Лого	**ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ**		
ОРЗД	Идент. № **POLITIKA**	Версия **0.1**	Стр. **1** от **27**
Администратор: **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**			

Версия	**Дата**	**Описание**	**Автор**	**Одобрил**
1	10 юни 2018г	Вътрешно организационен документ по защита на личните данни, съгласно изискванията на **ОРЗД.**		Решение на Представляващия от 10 юни 2018г

I.ВЪВЕДЕНИЕ

1.1. Общ регламент за защита на личните данни

Регламент (ЕС) 2016/679 (Общ регламент за защита на данните - **ОРЗД**) замества Директивата 95/46 / ЕО за защита на данните. Има пряко действие и предполага изменение в законодателството на страните-членки в областта на защитата на личните данни. Неговата цел е да защитава "правата и свободите" на физическите лица и да се гарантира, че личните данни не се обработват без тяхно знание, и когато е възможно, че се обработва с тяхно съгласие.

Настоящата Политика определя реда, по който **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** (наричана по-долу Фондацията, Администратор/а, в случаите, когато Дружеството събира, записва, организира, структурира, съхранява, адаптира или променя, извлича, консултира, използва, разкрива чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подрежда или комбинира, ограничава, изтрива, унищожава или обработва по друг начин лични данни за целите на своята дейност.

Политиката е изготвена в съответствие с изискванията на 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 за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните/ **ОРЗД**) и Закон за защита на личните данни (ЗЗЛД).

Настоящата Политика урежда:

- Принципите, процедурите и механизмите за обработка на личните данни;
- Процедурите за администриране на искания за достъп до данни, коригиране на обработваните данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат по закон;

- Процедурите за уведомяване на надзорния орган в случай на нарушения в сигурността;
- Лицата, които обработват лични данни и техните задължения;
- Правилата за предаване на лични данни на трети лица в България и чужбина;
- Необходимите технически и организационни мерки за защита на личните данни от неправомерно обработване и в случай на инциденти, като случайно или незаконно унищожаване, загуба, неправомерен достъп, изменение или разпространение;
- Техническите ресурси, прилагани при обработката на лични данни.
- Вътрешни политики и инструкции на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161.**

1.2. Обхват очертан от Общия регламент за защита на данните

Материален обхват (член 2) – **ОРЗД** се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни (например ръчно и на хартия), които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

Териториален обхват (член 3) – правилата на **ОРЗД** ще важат за всички администратори на лични данни, които са установени в ЕС, които обработват лични данни на физически лица, в контекста на своята дейност. Ще се прилага и за администратори извън ЕС, които обработват лични данни с цел да предлагат стоки и услуги или ако наблюдават поведението на субектите на данни, които пребивават в ЕС.

Настоящата Политика влиза в сила от датата на нейното одобрение и е задължителна за всички работници и служители на Фондацията, които са определени с нарочно решение на ръководството на Фондацията като отговорни за обработването на лични данни във връзка с изпълнението на служебните им задължения. В случаите и за периодите, когато няма назначени работници и служители, задълженията по настоящата Политика са на Представляващия администратора. Политиката се прилага от Фондацията в отношенията й като Администратор с други администратори на лични данни, обработващи лични данни, субекти на данни, отговорни лица по защита на данните, както и по отношение на всички трети лица, които имат право на достъп до лични данни в регистрите на дейностите по обработване.

Конкретни задължения и отговорности по настоящата политика имат служители във Фондацията, определени с нарочна заповед на Представляващия, а в отделни случай, както и когато няма назначени такива - Представляващия Фондацията.

1.3. Понятия

„Лични данни" - всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

„Специални категории лични данни" – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация.

„Обработване" - означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

„Администратор" - всяко 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 ЕС 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;

„Субект на данните“ – всяко живо физическо лице, което е предмет на личните данни съхранявани от Администратора.

„Съгласие на субекта на данните" - 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;

„Дете“ – Общият Регламент определя дете като всеки на възраст под 16 години въпреки че това може да бъде намалена на 13 от правото на държавата-членка. Обработката на лични данни на едно дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или упълномощен да даде съгласието си.

„Профилиране" - всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

„Надзорен орган“ – независим публичен орган, създаден от държава членка съгласно чл.51 от **ОРЗД**. В настоящата Политика „Надзорен орган“ обозначава Комисия за защита на личните данни (КЗЛД).

„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;

„Основно място на установяване “ – седалището на администратора в ЕС ще бъде мястото, в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде неговият административен център.

„Получател" - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели"; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

„Регистър с лични данни” е структурирана съвкупност от лични данни, достъпна по определени критерии съобразно вътрешните документи на Фондацията, която може да бъде централизирана и децентрализирана и е разпределена на функционален или географски принцип.

„Трета страна“ – всяко физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под

прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

1.4. Общи принципи на обработване на лични данни във Фондацията като Администратор.

1.4.1.Администраторът обработва личните данни законосъобразно, добросъвестно и прозрачно при спазване на следните принципи:

- Субектът на данните се информира предварително за обработването на неговите лични данни;
- Личните данни се събират за конкретни, точно определени и легитимни цели и не се обработват допълнително по начин, несъвместим с тези цели;
- Личните данни съответстват на целите, за които се събират и обработват;
- Личните данни са точни и при необходимост се поддържат в актуален вид;
- Личните данни се съхраняват 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;
- Личните данни се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, разкриване, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки;
- Приложените организационни и технически мерки осигуряват постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване на личните данни.

1.4.2.За да е законосъобразно обработването на данните, трябва да е налице поне едно от следните условия:

- Субектът на данните е дал своето съгласие;
- Обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;
- Обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;
- Обработването е необходимо, за да се защитят жизненоважни интереси на субекта на данните или на друго физическо лице;
- Обработването е необходимо за изпълнение на задача от обществен интерес;
- Обработването е необходимо за целите на легитимните интереси на Администратора, освен когато пред тези интереси преимущество имат интересите или основните права и свободи на субекта на данни.

II.ДЕКЛАРАЦИЯ - УВЕДОМЛЕНИЕ ОТНОСНО ПОЛИТИКАТА ПО ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

2.1. Ръководството на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**, се ангажират 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 **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** събира и обработва съгласно **ОРЗД**.

Декларацията – Уведомление за поверителност на личните данни на физически лица – клиенти, контрагенти и доставчици, посетители на сайта - Приложение №1 към настоящата Политика, заедно с разяснения за правата им по **ОРЗД** се публикува на сайта на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161–** https://www.innercompass.bg.

