ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

В "ИЗПИТАЙ МЕ" ООД

Дата на последна актуализация: 25.05.2023г.

Настоящата политика се издава на основание Регламент (ЕС) 2016/679 и има за цел да документира какви лични данни се събират и обработват от "ИЗПИТАЙ МЕ" ООД и какви мерки се прилагат за тяхното опазване и правилно съхранение.

I. ОБЩИ ПОЛОЖЕНИЯ

Обхват на документа

Чл. 1. (1) Настоящите правила се прилагат за лични данни по смисъла на Регламент (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година, и регламентира:

1. Механизмите за водене, поддържане и защита на регистрите, съхраняващи лични данни в "ИЗПИТАЙ МЕ" ООД с цел гарантиране на неприкосновеността на личността и личния живот, чрез осигуряване на защита на данните за физическите лица.

2. Видовете регистри, които се водят в дружеството и тяхното общо и технологично описание.

3. Определя вида на личните данни, целите и средствата за обработването им в "ИЗПИТАЙ МЕ" ООД.

4. Необходимите технически и организационни мерки за защита на личните данни, съдържащи се в регистрите от неправомерно обработване (случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни).

5. Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.

6. Предоставяне на лични данни на трети лица - основание, цел, категории лични данни;

7. Срокове за съхранение на личните данни и реда за тяхното унищожаване след изтичането на сроковете.

8. Процедури за докладване, управление и реагиране при инциденти.

9. Процедури за уведомяване на КЗЛД за настъпили инциденти;

10. Правата на субектите на данни и процедурата за отговаряне на запитвания и уведомяване на субектите на данните;

11. Организацията и реда за упражняване на контрол при обработването на лични данни;

(2) "ИЗПИТАЙ МЕ" ООД се придържа изключително към законовата рамка (Регламент (ЕС) 2016/679, ЗЗЛД, Конвенция 108 за защита на лицата при автоматизирана обработка на лични данни.

Администратор на лични данни

Чл. 2. "ИЗПИТАЙ МЕ" ООД е администратор на лични данни.

Обработващ лични данни

Чл.3 (1) В своята дейност "ИЗПИТАЙ МЕ" ООД има право да влиза в различни договорни и други отношения с контрагенти (физически и юридически лица, държавни и неправителствени организации), на които има право да възлага, при спазване условията на приложимото законодателство, обработване на лични данни.

(2) Администраторът използва само обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на действащото законодателство и да осигурява защита на правата на субектите на данни. Отношенията между администратора и обработващия лични данни се уреждат с писмен договор, който задължително съдържа предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни и задълженията и правата на администратора.

(3) Обработващият лични данни:

1. Обработва личните данни само по документирано нареждане на администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това, като в този случай обработващият лични данни информира администратора преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес;

2. Гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;

3. Взема всички необходими мерки за гарантиране сигурност на обработването;

4. Спазва установените правила за включване на друг обработващ лични данни;

5. Като взема предвид естеството на обработването, подпомага администратора, доколкото е възможно, чрез подходящи технически и организационни мерки при изпълнението на задължението на администратора да отговори на искания за упражняване на предвидените права на субектите на данни;

6. Подпомага администратора да гарантира изпълнението на задълженията му за гарантиране сигурност на обработването, уведомяване на КЗЛД или съответния надзорен орган и субекта на данни за нарушение на сигурността и извършване оценка на въздействието върху защитата на данните, когато това се изисква нормативно.

7. Заличава всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако нормативен акт не изисква тяхното съхранение;

8. Осигурява достъп на администратора до цялата информация, необходима за доказване на изпълнението на задълженията, определени в настоящия член, и позволява и допринася за извършването на одити, включително проверки, от страна на администратора или друг одитор, оправомощен от администратора.

9. Незабавно уведомява администратора, ако според него дадено нареждане нарушава нормативната уредба относно защитата на данните.

(3) Обработващи лични данни, които въз основа на договор с "ИЗПИТАЙ МЕ" ООД обработват лични данни от името на "ИЗПИТАЙ МЕ" ООД или имат пряк/косвен достъп до лични данни биха могли да бъдат:

1. Транспортни/куриерски фирми с оглед изпълнение на договорните ни задължения по доставяне на договори на хартиен носител и /или закупени/ ремонтирани стоки;

2. Лица, които по възлагане поддържат оборудване и софтуер, използвани за обработване на личните Ви данни;

3. Лица, предоставящи услуги по сервизна поддръжка на крайни устройства;

4. Агенции, събиращи неплатени клиентски задължения от името на "ИЗПИТАЙ МЕ" ООД.

5. Лица, осъществяващи дейности по инсталация и/или поддръжка и др. - подизпълнители по съответния договор;

6. Банките, обслужващи плащания по договор;

7. Охранителни фирми, притежаващи лиценз за извършване на частна охранителна дейност, обработващи видеозаписи и/или поддържащи други регистри в процеса на осигуряване на пропускателния режим в обектите на дружеството;

8. Лица, предоставящи услуги по организиране, съхраняване, индексиране и унищожаване на архиви на хартиен и/или електронен носител;

9. Лица, извършващи консултантски услуги в различни сфери - право, счетоводство и пр.

