Политика за защита на личните данни
на „ВОРИК ГРУП" ЕООД
/Политиката/

Въведение

Дружеството, като отговорна организация има мисията да предлага решения, позволяващи на хората да живеят спокойно, без компромис с качеството и предпочитанията си.

„ВОРИК ГРУП" ЕООД е компания с дългогодишен опит в обслужването на клиенти в областта на хотелиерството, нощните клубове и от скоро в кремиранете в крематориум. Въпросът, свързан със защитата на физическите лица във връзка с обработването на техните лични данни е от изключително значение за Дружеството, тъй като клиентите ни винаги са на първо място.

Тази политика разяснява:

- законовите задължения на Дружеството, в качеството му на *администратор* на лични данни,
- принципните положения, които Дружеството възприема с оглед защитата на физическите лица във връзка с обработването на техните лични данни;
- задълженията на служителите на Дружеството.

Политиката е задължителна и се прилага от всички служители на Дружеството, както и спрямо външните физически и юридически лица, обработващи лични данни за него.

Нарушаването на настоящата политика ще бъде взето под сериозно внимание и може да доведе до дисциплинарни санкции или прекратяване на бизнес взаимотношения.

Термини и дефиниции

Използваните в настоящата Политика и свързаните с нея политики/процедури термини следва да се четат и разбират по следния начин:

а) Регламент – Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент за защита на данните);

б) Субект на данни – физическо лице, чиито лични данни Дружеството събира или обработва. Тези физически лица включват, но не се ограничават до:

1. физическите лица, които са служители на Дружеството;

2. физическите лица, които са клиенти и доставчици на Дружеството;

3. физическите лица, които са законни представители, упълномощени лица или лица за контакт на клиентите и доставчиците на Дружеството;

4. други физически лица, които влизат в контакт с Дружеството във връзка с предоставяните от него продукти и услуги;

в) Лични данни – всяка информация, въз основа на която може пряко или непряко да бъде идентифицирано физическо лице, по специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или друг признак, специфичен за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

В общия случай, за да съществува и осъществява своите дейности съобразно предмета му на дейност, Дружеството събира и обработва основно следните категории лични данни:

1. обикновени лични данни (имена, ЕГН, адрес, телефон, имейл, образование, трудова дейност; банкова, счетоводна, данъчна и осигурителна информация*);*

2. специални категории данни (здравословно състояние на служителите; запис от видеокамери*);*

г) Администратор на лични данни – физическо или юридическо лице, което само или съвместно с други лица определя целите и средствата за обработването на лични данни.

Дружеството е администратор на лични данни;

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

е) Обработване – всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране,

съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

ж) Трета страна – физическо или юридическо лице, публичен орган, агенция или друг орган и/или организация, различен от субекта на данни, администратора или обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

з) 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;

и) Искане от субект на данни – изявление от субекта на данни или от изрично упълномощено от него лице за упражняване на правата му по Регламента;

й) Псевдонимизиране – обработване на личните данни по такъв начин, че личните данни да не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки, с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;

к) Анонимизиране – премахване на данните, които идентифицират лицето, така че то да не може повече по никакъв начин да бъде еднозначно определено;

л) Надзорен орган – независим публичен орган, създаден от държава членка съгласно член 51 от Регламента, който е отговорен за наблюдението на прилагането на Регламента, за да се защитят основните права и свободи на физическите лица във връзка с обработването и да се улесни свободното движение на личните данни в рамките на Съюза.

В Република България този надзорен орган е Комисия за защита на личните данни;

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

н) Трансфер на лични данни – предаване на лични данни на трета държава извън Европейския съюз или на международна организация;

о) Нарушение на сигурността на лични данни – накърняване 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.

Свързани политики и документи:

Тази политика разяснява законовите задължения на Дружеството, в качеството му на администратор на лични данни, задълженията и отговорностите на служителите и другите гореизброени адресати с цел спазване изискванията на Регламента, както и на приложимото действащо българско законодателство.

Тази политика се придружава от следните свързани с нея Политики/Процедури, които следва да бъдат консултирани при необходимост от предприемане на действие и/или спазване при изпълнението на задълженията, свързани със защитата на личните данни:

1. Политика за информационна сигурност и свързаните с нея политики/процедури;
2. Процедура за минимизиране на данни;
3. Проедура за искания от субектите на данни;
4. Декларация за поверителност;
7.Политика за съхранение на данни
8.Уведомление за видеонаблюдение

Контролът по спазването на настоящата политика и сързаните с нея политики се осъществява от Определен със заповед служител на Дружеството.