Декларацията – Уведомление за поверителност на личните данни на работници и служители на Фондацията, включително и лица по граждански договор, предоставящи услуги на Администратора, в случаите, когато има назначени такива - Приложение №2 към настоящата Политика, относно Политиката по защита на личните данни, която се отнася до засегнатите лица – работници и служители, както и лица, с които е сключен граждански договор с Фондацията, заедно с разяснения за правата им по **ОРЗД** им се връчва срещу подпис и се съхранява към личните им трудови досиета.

2.2. В съответствие с **ОРЗД** към тази Политика са описани и други релевантни документи, както и свързани процеси и процедури.

2.3. ОРЗД и тази политика се отнасят до всички функции по обработването на лични данни, включително тези, които се извършват относно лични данни на клиенти, контрагенти и доставчици, посетители на сайта, служители, партньори и всякакви други лични данни на физически лица, които организацията обработва от различни източници.

2.4. Партньори и трети лица, които работят с или за **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**, 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 **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**, без предварително да е сключила споразумение за поверителност на данните, което налага на третата страна задължения, не по-малко обременяващи от тези, които **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** е поело, и което дава право на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** да извършва проверки на спазването на наложените със споразумението задължения.

III.ЗАДЪЛЖЕНИЯ И РОЛИ ПО ОРЗД

3.1. **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** е Администратор, съгласно **ОРЗД**.

3.2. Представляващият **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** е отговорен за разработване и насърчаване на добри практики в областта на обработване на информация в **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**;

3.3. Спазването на законодателството за защита на данните е отговорност на всички служители на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**, в случаите, когато има назначени такива, на които ще бъде възложено да обработват лични данни, определени с нарочна заповед на Представляващия като лица, обработващи лични данни. Когато няма назначени такива служители, отговорен е Представляващият Фондацията.

3.4. Политиката за обучение на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** изисква да се извършва регулярно обучение и инструктаж на служителите, когато има назначени такива, по отношение изискванията за защита на личните данни в следните случай:

- първоначално обучение на служителите, имащи отношение към обработването на лични данни - при назначаването им;

- при въвеждане на съществени изменения и допълнения на настоящата Политика и другите изисквания на **ОРЗД –** тълкувания на компетентните органи и т.н. – за всички назначени служители, имащи отношение към процесите на обработване на лични данни;

- при въвеждане на нови технически и организационни решения – софтуери, правила– за всички назначени служители, имащи отношение към процесите на обработване на лични данни;

За проведеното обучение и инструктаж, служителите подписват нарочен документ – Протокол за обучение и инструктаж, Приложение №3а към настоящата Политика за проведено обучение и инструктаж, които се съхраняват към личните им трудови досиета.

IV. РОЛИ ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ ВЪВ ФОНДАЦИЯТА

4.1. Администратор на лични данни

Прилагането на необходимите технически и организационни мерки за защита на личните данни се осъществява от Администратора, **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**, с адрес:

- гр. София, 1000,
- район Оборище,
- Г.БЕНКОВСКИ No 12А, вх. Б, ап. 2
- тел.: 0888885082,
- Електронна поща: zori@compass98.com, Интернет страница: www.innercompass.bg;
- Представляващ: Зорница Георгиева Стефанова-Иванова

Администраторът има следните задължения:

- определя политиката за защита на личните данни във Фондацията, спазва изискванията на **ОРЗД**, законодателството на ЕС в областта защита на личните данни и националното законодателство;
- осигурява организацията по поддържане на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита и ги актуализира при необходимост;
- въвежда подходящи технически и организационни мерки, разработени с оглед на ефективното прилагане на принципите за защита на данните;
- осигурява упражняването на правата на физическите лица за защита на личните данни;
- осъществява контрол по спазване на изискванията за защита на регистрите, установява обстоятелства, свързани с нарушаване на тяхната защита, и предприема мерки за тяхното отстраняване;
- поддържа личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;
- периодично информира персонала по въпросите на защитата на личните данни;
- оказва съдействие при осъществяването на контролните функции на Надзорния орган - КЗЛД, подпомага установяването на обстоятелства, свързани със защитата на личните данни; в случай на нарушение на сигурността на личните данни уведомява Надзорния орган без ненужно забавяне при установен риск за засегнатите лица;
- определя правата на служителите за достъп до лични данни в информационните системи съобразно целите на обработване, така че да се гарантира законосъобразност и да се спазят принципите на обработване;

- използва само обработващи лични данни, които предоставят достатъчни гаранции посредством прилагането на подходящи технически и организационни мерки за защита;
- в случай на установен висок риск за физическите лица, да ги информира по подходящ начин за нарушението по сигурността на личните данни;
- 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.

4.2. Длъжностно лице по защита на данните (ДЛЗД). Отговорни лица по защита на личните данни.

4.2.1. ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161 няма задължение и не е определила **ДЛЗД**.

4.2.2. Отговорните лица по защита на личните данни, имат следните задължения:

- осигуряват организацията по водене на регистрите по XV от настоящата Политика, съгласно предвидените мерки за гарантиране на адекватна защита;
- следят за спазването на конкретните мерки за защита и контрол на достъпа съобразно спецификата на водения регистър;
- контролират спазването на правата на субектите на данни във връзка с регистъра и програмно-техническите средства за тяхната обработка;
- специфицират техническите средства, прилагани за обработка на личните данни;
- провеждат периодичен контрол за спазване на изискванията по защита на данните и при открити нередности уведомяват Представляващия Фондацията като съвместно предприемат необходимите мерки за тяхното отстраняване.

4.3. Служители на Фондацията, обработващи лични данни

4.3.1.Служителите (в случаите, когато има назначени такива) на Фондацията в качеството му на Администратор, обработват лични данни след запознаване с действащата нормативна уредба в областта на защитата на личните данни и настоящата Политика, като подписват Декларация за неразгласяване на лични данни – Приложение №3б към настоящата Политика.

4.3.2.Служителите на Фондацията (в случаите, когато има назначени такива), обработващи лични данни са длъжни:

- да обработват личните данни само при наличие на основание, което произтича от закона, от договорните отношения с лицето, от изрично съгласие на лицето; от легитимния интерес на Администратора;
- да използват личните данни, до които имат достъп, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели;
- да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват;
- да не изнасят и съхраняват личните данни извън специално определените за целта места, регламентирани с режим на специален достъп;
- да спазват правилото за „чисто бюро“ и „чист екран“ по отношение на защитата на информацията и личните данни съгласно настоящата Политика – т.14.2.2.

- да предприемат мерки, така че външни лица да нямат какъвто и да е неправомерен достъп до документи, съдържащи лични данни, включително да могат да ги преглеждат, копират или фотографират с мобилен телефон;
- когато изпълнението на съответния процес позволява, използваните лични данни се ограничават до максимална степен (минимизация);
- да осигуряват и гарантират спазването на правата на физическите лица във връзка с обработването на лични данни;
- да оказват съдействие на Отговорните по защита на личните данни лица при изпълнение на техните функции.
- За неспазването на разпоредбите на **ОРЗД**, действащото национално законодателство и настоящата Политика, служителите на Фондацията носят дисциплинарна отговорност. Ако в резултат на действията на съответен служител на Фондацията при обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.