10. Подизпълнители, на които е възложено извършването на определени услуги а клиенти на дружеството;

(4) Други администратори на лични данни, на които "ИЗПИТАЙ МЕ" ООД предоставя лични данни, обработващи данните на собствено основание и от свое име са цесионери – страна по договори за цесия, на които администраторът може да прехвърля (продава) свои вземания;

Лични данни

Чл. 4 Лични данни означава 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.

Регистри на лични данни

Чл.5 Лични данни се обработват в регистри при спазване на Регламент (ЕС) 2016/679.

Принципи при обработка

Чл.6 Личните данни в "ИЗПИТАЙ МЕ" ООД:

1. Се обработват законосъобразно, добросъвестно и по прозрачен начин;

2. Се събират за конкретни, точно определени и законни цели и да не се обработват допълнително по начин, несъвместим с тези цели

3. Следва да бъдат съотносими, свързани със и ненадхвърлящи целите, за които се обработват;

4. Да бъдат точни и при необходимост да се актуализират;

5. Се заличават или коригират, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

6. Се поддържат във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.

7. Се обработват по начин, който гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване, случайна загуба, унищожаване или повреждане.

Обработване на лични данни

Чл. 7. Обработване на личните данни е всяко действие или съвкупност от действия, които могат да се извършат по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване или предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване на данните.

Обработване под ръководството на администратора на лични данни

Чл.8 (1) Администраторът възлага обработването на личните данни вътре в дружеството на негови служители. Обработване на личните данни се извършва само от лица, чиито служебни задължения или конкретно възложена задача налагат достъп до лични данни и предварително са определени като натоварени да обработват лични данни, по подходящ за това начин (длъжностна характеристика, конкретна заповед на управителя и др.).

(2) Преди започването на дейности по обработка на данни, тези лица са длъжни да се запознаят с настоящия документ, Регламент (ЕС) 2016/679, ЗЗЛД и нормативната уредба по прилагането му и да я спазват при извършване на дейностите по обработка под страх от дисциплинарно наказание.

(3) Служителите, обработващи лични данни, действат само по указание на администратора, освен ако в закон не е предвидено друго.

(4) Личните данни не се разкриват на неоторизирани лица в процеса на тяхното обработване. Служителите натоварени да обработват лични данни подписват **Декларация за конфиденциалност Образец № 2** по отношение обработваните от тях данни.

(5) Данните да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване и няма възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.

(6) Осигурява се непрекъсната възможност за обработване на личните данни на оторизираните лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване.

(7) Служителите, обработващи данни са длъжни:

1. Да обработват лични данни законосъобразно и добросъвестно;

2. 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;

3. Да актуализират своевременно регистрите на личните данни (при необходимост);

4. Да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;

5. Да поддържат личните данни във вид, позволяващ изпълнение на целите за които се обработват и за период не по-дълъг от необходимия за същите тези цели;

Законосъобразност на обработването

Чл.9 Обработването на лични данни е допустимо само в случаите, когато е налице поне едно от следните условия:

1. Обработването е необходимо за изпълнение на нормативно установено задължение на администратора на лични данни;

2. Физическото лице, за което се отнасят данните е дало изрично своето съгласие;

3. Обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия, предхождащи сключването на договор и предприети по негово искане;

4. Обработването е необходимо, за да се защитят животът и здравето на физическото лице, за което се отнасят данните;

5. Обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес;

6. Обработването е необходимо за упражняване на правомощия, предоставени със закон на администратора или на трето лице, на което се разкриват данните;

7. Обработването е необходимо за реализиране на законните интереси на администратора на лични данни или на трето лице, на което се разкриват данните, освен когато пред тези интереси преимущество имат интересите на физическото лице, за което се отнасят данните.

Данни забранени за обработване в "ИЗПИТАЙ МЕ" ООД

Чл. 10 (1) В "ИЗПИТАЙ МЕ" ООД е забранено обработването на лични данни, които:

1. Разкриват расов или етнически произход;

2. Разкриват политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели;

3. Се отнасят до сексуалния живот или до човешкия геном.

(2) Алинея 1 не се прилага, когато:

1. Обработването е необходимо за целите на изпълнението на специфични права и задължения на администратора или субектите на данните в областта на трудовото и социално осигурително законодателство;

2. Физическото лице, за което се отнасят тези данни, е дало изрично своето съгласие;

3. Обработването е необходимо за защита на живота и здравето на физическото лице, за което тези данни се отнасят, или на друго лице и състоянието на физическото лице не му позволява да даде съгласие или съществуват законни пречки за това.

Видове регистри

Чл. 11. (1) Личните данни в "ИЗПИТАЙ МЕ" ООД се събират, обработват и съхраняват в 3 регистъра:

1. Регистър „Персонал“

2. Регистър „Контрагенти (клиенти и доставчици)"

3. Регистър "Потребители на izpitai.me"

(2) На основание чл.30, параграф 5 от Регламент (ЕС) 2016/679, "ИЗПИТАЙ МЕ" ООД не поддържа регистрите в табличен или писмен вид.