Политиката е приета от Управителя КРИСТИЯН НИКОЛАЕВ КИРОВ на 05.05.2021 г.

Политика се преглежда и актуализира редовно и в случай на необходимост, но не по-малко от веднъж годишно.

Структура и съдържание

I. Прилагани от Дружеството принципи за защита на личните данни
II. Ключови роли и отговорности
III. Данни на Деца
IV. Необходими условия за обработване на данните
V. Информиране на субектите на данни
VI. Сигурност на данните
VII. Съхранение на данните
VIII. Споделяне на данни
IX. Трансфер на данни
X. Искания на субектите на данни

XI. Нарушение на сигурността на данните
XII. Обучения и тренинги на служителите
XIII. Осигуряване на непрекъснато съответствие
XIV. Заключителни разпоредби

I. Прилагани от Дружеството принципи за защита на личните данни

1. Дружеството прилага и очаква от всички отговорни лица по настоящата политика да спазват следните принципи при събирането и обработването на личните данни:

*а) **Законосъобразност, добросъвестност и прозрачност***

Това означава, че винаги, когато се събират лични данни субектът на данни следва да е информиран за това (прозрачност). Обработването следва да се извършва в съответствие с предварително дадената информация (добросъвестност), както и да почива на валидно правно основание (законосъобразност);

*б) **Ограничение на целите***

Дружеството събира личните данни за конкретни, изрично указани и легитимни цели и не ги обработва по-нататък по начин, който е несъвместим с тези цели. Дружеството определя целите, за които се използват личните данни и ограничава обработването им в рамките на необходимото за постигане на тези цели. В случай на необходимост от използване на данните за вторични цели (други цели извън първоначалните), се извършва преценка за съвместимостта на новите с първоначалните цели;

*в**) Минимизиране на данните***

Дружеството не събира и съхранява други лични данни извън строго необходимите, подходящи и свързани с целта, за която се събират;

*г**) Точност на данните***

Дружеството въвежда разумни мерки за гарантиране на точността и поддържането на актуалността при необходимост на администрираните от нея лични данни, в това число мерки, които да позволят навременно идентифициране и изтриване на личните данни, които са в повече или чиито срокове са изтекли, както и коригирането на неточните лични данни.

*д) **Ограничение на съхранението***

Личните данни следва да бъдат съхранявани за период, не по-дълъг от необходимото за целите, за които се събират, както и се въвеждат мерки (там, където е необходимо), които не позволяват идентифицирането на субекта на данни за срок по-дълъг от необходимото.

*е) **Поверителност (конфиденциалност) и цялостност на данните***

Лините данни се обработват по начин, който осигурява подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или

повреждане. Дружеството прилага подходящи технически и организационни мерки, за да запази цялостта и поверителността на данните във всеки един момент.

ж) ***Отчетност,*** който принцип включва отговорност на Дружеството и възможности да докаже спазването на всички принципи на Регламента, изброени до тук.

2. Планирането на всички **нови или значителната промяна** на вече съществуващи системи, които събират или обработват лични данни, следва да са обект на надлежна преценка свързана със защитата на личните данни, оценка на риска за правта и свободите на субектите на данни и ако е необходимо се извършва оценка на въздействието.

II. Ключови роли и функции в организацията, свързани със защитата на личните данни:

1. Като администратор на лични данни Дружеството е отговорно за осигуряването на съответствие с изискванията на закона, разяснени и по-нататък в настоящата политика.

Нарушаването на законодателството може да доведе до негативни последици за Дружеството и неговите служители и партньори.