В периодите, когато в Фондацията няма назначени служители, които да бъдат определени с нарочна заповед на Представляващия като отговорни лица или лица, обработващи лични данни, то отговорностите по настоящата Политика се осъществяват от Представляващия Фондацията.

4.4. Обработващ лични данни

Във връзка с изпълнението на своята дейност, Фондацията като Администратор може да използва трети страни при обработването на лични данни (Обработващи лични данни) при условията на законосъобразност. Третите страни могат да бъдат:

- Търговски дружества, например специализирано счетоводно предприятие;
- Физически лица, наети на граждански договори – напр. адвокат;
- Публични институции;

При възлагане обработването на лични данни на трети страни, Администраторът задължително подписва Споразумение за поверителност с тези трети страни, с което се регламентират конкретните мерки, които ще се приложат във връзка с конкретното обработване така щото да се гарантира спазването изискванията на **ОРЗД.**

В случай, че Администраторът подлежи на одитиране по Закона за независимия финансов одит, той подписва Споразумение за поверителност на личните данни с избраното одитиращото дружество, което от своя страна се явява също Администратор на собствено правно основание.

В зависимост от поставената цел на обработване на лични данни, Администраторът може да сключва споразумение с друг администратор при наличие на общо определена цел. В това споразумение се определят отговорностите, правата и задълженията на всеки един администратор.

V.ПРИНЦИПИ ЗА ЗАЩИТА НА ДАННИТЕ

Цялата обработка на лични данни трябва да се извършва в съответствие с принципите за защита на данните, посочени в член 5 от **ОРЗД**. Политиките и процедурите на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** имат за цел да гарантират спазването на тези принципи.

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

Законосъобразно – да идентифицира законна основа, преди да може да обработва лични данни. Те често са посочени като "основания 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.

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

Прозрачно – **ОРЗД** включва правила относно предоставяне на поверителна информация на субектите на данни в членове 12, 13 и 14 от **ОРЗД.** 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.

Правилата за уведомяване на субекта на данни от **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** са определени в **т.VI** от настоящата Политика, уведомлението и съгласието на субекта на данните с Декларацията за поверителност, публикувана на сайта на Администратора се съхранява от Администратора в компютъра на Администратора до момента на унищожаване на данните. Подписаните уведомления на хартиен носител в офиса на Администратора се съхраняват по реда, по който се съхраняват личните данни на хартиен носител.

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

- данни, които идентифицират Администратора и данните за контакт с Администратора и, ако има такъв, на представителя на Администратора;
- целите на обработването, за което личните данни са предназначени както и правното основание за обработването;
- периода, за който ще се съхраняват личните данни;
- 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;
- категориите лични данни;
- получателите или категориите получатели на лични данни, където това е приложимо;
- където е приложимо, дали администраторът възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на данните;
- всякаква допълнителна информация, необходима да се гарантира добросъвестно обработване.

5.2. 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, официално обявени на надзорния орган като част от Регистъра на дейностите по обработване на данни (чл.30 от ОРЗД) на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**.

5.3. Личните данни трябва да бъдат адекватни, релевантни, ограничени до това, което е необходимо за обработването им със съответната цел. (принцип на минимално необходимото**).**

- Ръководството на Фондацията е отговорно да осигури **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** да не събира информация, която не е строго необходимо за целта, за която тя е получена.
- 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 връзка към Декларация-Уведомление за поверителност на Фондацията.
- Ръководството на Фондацията гарантира, че на (годишна) основа всички способи за събиране на данни се преглеждат от Ръководството на Фондацията, за да се гарантира, че събраните данни продължават да бъдат адекватни, релевантни, не са прекомерни.

5.4. 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.

- Данните, които се съхраняват в Фондацията, трябва да бъдат прегледани и актуализирани при необходимост. Не трябва да се съхраняват данни, в случаите, когато има вероятност да не са точни.
- Ръководството на Фондацията гарантира, че целият персонал е обучен в значението на събирането на точни данни и поддържането им.
- Също така, задължение на субекта на данните е да декларира, че данните, които предават за съхраняване от **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** са точни и актуални. Попълването на формуляр от субекта на данни, предназначени за Администратора, ще включва изявление, че съдържащите се в него данни са точни към датата на подаване – Приложение №4а към настоящата Политика.
- От служителите / работниците (клиентите / други) се изисква, да уведомяват **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Промяната в данните се отразява от Отговорното лице при възможност до седем дни, но не по-късно от един месец след подаването на информацията. Отговорността на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия.
- Най-малко на годишна база Отговорно лице, определено от Ръководството на Дружеството ще прегледа сроковете на съхранение на всички лични данни, обработвани от **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**, 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.
- Отговорно лице, определено от Ръководството на Фондацията е задължено да вземане 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.

5.5. 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.

- Личните данни няма да се запазват и ще се унищожават изтичане срокът им за обработване.
- Личните данни ще бъдат пазени за срока на обработка по следния начин:

- данните на клиенти хартиен носител – в шкафове в заключващо се помещение, като достъп до ключа имат само служителите, обработващи данните и определени с нарочна заповед на Представляващия на Фондацията, а когато няма назначени такива ключ се съхранява само от Представляващия на Фондацията.

- данните е електронен вид се съхраняват на персонален компютър на Фондацията, който се намира в самостоятелно помещение, в офиса на Фондацията и достъп до него има само Представляващия, съответно служителите, определени с нарочна заповед на Представляващия. Достъпването на данните може де се осъществи само от лицата, обработващи личните данни и определени със заповед на Представляващия, както и самия Представляващ. Всяко оторизирано лице достъпва данните чрез самостоятелно потребителско име и парола.

След като е преминал срокът им на съхранение, личните данни трябва да бъдат надеждно унищожени, както следва:

- данните на електронен носител се унищожават чрез изтриване по невъзстановим начин,
- данните на книжен носител се нарязват като „поверителен отпадък";

За унищожаването на данните винаги се съставя протокол, който се разписва от Представляващия и лицето, унищожаващо данните, съгласно Образец, Приложение №5 към настоящата Политика.