Защита на данните на етапа на проектирането и по подразбиране

Чл. 12. Администраторът извършва оценка на данните, поддържани в регистрите и рисковете от обработване при приемане на настоящия документ, при всяко изменение на вида данни или регистри и/или цели за обработване и/или дейности по обработване или поне веднъж на две години. На база тази оценка, администраторът, спазвайки принципа за защита на данните на етапа на проектирането и по подразбиране въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки за защита на данните.

Оценка на въздействието на дейностите по обработване

Чл. 13. (1) На основание направен анализ на вида обработвани данни, поддържани регистри и дейности по обработване за администратора на "ИЗПИТАЙ МЕ" ООД няма правно задължение да извършва Оценката на въздействието върху защита на данните по смисъла на чл.35 и 36 от Регламент (ЕС) 2016/679.

(2) "ИЗПИТАЙ МЕ" ООД извършва оценка на въздействието за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

Чл. 14 (1) Оценка на въздействието се извършва за всички поддържани регистри, като всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност. Най-високото ниво на въздействие, определено по всеки от критериите определя нивото на въздействие на съответния регистър.

(2) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни, дейностите по обработване или броя на засегнатите физически лица.

(3) Оценката на въздействието в "ИЗПИТАЙ МЕ" ООД се извършва от Управителя и технически специалист веднъж годишно.

(4) Нивата на въздействие и защита за всеки регистър се утвърждават от Управителя.

Нива на въздействие

Чл. 15. Нивата на въздействие са както следва:

1. „Изключително високо" - в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица;

2. „Високо" - в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;

3. „Средно" - в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;

4. „Ниско" - в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Чл. 16. (1) В зависимост от нивото на въздействие се определя и съответно ниво на защита или по-високо на данните в различните регистри в "ИЗПИТАЙ МЕ" ООД.

(2) Нивото на защита представлява съвкупност от технически и организационни мерки за физическа, персонална, документална защита и защита на автоматизираните информационни системи и/или мрежи, както и криптографска защита на личните данни.

Чл. 17. (1) Нивата на защита са, както следва:

1. при ниско ниво на въздействие - ниско ниво на защита;
2. при средно ниво на въздействие - средно ниво на защита;
3. при високо ниво на въздействие - високо ниво на защита;
4. при изключително високо ниво на въздействие - изключително високо ниво на защита.

Чл. 18. Видовете защита на личните данни са физическа, персонална, документална, защита на автоматизирани информационни системи и/или мрежи и криптографска защита.

II. РЕГИСТЪР „ ПЕРСОНАЛ“

Цели на обработка

Чл. 19. (1) Регистър „Персонал“ обхваща лични данни на кандидати за работа, служители и работници в "ИЗПИТАЙ МЕ" ООД, назначени по трудово правоотношение, както и изпълнителите по граждански договори в "ИЗПИТАЙ МЕ" ООД по време на дейността им по изпълнение на тези договори

(2) Данните се обработват с цел изпълнение на съответните трудови функции и задължения на администратора в качеството му на работодател и осигурител и са предназначени за:

1. Индивидуализиране на трудовите и граждански правоотношения, тяхното съществуване, изменение и прекратяване, документиране на произтичащите от трудовите и приравнени на тях правоотношения права и задължения на страните.

2. Изпълнение на нормативните изисквания по Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството, Закона за държавния архив, ЗОДФЛ, ЗЗД и др подобни, свързани с изпълнението на трудовите и приравнените на тях правоотношения.

3. Управление на човешките ресурси и повишаване квалификацията на персонала, за водене на финансово - счетоводна дейност и отчетност, пенсионна, здравна и социално-осигурителна дейност.

4. Осъществяване на търговски операции - търговски дейности като управление на пътувания и разходи, управление на активите на дружеството, осигуряване на ИТ услуги, информационна сигурност, провеждане на вътрешни одити и разследвания, изпълнение на задълженията по търговски договори, правно или търговско консултиране и подготовка за правни спорове и др.

Чл.20 Регистър „Персонал“ може да набира и съхранява временно лични данни на кандидати за работа през интернет сайта на фирмата или през публично достъпни онлайн платформи, с които дружеството е в договорни отношения. Данните по тази разпоредба се събират само при условия, че лицата са ги предоставили доброволно и предварително са били информирани за целите и срока на обработването.

Категории данни

Чл. 21 (1) В регистър „Персонал“ се съдържат следните групи данни:

1. Физическа идентичност – име, ЕГН, постоянен и настоящ адрес, телефон, паспортни данни; месторождение;

2. Социална идентичност:

а) Образование – документ за придобито образование, за квалификация и правоспособност, степени и звания и други подобни, за преминати при работодателя обучения и пр;

б)Трудова дейност – съгласно приложена автобиография, документи за трудов стаж и трудово възнаграждение и други подобни;

в) Социално положение - данни относно семейното положение на лицето (наличие на брак, развод, брой членове на семейството, в това число деца до 18 години - данните са необходими при установяване правата на лицата за получаване на семейни добавки и платен отпуск за деца до 18 години, за начисляване на удръжки от трудовото възнаграждение и пр.).

