, както и евентуалните последствия, ако тези данни не бъдат предоставени;
  - (ако е приложимо) дали има автоматизирано вземане на решения, включително профилиране.

2. **Ограничение на целите**
   - Лични данни се събират само за конкретни, изрично указани и законни цели и не се обработват по-нататък по начин, несъвместим с тези цели.
   - По-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели („ограничение на целите“)
3. **Свеждане на данните до минимум**
   - Личните данни трябва да бъдат адекватни, релевантни, ограничени до това, което е необходимо за обработването им със съответната цел с оглед спазване на принципа на минимално необходимото.
   - ДЛЗД/Отговорникът по защита на данните е отговорен да осигури Администратора да не събира информация, която не е строго необходима за целта, за която тя е получена.

- Отговорникът по защита на данните ще гарантира, че на годишна основа всички способи за събиране на данни се преглеждат, за да се гарантира, че събраните данни продължават да бъдат адекватни, релевантни, и не са прекомерни.

4. **Точност:** Личните данни трябва да бъдат точни и актуализирани във всеки един момент, и да са положени необходимите усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.
   - Данните, които се съхраняват от администратора на данни, трябва да бъдат преглеждани и актуализирани при необходимост. Не се съхраняват данни, в случаите, когато има вероятност да не са точни.
   - От клиентите / други се изисква да уведомяват Администратора за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Отговорността на Администратора е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия.
   - Отговорникът по защита на данните носи отговорност да се гарантира, 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, други релевантни фактори.
   - Най-малко на годишна база Отговорника по защита на данните ще преглежда сроковете на съхранение на всички лични данни, обработвани от АДМИНИСТРАТОРА, 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.
   - Отговорникът за защита на данните е отговорно за вземане на подходящи мерки, в случаите когато организациите на трети страни имат неточни или остарели лични данни, да ги информира, че информацията е неточна или остаряла и е да не се използва за вземане на решения относно лицата, да информира съответните страни и да препраща всяка корекция на лични данни към третите страни, където това е необходимо.

5. **Ограничение на съхранението:** 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.

- Когато личните данни се запазват след датата на обработването, те ще бъдат съхранявани по подходящ начин (минимизирани), за да се защити самоличността на субекта на данните в случай на нарушение на данните.
- Лични данни ще бъдат пазени в съответствие с Процедура за съхраняване и унищожаване на данните, а след като е преминал срокът им на съхранение, те трябва да бъдат надеждно унищожени по указания в тази процедура ред.
- Отговорникът за защита на данните специално трябва да одобри всяко запазване на данни, което надхвърля срока на съхранение, дефиниран в Процедура за съхраняване и унищожаване на данните 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. **Цялостност и поверителност:**
   - Личните данни са обработвани по начин, който гарантира подходящо ниво на сигурността им, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки;
   - Отговорникът за защита на данните оценява риска като взема предвид всички обстоятелства, свързани с операциите по управление или обработване на данни от АДМИНИСТРАТОРА.
   - При определянето на това доколко уместно е обработването, Отговорникът по защита на данните трябва също така да разгледа степента на евентуална вреда или загуба, която може да бъде причинена на физически лица (напр. клиенти), ако възникне нарушение на сигурността, както и всяка вероятна вреда за репутацията на администратора, включително евентуална загуба на доверие на клиентите.

7. **Спазване на принципа на отчетност**
   - Регламент (ЕС) 2016/679 включва разпоредби, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност. Принципът на отчетност в чл. 5, пар. 2 изисква от администратора да докаже, че спазва останалите принципите в ОРЗД и изрично заявява, че това е негова отговорност.
   - АДМИНИСТРАТОРА ще доказва спазването на принципите за защита на данните чрез прилагане на политики по защита на данните, като се присъединява към кодекси за поведение, внедрява подходящи технически и организационни мерки, както и чрез приемане на техники по защита на данните на

етапа на проектирането и защита на данните по подразбиране, оценка на въздействието върху защитата на личните данни, процедура за уведомяване за нарушаване на лични данни и т.н.

XIII. Практическо упражняване на права от субектите на данните

1. Администраторът осигурява практическа възможност за упражняване на правата, които Регламент 2016/679 предоставя на субектите на данни:
   - право на достъп до личните данни, които се обработват от дружеството;
   - право на коригиране или допълване на неточни или непълни лични данни;
   - право на изтриване („право да бъдеш забравен“) на лични данни, които се обработват незаконосъобразно или с отпаднало правно основание (изтекъл срок на съхранение, оттеглено съгласие, изпълнена първоначална цел, за която са били събрани и др.);
   - право на ограничаване на обработването – при наличие на правен спор между дружеството/организацията и физическото лице до неговото решаване и/или за установяването, упражняването или защитата на правни претенции;
   - право на преносимост на данните – ако се обработват по автоматизиран начин на основание съгласие или договор. За целта данните се предават в структуриран, широко използван и пригоден за машинно четене формат. Ако е технически осъществимо, прехвърлянето на данните може да стане пряко от един администратор към друг. Правото на преносимост обхваща само данни, предоставени лично от субекта на данни, както и лични данни, генерирани и събрани от неговата дейност.
   - право на възражение – по всяко време и на основания, свързани с конкретната ситуация на лицето, при условие, че не съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или съдебен процес;
   - право да не бъде обект на изцяло автоматизирано решение, включващо профилиране, което поражда правни последствия за субекта на данните или го засяга в значителна степен.