5.6. Личните данни трябва да бъдат обработени по начин, който гарантира подходяща сигурност (чл. 24, чл. 32 от ОРЗД)

Ръководството на Фондацията е извършило оценка на въздействието (оценка на риска), като е взело предвид всички обстоятелства, свързани с операциите по управление или обработване на данни от **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**. При определянето на това доколко уместно е обработването, Ръководството на Фондацията е разгледало степента на евентуална вреда или загуба, която може да бъде причинена на физически лица (напр. персонал или клиенти), ако възникне нарушение на сигурността, както и всяка вероятна вреда за репутацията на Администратора, включително евентуална загуба на доверие на клиентите. Рискът е оценен като нисък предвид малкия брой физически лица, чийто данни се обработват, както и с оглед вида на обработваните данни и начина на обработването им.

При оценяването на подходящи технически мерки, Ръководството на Фондацията разгледа следното:

- Защита с нива на достъп и пароли;
- Премахване на права на достъп за USB и други преносими носители с памет;
- Антивирусен софтуер;
- Правата за достъп основани на роли, включително тези, на назначен временно персонал.
- Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;
- Сигурност на локални и широкообхватни мрежи - пароли;
- Идентифициране на подходящи международни стандарти за сигурност подходящи за **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**.

При оценяването на подходящите организационни мерки Ръководството на Фондацията вземе предвид следното:

- Нивата на подходящо обучение в **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**;

- Мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.);
- Включването на защитата на данните в трудовите договори;
- Идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;
- Редовна проверка на персонала за спазване на съответните стандарти за сигурност;
- Контрол на физическия достъп до електронни и хартиено базирани записи;
- Приемането на правила на „чист екран и чисто работно място“;
- Съхраняване на хартия на базата данни в заключващи се шкафове в самостоятелно заключващо се помещение;
- Ограничаване на използването на портативни електронни устройства извън работното място;
- Ограничаване на използването от служителите на лични устройства на работното място;
- Редовно създаване на резервни копия на личните данни и физическо съхраняване на носителите с копия – правят се бекъпи на данните с период на съхранение – 120 дни като след изтичане на периода съответното архивно копие се унищожава;
- 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.

5.7. Спазване на принципа на отчетност

ОРЗД 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.

ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161 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.

VI. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Субектът на данни има следните права по отношение на обработването на данни, както и на данните, които се записват за тях:

- 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.
- Да поиска копие от своите лични данни от Администратора;
- Да иска от Администратора коригиране на лични данни когато те са неточни, както и когато не са вече актуални;
- Да изиска от Администратора изтриване на лични данни (право „да бъдеш забравен");

- Да иска от Администратора ограничаване на обработването на лични данни като в този случай данните ще бъдат само съхранявани, но не и обработвани.;
- Да направи възражение срещу обработване на негови лични данни;
- Да направи възражение срещу обработване на лични данни, отнасящо се до него за целите на директния маркетинг.
- Да се обърне с жалба до надзорен орган ако смята, че някоя от разпоредбите на ОРЗД е нарушена;
- Да поиска и да му бъдат предоставени личните данни в структуриран, широко използван и пригоден за машинно четене формат;
- Да оттегли съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до администратора;
- Да не е обект на автоматизирано взети решения, които да го засягат в значителна степен, без възможност за човешка намеса;
- Да се противопостави на автоматизирано профилиране, което се случва без негово съгласие;

ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161 осигурява условия, които да гарантират упражняването на тези права от субекта на данни:

6.1.Съгласие и оттегляне на съгласие.

6.1.1. Под „съгласие“ **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** 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.

6.1.2. **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** 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 му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

6.1.3. 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.

6.1.4. Когато не налице друго законово основание за извършване обработка на лични данни, трябва да се получи изрично писмено съгласие на субектите на данни по образец - Приложение №4б към настоящата Политика.

6.1.5. В повечето случаи съгласието за обработка на лични и специални категории данни се получава рутинно от **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**, като се използват стандартни документи за съгласие напр. когато нов клиент подписва договор или по време на набиране на нов персонал и т.н..

6.1.6. Когато **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** обработва лични данни на деца, трябва да бъде получено разрешение от упражняващите родителските права (родители, настойници и т. н.). Това изискване се прилага за деца на възраст под 16 години, освен ако не е налице друго основание за обработване на лични данни, например законово и договорно основание относно личните данни на децата, на които се предоставят образователни услуги от Администратора.

6.1.7.Субектът на данни е съгласен с обработването на лични данни, ако изрази това чрез ясно и недвусмислено изявление или друг потвърждаващ акт. Когато обработването се извършва въз основа на съгласие, то следва да е дадено лично чрез изявление – свободен текст, а ако субектът поиска съдействие от Администратора ще му бъде предложен образец на Декларация-съгласие за обработване на лични данни – Образец №4б. В случай че съгласието се дава чрез документ, който урежда и други въпроси, то следва да бъде изискано отделно от съгласието по други въпроси. Мълчаливото съгласие, предварително отметнатите полета или липсата на действие не представляват съгласие.

6.1.8.Субектът на данни може лесно да оттегли съгласието си за обработване по всяко време чрез подаване на писмено заявление до Администратора в свободен текст. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Ако не съществува друго условие за законосъобразност на обработването, с оттеглянето на съгласието то следва да се прекрати.

6.1.9.Съгласията на бивши, настоящи клиенти, контрагенти и техни представители; на бивши, настоящи служители и кандидати за работа се събират по следните канали:

- лично, в офиса на Дружеството;
- по електронна поща – z.stefanova@InnerCompass.bg

Декларацията-съгласие, Образец – Приложение №4б за обработване на лични данни и заявлението за оттегляне на съгласие се регистрират от Отговорното лице или от Представляващия Администратора в нарочен регистър – Приложение №6а на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** за съгласията и заявленията на субектите на личните данни.

6.2. Право на достъп до информация

6.2.1.Субектът на данни има право да поиска достъп до своите лични данни, включително и да иска потвърждение дали данните, отнасящи се до него се обработват, да се информира за целите на това обработване, категориите данни и за получателите на данните, както и за целите на всяко обработване на лични данни, отнасящи се до него.

6.2.2.Ако при осъществяване на достъпа до лични данни по искане на едно лице е възможно да се разкрият лични данни за друго лице, Администраторът е длъжен да предостави достъп само до частта от тях, отнасяща се до субекта на данни. Правото на достъп се осъществява чрез подаване на Заявление за достъп до лични данни – Образец, Приложение №5.

6.3. Право на изтриване, коригиране или блокиране (ограничаване на обработването)

6.3.1.Всеки субект на данни лице има право да поиска изтриването, коригирането или блокирането на негови лични данни, обработването на които не отговаря на изискванията на закона. Субектът на данни има право да поиска от Администратора да изтрие/коригира без ненужно забавяне личните му данни, чрез подаване на Заявление – Образец, Приложение №5.