3. Лични данни относно наказателно правния статус на лицата - свидетелство за съдимост;

4. Финансови данни - банкова сметка за заплащане на вземания от труд;

5. Данни, свързани със здравния статус на служителите, във връзка с допълнителното здравно осигуряване на лицата на трудов договор- здравни декларации.

Служители натоварени с обработка на данните от администратора

Чл. 22 (1) Данните се обработват на принципа „Необходимост да знае" от следните лица, на които изрично е възложено обработване на лични данни от администратора:

1. Служители от отдел "Счетоводство" - Финансов директор и счетоводител;

2. Специалист "Човешки ресурси";

3. Служител, на който е възложено от Управителя да координира допълнителното здравно осигуряване на служителите на трудов договор.

(2) За необходимостта от набиране на лични данни и целите, за които ще бъдат използвани, лицата по чл.21, ал.1 информират лицето и при необходимост взимат неговото съгласие. Данните, за които се изисква съгласие на лицето, се обработват само след като съгласието е писмено документирано, посредством **декларация Образец №1 и 1а** към настоящия документ.

Обработващи данни

Чл.23 (1) Администраторът има право да възлага обработването на лични данни от регистър "Персонал" на обработващи данни, които могат да бъдат консултантски дружества, предоставящи услуги в сферата на трудовото, данъчното, счетоводното и осигурително законодателство, правни услуги, услуги по трудова медицина и др.

(2) Всяко възлагане на обработване по реда на тази разпоредба се извършва при стриктно спазване на разпоредбите на чл.3 във вр. с чл.28 от Регламент (ЕС) 2016/679 и подписания между страните договор.

Събиране и обработване на данните

Чл. 24 (1) Личните данни в регистър "Персонал" се набират директно от физическите лица, за които се отнасят при кандидатстване и при постъпване/ възлагане на работа по трудово или гражданско правоотношение на дадено лице и в последствие до прекратяване на трудовото правоотношение.

(2) Данните се предоставят от лицата при кандидатстване, постъпване на работа, както и при всяка промяна в данните, за което те са длъжни да уведомят администратора. Данните се предоставят след а) изрично съгласие, б) във връзка с изпълнение на трудовия или граждански договор или в) в изпълнение на нормативно задължение по един от следните начини:

1. Устно - при интервю с лицето (при постъпване или в процеса на работа);

2. На хартиен носител – писмени документи – изпратени CV-та за кандидатстване за работа в структурата; молби, заявления за постъпване/извършване на работа по трудово или гражданско правоотношение; за изменение или прекратяване на тези отношения, болнични листове; по текущи въпроси в процеса на работа, подадени от лицето; здравни декларации;

3. На електронен носител – с кандидатурата си през електронен сайт или онлайн платформа, ако кандидатът ги е посочил доброволно.

(3) Събраните данни се обработват и съхраняват на хартиен и електронен носител.

Чл.25 (1) Лични данни снети от хартиен носител се обработват в електронен вариант за целите на водене на служебното трудово досие и за изготвяне на разплащателни документи, свързани с трудовото и осигурително правоотношение, в съответствие с действащото законодателство и за изпълнение на други дейности, свързани с посочените в настоящия документ цели.

(3) Документи, съдържащи лични данни на хартиен носител могат да бъдат размножавани, от упълномощените служители само ако е необходимо за изпълнение на служебните им задължения, свързани с обработване на данните, за предоставянето им на обработващи данни, с които дружеството има договор или ако са изискани по надлежния ред от упълномощени лица при стриктно спазване на нормативната уредба и този документ.

Правила при неавтоматизирано обработване на данни (на хартиен носител)

Чл. 26 (1) Лични данни на хартиен носител от регистър "Персонал" се съхраняват в отделна папка за всеки служител, работник или нает по граждански договор лице - кадрови досиета. Те се съхраняват съгласно изисквания от закона срок в помещение с контролиран достъп.

(2) Данни на хартиен носител относно финансово - счетоводните отношения на администратора и субектите на данни се съхраняват в отдел Счетоводство (ведомости за заплати и др. подобни) при същите условия, като тези приложими за кадровите досиета.