В тази връзка Дружеството изисква стриктно спазване на настоящата политика и в случай на невъзможност за прилагането ѝ (по някаква причина) всеки може да се обърне своевременно за консултация/съвет, разяснения към:

АНЕЛИЯ ИВАНОВА ИВАНОВА – Длъжностно лице по защита на данни- в организацията

2. Следните функции са определени като ключови в организацията с оглед защитата на личните данни:

а) Управителните органи на Дружеството взимат решения и одобряват стратегиите, политиките и правилата на **„ВОРИК ГРУП" ЕООД** във връзка със защитата на личните данни;

б) **АНЕЛИЯ ИВАНОВА ИВАНОВА – Длъжностно лице по защита на данни** е отговорен за управлението на програмата за защита на личните данни в Дружеството и за разработването, въвеждането и популяризирането на политиките и процедурите за защита на личните данни и участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни;

в) **АНЕЛИЯ ИВАНОВА ИВАНОВА – Длъжностно лице по защита на данни** наблюдава и анализира законодателството в областта на защитата на личните данни и промените в него, разработва и актуализира необходимите правни документи и оказват правна помощ на Дружеството за постигане на неговите цели, свързани с личните данни;

г) Специалистите по информационни технологии отговарят за това всички системи, оборудване и услуги, използвани за съхранение на данни, да съответстват на стандартите за сигурност и извършват периодични

проверки и сканирания, за да гарантират, че хардуера и софтуера функционират правилно;

д) Лицата, заети с управлението на човешките ресурси отговарят съвместно със служителя по б. „б" за провеждането на редовни обучения на служителите във връзка със защитата на личните данни, както и самостоятелно за това личните данни на служителите по трудови договори и изпълнителите по граждански договори с Дружеството да бъдат обработвани законосъобразно;

е) Лицата, натоварени с маркетинга и връзката с клиентите и външните лица, подпомагани от лицето по б. „б", отговарят за това всички маркетинг инициативи и комуникации до клиентите и външните лица да съответстват на принципите за защита на личните данни, в това число и комуникацията с медиите;

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

3. Гореизброените функции са определени като ключови в Дружеството с оглед защитата на личните данни. Това не изключва отговорността на всеки един адресат на настоящата политика по нейното спазване.

III. Данни на Деца

1. Регламентът поставя по-стриктни изисквания за обработване на данни на деца. Съгласно националното законодателство това са лица под 14-годишна възраст.

2. В общия случай Дружеството не събира и не обработва лични данни на деца.

Такива данни е възможно да се събират в изпълнение на българското законодателство.

3. Ако възникне необходимост от събиране на лични данни на деца, се взимат всички необходими мерки, за да се гарантира тяхната защита.

IV. Необходими условия за обработване на данните

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

а) субектът на данни е дал *съгласие* за обработване на личните му данни за една или повече цели;

б) 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;

в) обработването е необходимо за спазването на *правно задължение* на Дружеството;

г) обработването е необходимо, за *да бъдат защитени жизненоважните интереси* на субекта на данните или на друго физическо лице;

д) обработването е необходимо за *изпълнението на задача от обществен интерес* или при *упражняването на официални правомощия* от Дружеството;

е) обработването е необходимо за целите на *легитимните интереси* на Дружеството или трета страна и пред такива интереси нямат преимущество интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

2. Всички лични данни, които се събират и обработват от Дружеството, трябва да отговарят поне на едно от горните условия.

3. В допълнение, когато се налага събирането на специални категории лични данни и лични данни, свързани с присъди и нарушения, необходимо е да са налице по-строгите условия така, както са дадени в чл. 9 и чл. 10 от Регламента.

4. В общия случай Дружеството не събира и обработва лични данни по предходната точка.

5. В случай че при събирането и обработването на лични данни служител идентифицира данни от специалните категории лични данни, той следва да се обърне към **АНЕЛИЯ ИВАНОВА ИВАНОВА – Длъжностно лице по защита на данни** за да получи уверение и одобрение, че събирането се извършва в съответствие с настоящата политика.

6. Дружеството събира лични данни на правно основание:
- *закон;*
- *договор;*
- *легитимен интерес.*

7. Извън горните случаи на обработване на данни е възможно да е необходимо събиране и обработване на лични данни, за което да няма друго правно основание за обработване, освен **съгласие** от субекта на данни (тази и следващите точки не се отнасят до събирани лични данни, представляващи специални категории данни. За обработването на специалните категории данни погледнете т. 3 от настоящия раздел).

8. Такъв може да бъде случаят, при който Дружеството иска да използва нечии лични данни по неочакван или различен начин или по начин, от този, за който данните са събрани или който е несъвместим с това, за което субектите на данни вече са уведомени, че се събират и обработват техните лични данни.

9. „Съгласие на субекта на данни“ има значението, определено по-горе в раздел „Термини и дефиниции“. Мълчанието, предварително отметнатите полета или липсата на действие не се приемат за съгласие по смисъла на Регламента.

10. Всеки субект на данни може да оттегли съгласието си по всяко време.