6.3.2.Правото на блокиране (ограничаване на обработването) дава възможност на субекта на данни да изиска временно преустановяване обработката на личните му данни, с цел установяване тяхната точност и/или причините за тяхната обработка. Когато обработването е ограничено, личните данни се обработват само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции, за защита на правата на друго физическо лице или поради важни основания от обществен интерес. За да упражни това си право субектът на данни подава Заявление за ограничаване на обработването на личните данни – Образец, Приложение №5.

6.4. Право на преносимост на личните данни

6.4.1.Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на Администратора, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг Администратор, когато:

- обработването е основано на съгласие или на договорно задължение;
- обработването се извършва по автоматизиран начин.

6.4.2.Когато упражнява правото си на преносимост на данните, субектът на данните има право да получи пряко прехвърляне на личните данни от един администратор към друг, когато това е технически осъществимо.

6.4.3.Правото на преносимост се упражнява единствено, когато не влияе неблагоприятно върху правата и свободите на други лица. Субектът на данните упражнява правото си на преносимост чрез подаване на Заявление за преносимост на лични данни – Образец, Приложение №5.

6.5. Право на възражение срещу обработването на лични данни

6.5.1.Субектът на данните има право по всяко време на възражение срещу обработване на личните му данни и/или предоставянето им на трети лица без необходимото законово основание. Правото на възражение се упражнява чрез подаване на Заявление за възражение срещу обработване на лични данни – Образец, Приложение №5.

6.5.2.Администраторът разглежда подаденото заявление и прекратява обработването на личните данни, освен ако съществуват законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

6.5.3.Изброените по-горе заявления се регистрират от Отговорното лице, определено със заповед на Представляващия, в случаите, когато в Фондацията няма назначени служители, или от Представляващия в нарочен регистър – Приложение №6а на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** за съгласията и заявленията на субектите на личните данни.

6.5.4. Ръководството на Фондацията е длъжно да разгледа заявлението в 7-дневен срок от получаването му и да вземе решение. В 14-дневен срок, считано от датата на подаване на заявлението, Администраторът писмено уведомява заявителя дали са налице законовите основания за уважаване на искането. Ако Администраторът установи, че са налице законовите основания да уважи искането, той уведомява заявителя и за реда, по който може да упражни правото си или за отказа му да уважи искането поради липса на законови основания.

Сроковете за съхранение на всички заявления и декларации на хартиен носител са същите като сроковете за съхранение на самите данни и са посочени в Декларациите- уведомления за поверителност на личните данни на субектите, Приложение №1 и №2 към настоящата Политика, освен ако специален закон не изисква по-продължителен срок на съхранение на отделни документи.

6.6. Правото на жалба до Надзорен орган (КЗЛД)

6.1.Субектът на лични данни има право на жалба до КЗЛД във всички случаи, когато са нарушени правата му, в едногодишен срок от узнаване на нарушението, но не по-късно от 2 (две) години от извършването му.

VII.СИГУРНОСТ НА ДАННИТЕ

7.1. Всички служители / работници са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК**

176995161 държи, както и, че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** не е дал такива права на тази трета страна, като са сключили Споразумение или клауза за поверителност.

7.2. Всички лични данни са достъпни само за тези, които се нуждаят от тях, а достъпът може да бъде предоставен само в съответствие с настоящата Политика и изградените правила за контрол на достъпа на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**.

Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:

- в самостоятелна стая с контролиран достъп;
- данните в електронен вид са защитени с потребителско име и парола.

7.3. Компютърните екрани не могат да бъдат гледани от друг, освен от оторизираните служители / работници на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** и от Представляващия Фондацията. От всички служители / работници, когато има назначени такива, се изисква да бъдат обучени и да приемат съответните договорни клаузи/декларация за спазване на организационните и технически мерки за достъп, както и правилата за заключване на работните станции, преди да им бъде предоставен достъп до информация от всякакъв вид.

7.4. 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 по поддръжката на клиенти, те трябва да бъдат унищожени в съответствие със създадена за това с настоящата Политика процедура и съответен протокол.

7.5. Личните данни могат да бъдат изтривани или унищожавани в присъствие на най-малко двама служители, отговорни за обработката на личните данни, когато има назначени такива служители или от Представляващия, когато няма назначени такива. Записите на хартиен носител, които са достигнали датата на съхранение, трябва да бъдат нарязани и унищожени като "поверителни отпадъци". Данните върху твърдите дискове на излишните персонални компютри трябва да бъдат изтрити или дисковете унищожени, съгласно изградените с настоящата Политика правила/процедури. Във всички случаи на унищожаване на лични данни се съставя нарочен Протокол – Приложение №8.

7.6. Обработването на лични данни "извън офиса" представлява потенциално по-голям риск от загуба, кражба или нарушение на лични данни. Персоналът трябва да бъде специално упълномощен да обработва данните извън обекти на Администратора.

VIII. РАЗКРИВАНЕ НА ДАННИ

8.1. ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161 трябва да осигури 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.

Необходимо е на служителите да се извърши специално обучение и периодични инструктажи с цел да се избегне рискът от такова нарушение.

8.2. 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 Ръководството на Дружеството.

IX. СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ДАННИТЕ

9.1. ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161 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.

9.2. **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** 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.

9.3. Периода на съхранение за всяка категория на лични данни за персонала на Дружеството е:

- 10 години, считано от 01.01. на годината, следваща годината, през която е прекратен трудовия (граждански) договор – за данните в трудовите (гражданските) договори;
- за данните във ведомостите за заплати08 на работниците и служителите – 50 г., считано от 01.01. на годината, следваща годината, през която са съставени;
- за данните в автобиографии и други документи на кандидати за работа – до един месец след сключване на договор с избрания кандидат, освен ако лицето не е дало съгласие за по-дълъг период за участие в нов подбор;
- за данните в други счетоводни документи – 5 години, считано от 01.01. на годината, следваща годината, през която са съставени;
- за данни в копия от болнични листове - 3 години, считано от 01.01. на годината, следваща годината, през която са издадени;

Не се пазят копия от лични карти. Копията от болнични листове се съхраняват в заключващи се шкафове и помещения на Дружеството и след изтичане на 3 годишен период се унищожават като „поверителен“ отпадък или се връщат на лицата, за които се отнасят срещу подпис.

9.4. Периода на съхранение за всяка категория на лични данни на клиентите на Фондацията, е:

- за и при сключване на договор и документите по изпълнението му, както и данните в тези документи – 10 години, считано от 01.01. на годината, следваща годината, през която договора е прекратен;
- документи и лични данни, свързани с извършени дарения и данните – 20 години;
- за данни в други счетоводни документи по Договора – 3 години, считано от 01.01. на годината, следваща годината, през която документите са съставени;
- във всички останали случаи, личните данни се съхраняват до постигане на целите, за които се обработват.

9.5. Процедура за съхраняване и унищожаване на данните, както и правилата за унищожаване на информацията на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161,** разписани в настоящата Политика ще се прилагат във всички случаи.