Правила при автоматизирано обработване на данни

Чл. 27. Въведени са високо технологични, технически и административни мерки за опазване на личните данни, които "Изпитай ме" обработва в дигитален формат. Тези мерки имат за цел да не позволим изтичането и неправомерното използване на тези данни, както да гарантират правилното им използване съгласно целите за които са събрани и периода за който следва да се съхраняват. Достъпът до личните данни в дигитален формат е ограничен до хората, оправомощени да ги обработват

Категории лица, на които се предоставят данните

Чл.28 Личните данни от регистър "Персонал" се предоставят на следните категории трети лица:

1. Органи на държавна, местна власт или съдебни органи, на които законът е възложил контролни функции, след получаване на съответното законно искане за това;
2. На обработващи данни, при спазване правилата за това;
3. На други лица - само след взето изрично писмено съгласие на субекта на данни;

Срок за съхранение на данните

Чл. 29 (1) Всички данни в регистър „Персонал" се съхраняват както следва:

1. ведомости за заплати, трудови договори, (заповеди за назначаване), заповеди за преназначаване, заповеди за ползван неплатен отпуск над 30 работни дни годишно, заповеди за освобождаване от работа, трудови книжки, издадени удостоверения обр. УП-1, обр. УП-2, обр. УП-3 и обр. 30.и др. документи, въз основа, на които може да се установи осигурителен стаж и доход, категория труд на лицата и др. 50 г., считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят;
2. лични данни на кандидати за работа - за времето на провеждане на подбора, но за не повече от 6 месеца, освен в случаите в които лицето изрично е дало съгласие данните (**декларация Образец №** 1а) му да се обработват и с оглед бъдещи подбори на персонал. В този случай данните се съхраняват за не повече от 3 години.
3. всички други данни - 3г., считано от датата на прекратяване на трудовото правоотношение, но не по-малко от съответния давностен срок, предвиден в законодателството за установяване, изменение или заплащане на суми за възнаграждения, обезщетения или осигурителни плащания;

Ниво на защита

Чл. 30 (1) Оценката на въздействието върху личните данни в регистър "Персонал"се определя на *ниско ниво* на въздействие. При оценката са отчетени характера на обработваните

лични данни, както и обстоятелството, че неправомерното обработване на лични данни би могло да застраши неприкосновеността на личността и личния живот, на отделно физическо лице или група физически лица.

III. РЕГИСТЪР „ КОНТРАГЕНТИ“

Цели на обработка

Чл. 31 (1) Регистър „Контрагенти (клиенти и доставчици)“ набира и съхранява лични данни на контрагенти - клиенти, партньори, доставчици, подизпълнители и пр., или данни предоставени от контрагенти с цел:

1. Идентифициране и установяване на контакт с оглед сключване на договор (преддоговорни отношения);
2. Сключване и изпълнение на договор;
2. Изпълнение на задължения свързани с финансово-счетоводна отчетност.

Категории данни

Чл. 32 В регистър контрагенти се обработват следните групи данни:

1. Физическа идентичност – име, ЕГН, адрес за кореспонденция, телефон за контакт и е-мейл;
2. Финансова идентичност - банкова сметка, банкови референции;

Служители натоварени с обработка на данните от администратора

Чл. 33 (1) Данните се обработват на принципа „Необходимост да знае" от следните лица, на които изрично е възложено обработване на лични данни от администратора:

1. Служители на "Търговски отдел";
2. Отдел "Счетоводство";
3. Служители “Техническа поддръжка”

Обработващи данни

Чл.34 Администраторът има право да възлага обработването на лични данни от регистър "Контрагенти" на обработващи данни, подизпълнители, консултантски дружества, предоставящи услуги в сферата на данъчното, счетоводното законодателство, правни услуги и др. подобни. Всяко възлагане на обработване по реда на тази разпоредба се прилагат действащите нормативни разпоредби относно личните данни, правилата за обработване в рамките на целта, за която данните са събрани, при спазване на принципа "Необходимост да знае" и съобразно уговореното в съответния договор с обработващия данни.

Събиране и обработване на данните

Чл.35 (1) Данните в регистър "Контрагенти" се събират директно от съответния контрагент.

(2) В случаите, в които контрагентът е юридическо лице, същият предоставя данните за контакт на свои служители или натоварени от него лица за изпълнение на дейности по договора, като изрично декларира изпълнение на задължението си за вземане на съгласие за предоставянето ми, ако такова се изисква и поемане на задължение за поддържането им в актуален вид. По отношение на тези данни "ИЗПИТАЙ МЕ" ООД е обработващ данни и за него се прилагат правилата на чл. 28 от Регламент (ЕС) 2016/679.

Чл.36 (1) Данните се предоставят от контрагенти по имейл или лично (чрез куриерска пратка), като директно се въвеждат в конкретния договор.

(2) След подписване на договора или съответното допълнение към него, един екземпляр се предава на контрагента, прави се електронно копие в PDF формат на договора, а оригиналът на хартиения носител, се съхранява в класьор на специално определено място за това в помещение с контролиран достъп.

Чл.37 Данни необходими за изпълнение на финансово-счетоводни задължения във връзка с изпълнение на договорите се предоставят от всеки акаунт мениджър на Счетоводен отдел на принципа "Необходимост да знае" по имейл или устно, след което се въвеждат в съответния счетоводен софтуер.

Правила при обработване на данните

Чл.38 Всички технически и организационни мерки, които се прилагат за обработването и съхранението на данните в Регистър "Персонал" се прилагат и по отношение на данните в регистър "Списък за достъп". В този смисъл чл.26-28 се прилагат по аналогия.