11. Служителят, който изисква съгласието на субекта на данни, следва да се увери, че субектът на данни разбира ясно и различава исканото съгласие от другите документи, предоставяни за подпис.

12. Когато се прави оценка дали съгласието е било свободно изразено, се отчита най-вече дали изпълнението на даден договор, включително предоставянето на дадена услуга, е поставено в зависимост от съгласието за обработване на лични данни, което не е необходимо за изпълнението на този договор.

13. Съгласието следва да бъде документирано. За повече информация следва да бъде консултирана *Процедурата по искане на съгласие и формите за съгласие*.

14. В качеството си на администратор на лични данни Дружеството може да поддържа регистър на дейностите по обработване в съответствие с изискванията на чл. 30, параграф 1 от Регламента. Регистърът се поддържа в електронен и хартиен вариант в офиса на дружеството

При въвеждане на нова дейност по обработване регистърът се актуализира своевременно.

V. Информиране на субектите на данни

1. В съответствие с изискването на Регламента за „добросъвестно и прозрачно“ обработване на лични данни, всеки субект на данни следва да бъде информиран за конкретни обстоятелства относно личните му данни.

2. Информацията следва да се предостави в момента, в който се събират данните от субекта на данни, а когато данните не са получени от него, в разумен срок след получаването им, но най-късно в срок до един месец, като се отчитат конкретните обстоятелства, при които личните данни се обработват или най-късно при осъществяване на първия контакт със субекта на данните, но не по-късно от този момент или ако е предвидено разкриване пред друг получател, най-късно при разкриването на личните данни за първи път.

3. Всички служители, които събират лични данни (осъществяват първия контакт при събирането на личните данни) следва да информират субектите на данни поне относно следните неща: данните, които идентифицират Дружеството и координатите за връзка с него; какви лични данни, на какво основание и за какви цели се събират; кои са легитимните интереси, преследвани от Дружеството или от трета страна, когато обработването се извършва на това основание; на кои получатели или

категории от получатели се разкриват; ще бъдат ли предавани на трети държави извън ЕС или на международни организации и какви гаранции за защита ще се прилагат; за какъв срок се съхраняват данните, какви права има лицето във връзка с тях, в това число правото му да оттегли съгласието си; дали предоставянето на лични данни е задължително или договорно изискване или изискване за сключването на договор, както и дали субектът на данните е длъжен да предостави данните си и евентуалните последствия, ако не го направи; използват ли се средства за автоматизирано вземане на решения спрямо лицето, включително профилиране, както и каква логика се използва и какво е значението и последиците за лицето от това обработване.

4. Дружеството е разработило Споразумение-информация за правата на лицата по защита налични данни (Praivacy notice), която е един от методите, чрез които информира субектите на данни относно обстоятелствата по предходната точка.

5. Хартиено копие на Споразумение-информация за правата на лицата по защита налични данни (Praivacy notice) *служителите могат да поискат от* **АНЕЛИЯ ИВАНОВА ИВАНОВА – Длъжностно лице по защита на данни, на място във офиса на дружеството или на телефон 0885537336**

6. В общия случай Дружеството събира данните директно от субекта на данни. В някои от случаите даните могат да бъдат събирани данни от публични регистри или трети лица.

VI. Сигурност на данните

1. Минималните изисквания към служителите и техническите и организационни мерки за сигурност, прилагани от Дружеството, са описани в Политиката за информационна сигурност и свързаните с нея политики, процедури и правила.

2. По-долу са резюмирани основните мерки за информационна сигурност, които Дружеството прилага:

- достъпът до информационните масиви, съдържащи лични данни, се предоставя и осъществява в съответствие с изискването „необходимост да се знае";
- там, където е необходимо, се прилагат изискуемите мерки с цел данните да не могат при тяхното електронно изпращане да бъдат прочетени, копирани, променяни, изтривани без разрешение;
- въведена е система за проследяване на логовете, която съдържа информация за това дали и от кого са достъпени, променени или изтрити личните данни в информационната система;
- когато личните данни се обработват от обработващ лични данни, това се случва в съответствие с указанията на Дружеството;
- личните данни са защитени от случайна загуба, унищожаване или повреждане;

- личните данни, събрани за различни цели, могат да бъдат и се обработват отделно;
- личните данни се съхраняват за определения срок.