9.6. Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност (чл. 5, пар. 1 б. от **ОРЗД**) – включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“);

X.ТРАНСФЕР НА ДАННИ

10.1. Всеки износ на данни от рамките на ЕС към страни извън ЕС (посочени в **ОРЗД** като "трети страни") са незаконни, освен ако няма подходящ "ниво на защита на основните права на субектите на данни. **Към настоящия момент ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161 не трансферира данни към страни извън ЕС.**

Прехвърлянето на лични данни извън ЕС е забранено, освен ако не се прилагат една или повече от указаните гаранции или изключения: Европейско икономическо пространство. (ЕИП – ЕС и Лихтенщайн, Норвегия и Исландия). Тези страни прилагат регламенти на ЕС чрез решение на Съвместния комитет, както и в случая с **ОРЗД**.

10.2. Решение за адекватност

Европейската комисия може да оцени трети страни, територия и/или специфични сектори в трети страни, за да прецени дали има подходящо ниво на защита на правата и свободите на физическите лица. Информация за тези страни се публикува тук:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

В тези случаи не се изисква разрешение.

10.3. Щит за личните данни в отношенията между ЕС и САЩ (EU-U.S. Privacy Shield)

Ако се налага за изпълнение на договор Администраторът да прехвърли лични данни от ЕС на трета страна в САЩ, то Отговорният служител трябва да провери дали организацията е подписала Рамковото споразумение „Privacy Shield“ с Министерство на търговията на САЩ.

Американското министерство на търговията отговаря за управлението и администрирането на Privacy Shield и гарантира, че компаниите изпълняват своите ангажименти. За да могат да се сертифицират пред министерството, фирмите трябва да имат политика за защита на личните данни в съответствие с принципите на **ОРЗД**, напр. използват, съхраняват и прехвърлят личните данни в съответствие набор от строги правила и предпазни мерки за защита на данните.

10.4. Задължителни фирмени правила

ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161може в последствие да приеме одобрени задължителни корпоративни правила за прехвърляне на данни извън ЕС. Това изисква подаването им за одобрение до съответния надзорен орган.

10.5. Стандартни договорни клаузи

ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161 може да приеме утвърдени стандартни договорни клаузи за защита на данните при прехвърляне на данни извън Европейското икономическо пространство. Ако **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** приема стандартни договорни клаузи, одобрени от съответния надзорен орган има автоматично признаване на адекватността.

10.6. Изключения

При липса на решение за адекватност, членство в US Privacy Shield, задължителни фирмени правила и / или договорни клаузи, прехвърляне на лични данни в трета страна или международна организация се извършва само при едно от следните условия:

- субектът на данните изрично се е съгласил с предложеното прехвърляне, след като е бил информиран за възможните рискове от такива прехвърляния;
- предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;
- 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.

XI. ПРОЦЕДУРА ПРИ ВЪЗНИКВАНЕ НА ИНЦИДЕНТИ

11.1.Подаване на сигнал за нарушение на сигурността на личните данни

Служителите на Фондацията и кандидатите за работа, клиентите, контрагентите и доставчиците подават **Сигнал за нарушение на сигурността на личните данни** в свободна форма, по един от следните начини:

- лично, в офиса на Администратора до Представляващия Фондацията;
- чрез лицензиран пощенски оператор.

Полученият **Сигнал за нарушение на сигурността на личните данни** се регистрира от определения служител в Регистъра – Приложение №6б към настоящата Политика, който незабавно информира Представляващия за получения сигнал.

След получаване на сигнала, Представляващият Фондацията определя дали конкретното събитие представлява „**нарушение на сигурността на лични данни**“. В зависимост от характера, обхвата и сериозността на нарушението, Представляващият Фондацията определя засегнатите области, кои данни са засегнати, както и риска за засегнатите физически лица, предприема съответните мерки за справяне с нарушението на сигурността на личните данни, включително и по целесъобразност извършва необходимите действия за отстраняване на неблагоприятните му последици. В случай на **„нарушение на сигурността на личните данни“** и когато съществува вероятност да се породи риск за правата и свободите на физическите лица, Администраторът, без ненужно забавяне и когато това е осъществимо (не по-късно от **72 часа** след като е разбрал за него), изпраща **Уведомление относно**

нарушение на сигурността на личните данни - Приложение №7а към настоящата Политика до контролния орган и до субекта на данните.

Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

11.2.Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с нарушението. За инцидентите във Фондацията, се води Регистър - Приложение №7б за регистриране на нарушения на сигурността на личните данни, в който задължително се вписват:

- предполагаемото време или период на възникване;
- времето на установяване на установяване на инцидента;
- името и длъжността на лицето, установило наличието на инцидента и подало сигнал;
- описание на нарушението – източник, вид и мащаб на засегнатите данни, причина за нарушението (ако е приложимо);
- описание на извършените уведомявания: уведомяване на КЗЛД и засегнатите лица (ако е било извършено);
- предприети мерки за ограничаване на възможността от последващи нарушения на сигурността.
- Ръководството на Фондацията извършва подробна оценка на степента на засягане и увреждане на носителите на лични данни и на електронния масив лични данни. Предприема подходящи мероприятия за възстановяване базата данни с лични данни при тяхното пълно унищожаване/изгубване. При анализа са отделят особено внимание на причините, довели до повреждането/загубата на личните данни и се вземат мерки за предприемане на подходящи мерки за бъдещо предотвратяване на последващи инциденти.

XII. ПРОЦЕДУРА ЗА ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ

12.1.Оценка на въздействието се извършва, само когато това се изисква съгласно приложимото законодателство и с оглед на риска за физическите лица и естеството на обработка на лични данни, извършвана от Фондацията. Оценка на въздействието се извършва за високорискови дейности по обработване.

12.2.Оценка на въздействието е необходимо при всяко въвеждане на ключова система, която е свързана с обработване на лични данни, включително:

- Първоначалното въвеждане на нови технологии или прехода към нови технологии;
- Автоматизирано обработване, включително профилиране или автоматизиране вземане на решения;
- Обработване на чувствителни лични данни в голям мащаб;
- Мащабно, систематично наблюдение на публично обществена зона;
- За оценката се съставя доклад, който се предоставя при поискване от страна на КЗЛД.

12.3. Към 08 август 2023 г. **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** не обработва данни по начин, който налага оценка на въздействието.