Категории лица, на които се предоставят данните

Чл.39 Личните данни от регистър "Контрагенти" се предоставят на следните категории трети лица:

1. Органи на държавна, местна власт или съдебни органи, на които законът е възложил контролни функции, след получаване на съответното законно искане за това;
2. На обработващи данни, при спазване правилата на целите на обработване;
3. На други лица - само след взето изрично писмено съгласие на субекта на данни;

Срок за съхранение на данните

Чл.40 Всички данни в регистър „Контрагенти“ се съхраняват както следва**:**

1. Договорите, след като са прекратени и всякакви документи за данъчен контрол, одит и последващи финансови инспекции - 10 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят ако са прекратени след прекратяване;

2. Всички останали документи - 5г. след подписването им от страните;

Ниво на въздействие

Чл. 41 (1) Оценката на въздействието върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни в "ИЗПИТАЙ МЕ" ООД за регистър “Контрагенти“ се определя на *ниско ниво на въздействие*.

(2) При оценката са отчетени характера на обработваните лични данни (бизнес данни), фактът, че контрагенти физически лица са по-скоро изключение, както и обстоятелството, че неправомерното обработване на тези данни не би застрашило неприкосновеността на личността и личния живот или икономически интерес на отделно физическо лице в голяма степен.

(2) За регистър „Клиенти“ в "ИЗПИТАЙ МЕ" ООД са реализирани всички изискващи се технически и организационни мерки за физическа, персонална, документална защита и защита на автоматизираните информационни системи и/или мрежи, както и криптографска защита на личните данни, съответстващи на високо ниво на защита на личните данни, съгласно **"Технически и организационни мерки за защита на личните данни в "ИЗПИТАЙ МЕ" ООД**.

IV. РЕГИСТЪР „ ПОТРЕБИТЕЛИ“

Цели на обработка

Чл.54 (1) Регистър "Потребители" се попълва с данни генерирани от сайтовете, които “Изпитай ме” ООД оперира, което включва.

Категории данни

Чл.55 Във регистър "Потребители" се обработват следните видове данни -

1. информация, която потребителят въвежда ръчно
2. информация, получена от софтуер и/или хардуер, които участват във взаимодействието между потребителя и системите на Изпитай.ме
3. информация, предоставена от трети лица след съгласието на потребителя
4. информация, произтичаща от комуникацията между потребителя и сървърите на Изпитай.ме

Служители натоварени с обработка на данните

Чл.56 (1) Данните се обработват на принципа „Необходимост да знае", като достъп до тях имат следните лица:

1. Управител;
2. Специалист Сигурност;
3. Технически персонал който поддържа системите;
4. Специалист Обслужване на клиенти

Обработващи данни

Чл.57 Администраторът има право да възлага обработването на лични данни от регистър "Потребители" на обработващи данни, дружества, лицензирани за извършване на охранителна дейност. За всяко възлагане на обработване по реда на тази разпоредба се прилагат действащите нормативни разпоредби относно личните данни, правилата за обработване в рамките на целта, за която данните са събрани, при спазване на принципа "Необходимост да знае" и съобразно уговореното в съответния договор с обработващия.

Събиране и обработване на данните

Чл.58 (1) Данните в регистър "Потребители" се предоставят доброволно от лицата при използването им на системите на Изпитай ме.

1. информация, която потребителят въвежда ръчно
2. информация, получена от софтуер и/или хардуер, които участват във взаимодействието между потребителя и системите на Изпитай.ме
3. информация, предоставена от трети лица след съгласието на потребителя
4. информация, произтичаща от комуникацията между потребителя и сървърите на Изпитай.ме

Правила при обработване на данните

Чл.59 (1) Всички технически и организационни мерки, които се прилагат за обработването и съхранението на данните в Регистър "Персонал" се прилагат и по отношение на данните в регистър "Потребители" по аналогия. Помещението, в което се съхранява сървърът е с контрол на

достъп с електронен ключ. Същото е климатизирано, пожарообезопасено, обезопасено от наводнения. Достъпът до сървъра се осъществява през специална криптирана връзка, като достъпът до данните от оторизираните лица става чрез потребителско име и парола.

Категории лица, на които се предоставят данните

Чл.60 Достъп до данните в регистър "Потребители" се предоставят на следните категории трети лица:

1. Органи на държавна и местна власт, на които законът е възложил контролни функции, след получаване на съответното законно искане за това;

2. На обработващи данни, при спазване правилата на целите на обработване;

3. На субектите на данни - само ако е възможно достъпът да се предостави единствено до отнасящите за тях данни;

Срок за съхранение на данните

Чл.61 **Д**анните в регистър Потребители“ се съхраняват при необходимите технически условия на сигурност, освен ако потребителят изрично не е поискал да бъде заличен.

Ниво на въздействие

Чл.62 (1) Оценката на въздействието върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни в "ИЗПИТАЙ МЕ" ООД за регистър “Потребители“ се определя на *ниско ниво на въздействие*.

(2) При оценката са отчетени характера на обработваните лични данни, както и обстоятелството, че неправомерното обработване на тези данни не би застрашило неприкосновеността на личността и личния живот или икономически интерес на отделно физическо лице в голяма степен.