2. Администраторът има разписани вътрешни процедури за приемане, разглеждане и отговаряне в едномесечен срок на искания от физически лица за упражняване на правата им като субекти на лични данни и създаване на организация за прилагането им на практика.

XIV. Уведомяване за нарушение на сигурността на данните

1. В случай на нарушение на сигурността на личните данни Администраторът като администратор на лични данни, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрала за него, уведомява за нарушението на сигурността на личните данни КЗЛД като надзорен орган за Република България. , компетентен в съответствие с член 55, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.
2. Администраторът, като обработващ лични данни уведомява администратора без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.
3. В уведомлението се съдържа най-малко следното:
    - описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
    - посочване на името и координатите за връзка на отговорника по защита на данните или на друга точка за контакт, от която може да се получи повече информация;
    - описание на евентуалните последици от нарушението на сигурността на личните данни;
    - описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.
4. Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.
5. Администраторът, като администратор документира всяко нарушение на сигурността на личните данни, включително фактите,

свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на надзорния орган да провери дали е спазен член 33 от ОРЗД.

XV.Декларация относно политиката по защита на личните данни

1. Ръководството на Администратора се ангажира да осигури съответствие със законодателството на ЕС и държавите-членки по отношение на обработването на личните данни и защитата на “правата и свободите” на лицата, чиито лични данни Администраторът събира и обработва съгласно Общия регламент за защита на данните (Регламент (ЕС) 2016/679).
2. В съответствие с Общия регламент към тази политика са описани и други релевантни документи, както и свързани процеси и процедури.
3. Регламент (ЕС) 2016/679 и тази политика се отнасят до всички функции по обработването на лични данни , включително тези, които се извършват относно лични данни на клиенти, доставчици и партньори и всякакви други лични данни, които организацията обработва от различни източници.
4. Отговорникът по защита на данните отговаря за преразглеждането на Регистъра на дейностите по обработване ежегодно в светлината на всякакви промени в дейността на Администратора, както и всички допълнителни изисквания, оценки на въздействието върху защитата на данните. Този регистър трябва да бъде на разположение по искане на надзорния орган.
5. Тази политика се прилага за всички партньори на Администратора като външни доставчици. Всяко нарушение на Общия регламент ще бъде разглеждано като нарушение на трудовата дисциплина, а в случай че има предположение за извършено престъпление, въпросът ще се предостави за разглеждане в най-къс възможен срок на съответните държавни органи.
6. Партньори и трети лица, които работят с Администратора, както и които имат или могат да имат достъп до личните данни, ще се очаква да се запознаят, разбират и да се съобразят с тази политика. Никоя трета страна не може да има достъп до лични данни, съхранявани от Администратора, без предварително да е сключила споразумение за поверителност на данните, което налага на третата страна задължения, не по-малко обременяващи от тези, които Администратора е поел, и което дава право на

АДМИНИСТРАТОРА да извършва проверки на спазването на наложените със споразумението задължения.

XVI. Документиране и отчетност

1. Администраторът е създал 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 Регламент (ЕС) 2016/679. При инвентаризацията на данните в работният 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. Във връзка с точка 1, Администраторът изготвя и актуализира периодично следните документи съгласно Регламент 2016/679
    - **Вътрешен регистър на дейностите по обработване на лични данни в организацията** със следната информация:
        1. името и координатите за връзка на всички съвместни администратори, на представителите на администраторите и на Длъжностното лице по защита на данните;
        2. целите на обработването;

- описание на категориите субекти на данни и на категориите лични данни;

3. категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
4. когато е приложимо – предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, документация за подходящите гаранции;
5. предвидените срокове за изтриване на различните категории данни;

- общо описание на техническите и организационни мерки за сигурност.

- **Вътрешна политика за защита на личните данни** в организацията (настоящият документ).
- **Договори с обработващи лични данни** с цел включване в тях на всички задължителни реквизити съгласно чл. 28 от Общия регламент относно защитата на данните.
- **Други процедури и правила:**
- Процедура за управление на исканията на субектите
- Процедура за начините на комуникация при жалби
- Процедура за получаване на съгласие за обработване на данните и по оттегляне на съгласието от субекта на данните
- Процедура за съхраняване и унищожаване на данните, която включва и оценка на риска и избор на подходящи технически и организационни мерки
- Правила за възлагане на работа на подизпълнители
- Процедура по уведомяване за нарушение на сигурността на личните данни.
- **Декларации и договори:**
- Декларация за поверителност
- Форма за искане от субект на данните
- Декларация за съгласие на субекта на данните
- Форма за оттегляне на съгласието от субекта на данните
- Декларация за съгласие от родител/настойник
- Форма за оттегляне на съгласието от родител/настойник

3. Администраторът като администратор на лични данни определя по прозрачен начин съответните си отговорности за изпълнение на задълженията по ОРЗД, по-специално що се отнася до упражняването на правата на субектите на данни и съответните им задължения за предоставяне на информацията, посочена в членове 13 и 14 от Регламента, посредством договореност помежду си, отразена в отделен документ.

XVII. Промени в тази политика

1. Всички промени, които може в бъдеще да бъдат направени в тази политика, ще бъдат публикувани на посочените сайтове.
2. Последна промяна: 25 май 2018 г.