XIII. ПРОЦЕДУРА ПО ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

13.1.При необходимост, Фондацията може да предоставя лични данни на трети лица, действащи в качеството на Обработващи по Споразумение за обработка на лични данни, чието съдържание ще се определя от вида и целта на обработване на личните данни на субектите. В случаите на предоставяне на данните на служители, клиенти или доставчици на услуги на друг Обработващ, Дружеството:

- изисква достатъчно гаранции от Обработващия за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;
- сключва писмен договор, който урежда задълженията на обработващия и отговаря на изискванията на чл. 28 от **ОРЗД**;
- информира физическите лица, чиито данни ще бъдат предоставени на обработващ.
- Обработване на лични данни от обработващи извън ЕС/ЕИЗ е допустимо само когато:
- Европейската Комисия е приела решение, потвърждаващо, че страната, към която се извършва трансфера, осигурява адекватно ниво на защита на правата и свободите на субектите на данни;
- Налице са подходящи мерки за защита – като например Обвързващи Корпоративни Правила (ОКП), стандартни договорни клаузи, одобрени от Европейската Комисия, одобрен кодекс за поведение или сертификационен механизъм;
- Субектът на данни е дал своето изрично съгласие за трансфера, след като е информиран за възможните рискове, или
- Трансферът е необходим за една от целите, изброени в **ОРЗД**, включително изпълнението на договор със субекта, защита на обществения интерес, установяване и защита на правни спорове, защита на жизненоважните интереси на субекта на данни в случаите, когато той е физически или юридически неспособен да даде съгласие.

XIV. ЗАЩИТА НА ЛИЧНИТЕ ДАННИ. ОСНОВНИ ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

14.1. Видове защита

- **Физическа защита -** система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.
- **Персонална защита -** система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на Администратора.

- **Документална защита -** система от организационни мерки при обработването на лични данни на хартиен носител. **Защита на автоматизирани информационни системи и мрежи -** система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.

- **Криптографска защита –** система от технически и организационни мерки, които се прилагат с цел защита на личните данни от нерегламентиран достъп при предаване, разпространяване или предоставяне.

- За защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение, както и от други незаконни форми на обработване, Администраторът организира и предприема мерки, съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

14.2. Основни технически и организационни мерки на отделните видове защита на личните данни в регистрите по т. XIV са.:

14.2.1.Мерки за физическата защита – определяне на помещенията, в които ще се обработват лични данни - заключващи се помещения със секретни ключалки;

- определяне на помещенията, в които има монтирани програмно-технически и комуникационни средства, съхраняващи и обработващи лични данни;
- определяне на зони с контролиран достъп;
- определяне на характеристиките на физическата среда и зоните с контролиран достъп;
- разполагане на техниката – на работно бюро;
- заключване на картотечните шкафове, в които се съхраняват данните на хартиен носител;
- определяне на организацията на физическия достъп – физически достъп до личните данни имат само лицата, обработващи лични данни, а при спазване на съответните законови правила и трети лица.

14.2.2.Мерки за персонална защита

- познаване на нормативната уредба в областта на защитата на личните данни;
- знания за опасностите за личните данни, обработвани от Администратора;
- поемане на задължение за неразпространение на личните данни чрез подписване на Декларация за неразгласяване на лични данни – Образец, Приложение №4;
- познаване на Политиката за поверителност и защита на личните данни;
- спазване на политика на чисто бюро и чист екран спазване на Политика на чисто бюро и чист екран – това означава на работното бюро и на екрана да са достъпни само данните, които се обработват в момента от служителя и само до момента на приключване на тяхната обработка. След приключване на обработката данните да се съхранят по предвидения в настоящата Политика начин – данните на хартиен носител в заключващи се помещения и шкафове, а данните в електронен формат чрез затваряне на екраните с достъп до тях и съответна парола и на компютър на дружеството. Данните се пазят и в електронната пощенска кутия на Дружеството, като се изтриват след изтичане на 3659 – дневен срок;
- несподеляне на критична информация между персонала (напр. идентификатори, пароли за достъп и др.);
- обучение на служителите, обработващи лични данни;

- обучение на персонала за реакция при събития, застрашаващи сигурността на личните данни.
- Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае".

14.2.3.Мерки за документална защита

- Регистрите за личните данни, се поддържат в електронен и писмен вид, съгласно съответните инструкции за воденето им – неразделна част от настоящата Политика.
- Сроковете за съхранение и редът за унищожаване на личните, се определят, както е посочено в т.**9.3** и **9.4** по-горе.

14.2.4.Мерки за защита на автоматизираните информационни системи и/или мрежи

14.2.4.1.Основните мерки за защита на автоматизираните информационни системи и/или мрежи на Администратора са: стандартни защити с достъп с потребителско име и пароли и антивирусни софтуери.

14.2.4.2.В дейността на Администратора са предвидени необходимите технически и организационни мерки за защита на личните данни от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

Мерки за криптографска защита

Предприетите мерки за криптографска защита включват:

- криптографски възможности на операционните системи;
- криптографски възможности на системите за управление на бази данни;
- криптографски възможности на комуникационното оборудване.

  Администраторът не предвижда към настоящия момент предприемане на мерки за криптографска защита.

XV. ДЕЙНОСТИ ПО ОБРАБОТВАНЕ СЪГЛАСНО ЧЛ.30 от ОРЗД

15.1.Дейностите по обработване на лични данни са посочени за всеки един от поддържаните от Администратора регистри. Дружеството документира дейностите по обработване на лични данни при спазване на принципа на отчетност и принципите за законосъобразно обработване на личните данни.

15.2.Във Фондацията се обработват лични данни в следните регистри:

- **"ПЕРСОНАЛ"**
- **"КЛИЕНТИ"**

15.3. Регистър „ПЕРСОНАЛ"

15.3.1. Общо описание на поддържания регистър

15.3.1.1. Регистър „Персонал" се поддържа на основание Кодекс на труда (КТ), Кодекс за социално осигуряване (КСО), Закон за здравословни и безопасни условия на труд (ЗЗБУТ), Закон за здравното осигуряване (ЗЗО) и подзаконовите актове по тяхното прилагане.

15.3.1.2. Личните данни по този регистър се събират и обработват за следните цели: управление на човешките ресурси (вкл. подбор на персонал, промяна в договорните условия по трудовите

правоотношения, командироване на служителите в страната и чужбина, издаване на визи, издаване на застраховки при пътуване, закупуване на самолетни билети, издаване на разрешения за достъп до стратегически зони и стратегически обекти), изплащане на трудовите възнаграждения на служителите, удържане и внасяне на данъчни, здравни и осигурителни вноски, спазване договореностите в КТД.