(2) За регистър “Потребители“ в "ИЗПИТАЙ МЕ" ООД са реализирани всички изискващи се технически и организационни мерки за физическа, персонална, документална защита и защита на автоматизираните информационни системи и/или мрежи.

V. УНИЩОЖАВАНЕ НА ДАННИТЕ

Чл.63 (1) Всички лични данни, по отношение, на които е получено писмено искане за заличаване от потребителя се унищожават.

(2) Документите от съответните регистри, които са на хартиен носител и съдържат лични данни, се унищожават само чрез специално устройство (шредер) от съответния служител, натоварен с обработването им.

(3) Данни съхранени в електронен вид се изтриват.

(4) Всяка година през януари месец, лицата на които е възложено обработване на данни извършват инвентаризация за установяване на данните, подлежащи на унищожаване, след което съставят опис на унищожените данни на хартиен и електронен носител.

(5) По отношение съхранението и унищожаването на лични данни се прилага и **"Политика за съхранение на личните данни в "ИЗПИТАЙ МЕ" ООД.**

VI. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ, УПРАВЛЕНИЕ И РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ

Действия при инцидент

Чл. 64. (1) При възникване и установяване на инцидент – бедствие, пробив в сигурността отпадане на оборудване, неоторизиран достъп и др., който би застрашил целостта, поверителността или наличността на личните данни, инцидентът се докладва незабавно, но не по-късно от 12 часа от узнаването на Мениджър Информационни технологии.

(2) Отговорен за докладването е всеки служител в дружеството, извършващ дейност по обработване на лични данни.

(3) Веднага след получаване на уведомлението Мениджър Информационни технологии отваря ТТ (trouble ticket) в системата и определя отговорно лице, което да събере данни за инцидента в срок от 24 часа.

(4) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада, името на лицето оценило инцидента. Регистърът за инциденти се съхранява в Технически отдел и е част от общ регистър за инциденти, воден в дружеството (**Регистър за инциденти**).

(5) След анализ на инцидента в дневника се записват последствията от инцидента, наличие или липса на компрометиране на данни, вида данни, които са засегнати и мерките, които са предприети за отстраняването му, както и преценка дали са налице необходимите предпоставки за уведомяване на КЗЛД и засегнатите субекти на данни, ако има такива.

(6) Целият процес се намира под общото ръководство на Мениджър Качество в дружеството.

Уведомяване на КЗЛД

Чл.65 (1) В случай, че в рамките на анализа на инцидента се установи нарушение на сигурността на личните данни с вероятност нарушението да породи риск за правата и свободите на физическите лица, Мениджър Информационни технологии без ненужно забавяне и когато това е осъществимо - не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението Комисията за защита на лични данни. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

(2) В случаите, в които инцидентът засяга данни, по отношение на които “Изпитай ме” ООД е обработващ лични данни, уведомлението се отправя до администратора на тези данни без ненужно забавяне.

Чл.66 (1) В уведомлението се съдържа най-малко следното:

1. 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 приблизително количество на засегнатите записи на лични данни;

2. Посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

3. Описание на евентуалните последици от нарушението на сигурността на личните данни;

4. 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.

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

Чл.67 По отношение установяването, докладването и управлението на инциденти се прилагат и следните процедури: **"Процедура за обработка на инциденти, свързани с физически достъп" и "Процедура за мониторинг на реакцията при инциденти и сигнали"**.

Уведомяване на субекта на данните

Чл.68 (1) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица Мениджър Информационни технологии уведомява лицата, натоварени да обработват съответните компрометирани данни, като същите имат задължение да съобщят на субектите на данни за нарушението на сигурността на личните данни.

(2) В съобщението се описва естеството на нарушението, какви категории дани са засегнати, евентуалните последици и предприетите мерки за намаляване вредния ефект от нарушението и информация за контакт с администратора за получаване на допълнителна информация.

(3) Този ред не се прилага, ако:

1. В резултат на предприетите технически и организационни мерки за защита данните биха били неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

2.Администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

2. Уведомлението би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

VII. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Право на достъп

Чл.69 (1) Администраторът е длъжен да даде на субект на данни достъп до отнасящи се за него лични данни, които той обработва. Освен достъп до данните администраторът предоставя и следната допълнителна информация:

1.Целите на обработването;

2. Съответните категории лични данни;

3. Получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави или международни организации;

4. Когато е възможно, предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;

5.Съществуването на право да се изиска от администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване;

6.Правото на жалба до КЗЛД;

7. Когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

8. Съществуването на автоматизирано вземане на решения, включително профилирането и в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

(2) В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, администраторът предоставя на съответното физическо лице достъп до частта от тях, отнасяща се само за него.

(3) "ИЗПИТАЙ МЕ" ООД предоставя информацията по ал. 1 безплатно.

(4) При смърт на физическото лице правата му по ал. 1 и 2 се упражняват от неговите наследници.