3. Всички служители са задължени да спазват най-малко следното:

- да спазват правилата за достъп;
- да спазват правилата за използване на служебните пощи и правилата относно обновяване на паролите;
- да спазват правилата за споделяне на информация и там, където се налага, изпращането на информацията да се извършва с архивирани папки и пароли за достъп;
- да спазват правилата за съхраняване на хартиени документи (шкафовете и помещенията, в които се съхраняват хартиени носители на лични данни, се заключват, за да се предотврати случаен или преднамерен неоторизиран достъп до тях от трети лица);
- да спазват правилата за „бекъпиране" на информация;
- да спазват правилата за „чисто бюро";
- да не предоставят паролата за достъп до профила си на друго лице, освен на оторизираните служители, които поддържат компютрите;
- да не предоставят парола за достъп до споделените папки;
- да спазват процедурите и правилата за унищожаване на данните (хартиените носители се унищожават по начин, който да не позволява възстановяване на носителя и данните в него. За данните, съхранявани в електронен формат, се предприемат нужните действия, така че да се осигури тяхното трайно изтриване или унищожаване.)

4. Подробните мерки и нструкции са описани в горецитираната Политика за информационна сигурност.

VII. Съхранение на данните

1. За да осигури добросъвестно обработване на данните и ограничение на срока за съхранение, Дружеството няма да съхранява за период по-дълъг от необходимото събираните и обработвани лични данни.

2. Сроковете за съхранение на данните са съобразени с изискванията на чл. 5, парагаф 1, б. „д" от Регламента и съществуващите добри практики, като Дружеството е взело предвид спецификата на дейността си.

3. Веднага, след като информацията не е необходима повече или срокът за съхранение е изтекъл, тя следва да бъде унищожавана. Правилата за съхранение и унищожаване на лични данни се съдържат в Общата политика за съхранение и унищожаване на лични данни.

4. Анонимизирани данни могат да бъдат съхранявани за неограничен срок съгласно законодателството в сферата на защитата на личните данни. Анонимизирането е способ, чрез който данните се променят по такъв начин, че лицето вече да не може да бъде идентифицирано и това е необратимо.

VIII. Споделяне на данни

1. Споделянето на лични данни следва да се извършва в съответствие с всички принципи за обработване на лични данни, установени в Регламента, и в частност законосъобразно и по прозрачен за субектите на данни начин.

2. При избор на партньор, който ще се явява обработващ за Дружеството се извършва оценка на обработващ от гледна точка защитата на личните данни и се прилагат всички изисквания на Регламента с оглед осигуряване защитата и поверителността на данните.

3. Обработването на лични данни от външно лице се извършва въз основа на писмен договор.

IX. Трансфер на данни

1. Дружеството не съхранява лични данни извън Европейския съюз и не извършва трансфер на данни извън Европейския съюз.

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

X. Искания на субектите на данни

1. Съгласно Регламента субектите на данни имат следните права:

а) право на информираност;

б) право на достъп;

в) право на коригиране;

г) право на изтриване (право "да бъдеш забравен");

д) право на ограничаване на обработването;

е) право на преносимост на данните;

ж) право на възражение;

з) права при автоматизирано вземане на индивидуални решения и профилиране;

и) право на жалба.

2. Всички служители съдействат на субектите на данни при упражняване на техните права. Ако субект на данни иска да упражни някое

от горните права, служителите на Дружеството са задължени да му съдействат.

3. В случай на получено искане от субект на данни, искането се входира в специален регистър в Дружеството.

4. Субектът на данни има право да получи отговор и информация без заплащане на такса. Независимо от последното, в определени случаи, ако исканията са прекомерни, Дружеството може да откаже да предостави информация или да събере административна такса. Дружеството дефинира случаите за прекомерности, както и събирането на административната такса в Процедурата за разглеждане на искания от субекти на данни.

5. При предоставянето на данни и/или достъп до информация на субект на данни следва да се вземат всички необходими мерки с цел опазване правата и свободите на третите лица.

6. Гореописаните правила се прилагат и по отношение на искане, когато субектът на данни е служител на Дружеството, в който случай исканията се отправят към **АНЕЛИЯ ИВАНОВА ИВАНОВА – Длъжностно лице по защита на данни**

XI. Нарушение на сигурността на данните

1. Дружеството се стреми да поддържа подходящо ниво на сигурност на личните данни чрез въведени технически и административни контроли, така че данните да бъдат защитени от неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане.