15.3.2.Категориите лични данни, обработвани в регистъра са:

- **от тип физическа идентичност:** имена, ЕГН/ЛНЧ, данни от документи за самоличност – номер и дата на издаване на личната карта, адрес – постоянен и по местоживеене, месторождение, дата на раждане, телефонен номер, имейл адрес, пол, снимка;
- **от тип социална идентичност:** вид на образованието, допълнителна квалификация, степени, звания, място, номер и дата на издаване на дипломата, предишен опит, данни относно трудова дисциплина, удостоверения за курсове и квалификации, номер, дата на издаване и категория на шофьорска книжка, други лични данни, предоставени от съответното лице в автобиография при кандидатстване за работа или в процеса по подбор;
- **от тип семейна идентичност:** данни относно семейното положение на физическото лице (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години), данни на съпруг/а и други близки, родствени връзки;
- **от тип физиологична идентичност:** общ здравен статус (данните се съдържат в медицинска документация от личен лекар, ЛКК, ТЕЛК, НЕЛК, лечебни заведения);
- **други:** информация за присъди и нарушения, ако нормативен акт предвижда това; информация за имотно състояние; информация за банкова сметка, заплата и социални придобивки; информация за образувани или висящи досъдебни производства и производства пред ЧСИ.

15.3.3. Технологично описание на регистъра

15.3.3.1.Администраторът събира и обработва лични данни на хартиен носител и автоматизирано (защитен софтуер, достъпен посредством потребителско име, парола и/или електронен ключ) и неавтоматизирано (хартиен носител). Личните данни се поддържат във вида и формата, които позволяват идентифициране самоличността на физическите лица.

15.3.3.2.Данните на всеки работник и служител на Фондацията, както и на кандидатите за работа, се събират, обработват и съхраняват на хартиен и технически носител от служители, определени с нарочна заповед на Представляващия. Хартиените носители на личните данни на работниците и служителите се съхраняват в трудови досиета, които се подреждат в специални заключващи се шкафове в работните заключващи се помещения на лицата, оправомощени да обработват личните данни. Някои данни могат да се съхраняват или обработват и на технически носител. Данните от проведени конкурси и интервюта се съхраняват на технически и/или хартиен носител, в специални шкафове със заключване в кабинета на лицето отговорно за личните данни.

15.3.3.3.Досиета на работниците и служителите, както и данните на кандидатите за работа не се изнасят извън административния офис на Фондацията.

15.3.4. Оценка на въздействието и съответно ниво на защита.

Предвид сравнително малкия брой субекти, както и размера на вредите, които биха могли да бъдат причинени на субектите, чийто данни се обработват, оценката на риска за сигурността на тези данни е ниска.

15.4. Регистър „Клиенти“

15.4.1. Общо описание на поддържания регистър

Регистър „**КЛИЕНТИ**“ се поддържа на основание на Закона за задължения и договорите, Търговския закон, Данъчно процесуалния кодекс, Закона за данък върху добавената стойност, Закона за счетоводството и подзаконовите актове по тяхното прилагане. Обработват се лични данни на клиенти, контрагенти и доставчици, посетители на сайта.

15.4.2.Категориите лични данни, обработвани в регистъра са:

Категория лични данни за:

15.4.2.1.За сключване и изпълнение на договор:

- **от тип физическа идентичност**:
  - имена, ЕГН/ЛНЧ, данни от документи за самоличност, адрес, месторабота;
  - телефон, e-mail адрес, подпис на лицето

15.4.2.2.За сключване на договор за дарение - имена, ЕГН/ЛНЧ, данни от документи за самоличност, адрес на дарителя и размера и вида на направеното дарение;

15.4.2.4.Други - информация за банкова сметка при плащания по банков път;

15.4.2.5.Данни за посетителите на сайта електронна поща и име.

15.4.3. Технологично описание на регистъра

Администраторът събира и обработва личните данни автоматизирано (защитен електронен регистър, достъпен посредством потребителско име, парола и/или електронен ключ) и неавтоматизирано (хартиен носител). Личните данни се поддържат във вида и формата, които позволяват идентифициране самоличността на физическите лица.

Данните в регистъра на хартиен и технически носител се събират, обработват и съхраняват от лица, определени с нарочна заповед на Представляващия Фондацията или от самия Представляващ, в периодите, когато във Фондацията няма назначени служители. Хартиените носители на личните данни на физическите лица по този регистър се съхраняват в класьори, които се подреждат в специални шкафове със заключване, в работните помещения на лицата, оправомощени да обработват личните данни. Някои данни могат да се съхраняват или обработват и на технически носител.

15.4.4. Оценка на въздействието и определяне на ниво на защита

Предвид сравнително малкия брой субекти, както и размера на вредите, които биха могли да бъдат причинени на субектите, чийто данни се обработват, оценката на риска за сигурността на тези данни е ниска.

11.5.4. Технически и организационни мерки за защита

Видовете защита на личните данни в регистър „Клиенти“ са физическа, персонална, документална и защита на автоматизирани информационни системи и/или мрежи. Специална криптографска защита не се прилага.

15.6.Инвентаризация на данните

ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161е създала 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 **ОРЗД**. При инвентаризацията на данните в **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** и 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.

ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161е наясно с рисковете, свързани с обработването на определени видове лични данни.

ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161 оценява нивото на риска за лицата, свързани с обработването на личните им данни. Когато е необходимо, се извършват оценки на въздействието върху защитата на данните във връзка с обработването на лични данни от **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** и във връзка с обработването, предприето от други организации от името на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161**.

ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161управлява всички рискове, идентифицирани от оценката на въздействието, когато такава е направена, 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 **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** 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.

Настоящата Политика и приложенията към нея са утвърдени със заповед на Представляващия – Приложение №9 на **ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161** от 10 юни 2018г

ПРИЛОЖЕНИЯ:

1. Декларацията – Уведомление за поверителност на личните данни на физически лица - клиенти, контрагенти и доставчици;

2. Декларацията – Уведомление за поверителност на личните данни на работници и служители на Фондацията, включително и лица по граждански договор, предоставящи услуги на Администратора;

3а. Протокол за обучение и инструктаж;

3б. Декларация за неразгласяване на лични данни

4а. Декларация за предоставяне на лични данни;

4б. Декларация - съгласие за обработка на лични данни;

5. Заявление на субекта на лични данни за достъп до лични данни; за изтриване/коригиране на лични данни; за упражняване правото на блокиране (ограничаване на обработването); за възражение срещу обработване на лични данни;

6а. Регистър на съгласията и на заявленията съгласно политика за поверителност и защита на личните данни на ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161;

6б. Регистър на нарушенията на сигурността на личните данни на ФОНДАЦИЯ "ВЪТРЕШЕН КОМПАС", ЕИК 176995161;

7а. Уведомление относно нарушение на сигурността на личните данни до надзорния орган;

7б. Уведомление относно нарушение на сигурността на личните данни до субекта на лични данни;

8. Протокол за унищожаване на данни и информация;

9. Заповед на Представляващия Фондацията за въвеждане на Политика за защита на личните данни и определяне на Отговорни лица и лица, имащи задължение за обработване на личните данни.