Право на коригиране и ограничаване

Чл.70 Субектът на данни има право да поиска от администратора да коригира без ненужно забавяне неточните лични данни, свързани с него, както и да ограничи обработването на данните, при условията на чл.18 от Регламент 2016/679.

Право на изтриване

Чл.71 Субектът на данни има правото да поиска от администратора изтриване на свързаните с него лични данни без ненужно забавяне, когато е приложимо някое от посочените по-долу основания:

1. Личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;

2. Субектът на данните оттегли своето съгласие, когато данните се обработват въз основа на дадено съгласие и няма друго правно основание за обработването;

3. Личните данни са били обработвани незаконосъобразно;

4. Личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на Съюза или правото на държава членка, което се прилага спрямо администратора;

(2) Когато администраторът е предоставил личните данни на други администратори и/или обработващи данни, като се отчита наличната технология и разходите по изпълнението, администраторът предприема разумни стъпки, включително технически мерки, за да уведоми администраторите, обработващи личните данни, че субектът на данните е поискал изтриване от тези администратори на всички връзки, копия или реплики на тези лични данни.

(3) Субектът на данни не може да иска изтриване на данни, когато:

1. Обработването се извършва в изпълнение на правно задължение, което обвързва администратора;

2. За установяването, упражняването или защитата на правни претенции и в др. случаи предвидени в приложимото законодателство.

Право на преносимост на данните

Чл. 72. 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 а) обработването е основано на съгласие в съответствие или на договорно задължение и б) обработването се извършва по автоматизиран начин.

Начин на упражняване на правата

Чл. 73 (1) Физическите лица, упражняват правата си, като подават писмено заявление до "ИЗПИТАЙ МЕ" ООД съдържащо минимум следната информация:

1. име, адрес и други данни за идентифициране на съответното физическо лице;

2. описание на искането;

3. предпочитана форма за предоставяне на информацията;

4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) Заявлението се подава подава по електронен път при спазване правилата на Закона за електронния документ и електронния подпис, по пощата, лично на посочените на интернет сайта на дружеството контакти. При подаване на заявление от упълномощено лице, към заявлението се прилага и изрично нотариално заверено пълномощно.

(3) Заявлението се завежда в **Регистър на заявления за достъп.**

(3) Срокът за разглеждане на заявлението и произнасяне по него е 14-дневен от деня на подаването на искането, съответно – 30-дневен, когато е необходимо повече време за събиране исканите данни, с оглед възможни затруднения в дейността на администратора.

(4) Отговорът се предоставя срещу подпис или по пощата, с обратна разписка, като се съобрази с предпочитаната от заявителя форма на предоставяне на информацията.

(5) Когато данните не съществуват или предоставянето им е забранено със закон, на заявителя се отказва достъп до тях, като мотивира отказа си и уведомява субекта за правото му на защита пред КЗЛД, или компетентния административен съд.

(6) Отговорен за спазването и изпълнението на процедурите, свързани с попълване на регистъра на Заявленията за достъп и изготвяне на отговори по постъпилите заявления е Финансовия директор. Контрол по спазване на правилата по тази разпоредба се извършва от Мениджър Качество.

VIII. КОНТРОЛ ПРИ ОБРАБОТВАНЕТО НА ДАННИ

Контрол

Чл.74 Контролът в дружеството при обработването на лични данни се извършва с цел проследяване и оценка на ефективността и ефикасността на операциите, надеждността на въведените организационни и технически мерки, съответствие на дейностите по обработване с приложимата правна рамка и спазването на вътрешно-фирмените правила и политики.

Лица отговорни за контрола

Чл.75 (1) Общ контрол по спазване на нормативната уредба и вътрешните правила за защита на лични данни се извършва от ръководството на дружеството - Управителя и от Мениджър "Качество".

(2) Ръководителите на отдели извършват текущ и последващ контрол при спазване отделните правила и политики в съответните отдели, като при констатиране на нарушение уведомяват лицата по предходната алинея.

(3) За нарушения на приложимата нормативна уредба и вътрешните правила и политики за защита на личните данни съответните длъжностни лица носят дисциплинарна, административна, гражданска и наказателна отговорност.

(4) Дисциплинарната отговорност се реализира по реда на КТ.

Международен трансфер на лични данни

Чл. 76 (1) “Изпитай ме” има право да прехвърля лични данни, в качеството си на техен администратор, или обработващ в страни извън ЕИП, когато това е необходимо за дейността на фирмата и за постигането на целите, с които за събрани съответните лични данни.
(2) Когато се наложи такова прехвърляне на лични данни извън ЕИП, “Изпитай ме” ООД подбира определени доставчици на услуги, които поддържат висок стандарт на сигурност на данните.

Настоящата политика е приета и утвърдена през Май 2023 г. и влиза в сила, считано от 25.05.2023г.

Приложения и относими документи:

1. Декларация - съгласие за обработване на данни от служител Образец №1

2. Декларация - съгласие за обработване на данни от кандидат за работа Образец № 1а

3. Декларация за конфиденциалност от служител, натоварен с обработване на данни Образец № 2;