2. За нарушения се считат, например:

а) загуба или кражба на данни или оборудване, носител на лични данни;

б) недостатъчен контрол на достъпа, водещ до неразрешено използване на данни;

в) повреда на оборудване;

г) неразрешено разкриване на данни (например изпращане на имейл до грешен получател);

д) човешка грешка;

е) хакерска атака.

3. Всички служители на Дружеството полагат усилия да предотвратят каквито и да било нарушения на сигурността на личните данни.

4. Когато служител на Дружеството разбере за нарушение на сигурността на личните данни, той е длъжен незабавно да уведоми **АНЕЛИЯ ИВАНОВА ИВАНОВА – Длъжностно лице по защита на данни**

5. **АНЕЛИЯ ИВАНОВА ИВАНОВА – Длъжностно лице по защита на данни** събира по-подробна информация за нарушението в срок до 24 часа от откриването му.

6. В случай на нарушение на сигурността на личните данни, което е вероятно да породи риск за правата и свободите на физическите лица,

Дружеството уведомява Комисия за защита на личните данни без ненужно забавяне, но не по-късно от 72 часа от узнаване за нарушението.

7. Уведомяването на Комисия за защита на личните данни за нарушението и съобщаването му на субектите на данни се извършва по реда и начина, установени в Процедурата за уведомяване и съобщаване на нарушения на сигурността на личните данни.

XII. Обучения и тренинги на служителите

1. Дружеството осъзнава важната роля на всеки един служител в спазването на закона и защитата на субектите на данни при обработване на техните лични данни.

2. За да се справи с предизвикателствата на защитата на личните данни, всеки служител, който има достъп до лични данни администрирани от Дружеството следва да е обучен и да познава най-малко следните неща:

- принципите за защита на личните данни;
- задълженията си при използването на личните данни само в разрешените му случаи и разрешаване на използването на личните данни само на оторизирани лица;
- необходимостта от стриктното спазване на описаните в настоящата политика и свързаните с нея политики и процедури правила, както и правилното използване на съответните форми и образци;
- правилното използване на служебните компютри, служебните пощи, минималните мерки за информационна сигурност;
- важността от заключване на мониторите при напускане на служебното място;
- сигурното съхраняване на информация на хартиени и електронни носители и копия на такива;
- мерките и правилата за унищожаване на данните;
- специфичните рискове, отнасящи се до отдела, в който работи.

3. На служителите се провежда въвеждащо обучение.

XIII. Осигуряване на непрекъснато съответствие

1. **Служител определен със заповед** извършва планирани проверки и/или вътрешен одит на защитата на личните данни, който включва минимум оценка на следното:

- спазването на политиките за защита на личните данни, включително разпределянето на отговорностите;
- повишаването на осведомеността;
- обученията и тренингите на служителите;
- ефективността на практиките за защита на личните данни, включително спазването на правата на субектите на данни;
- трансферите на лични данни, ако се извършат такива;
- управлението на нарушения на сигурността на личните данни;
- решенията по жалби във връзка със защитата на личните данни;
- нивото на разбиране на политиките и процедурите за защита на личните данни и Декларацията за поверителност;

- актуалността на политиките и процедурите за защита на личните данни и Декларацията за поверителност;
- точността на съхраняваните лични данни;
- съответствието с изискванията на дейностите, извършвани от обработващите лични данни;
- ефективността на мерките за справяне с недостатъчно ниво на съответствие и нарушения на сигурността на личните данни.

2. Извън гореописаните планирани проверки се извършват и регулярни, ежедневни проверки и наблюдение на спазването на Политиката.

3. **АНЕЛИЯ ИВАНОВА ИВАНОВА – Длъжностно лице по защита на данни** в сътрудничество със служителите и лицата, които имат ключови роли и функции във връзка със защитата на личните данни в Дружеството, разработва план за отстраняване на констатираните несъответствия с правилата за защита на личните данни в разумен срок. При установено голямо несъответствие се докладва на Управителя, който извършва надзор върху отстраняването на несъответствието.

XIV. Заключителни разпоредби

Служителите на Дружеството, заемащи ръководни позиции, поемат отговорност да гарантират, че подчинените им служители, имащи отношение към обработването на лични данни, разбират и спазват настоящата Политика и всички други вътрешни политики, процедури и правила, приети от Дружеството в тази област.

УТВЪРДИЛ:…….