ВЪТРЕШНИ ПРАВИЛА
ЗА СИГУРНОСТ, ЗАДЪЛЖИТЕЛНИ ЗА
СЛУЖИТЕЛИТЕ, ИМАЩИ ДОСТЪП ДО РЕГИСТРИ С ЛИЧНИ ДАННИ
НА ИНВЕСТИЦИОНЕН ПОСРЕДНИК “ФАКТОРИ” АД

I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Настоящите вътрешни правила уреждат условията и реда за водене на регистри по Закона за защита на личните данни (ЗЗЛД), както и организацията и реда за упражняване на контрол при обработването на лични данни от служителите на Инвестиционен посредник (ИП) “ФАКТОРИ” АД.

(2) 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.

(3) Обработване на личните данни се състои и в осигуряване на достъпа до определена информация само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.

Чл. 2. (1) Вътрешните правила се приемат с цел да регламентират:

1. Създаване на процедури и механизми за гарантиране на неприкосновеността на личността и личния живот на клиенти и служители на ИП чрез осигуряване на защита от неправомерно обработване на свързаните с тях лични данни в процеса на обработване и движение на данните;

2. Видовете регистри, които се водят при ИП и тяхното описание.

3. Необходимите технически и организационни мерки за защита на личните данни на посочените по-горе лица от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други форми на обработване на лични данни).

4. 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.

5. Процедури за докладване, управляване и реагиране при инциденти.

(2) Вътрешните правила се утвърждават, допълват, изменят и отменят от Съвета на Директорите (СД) на ИП “ФАКТОРИ” АД.

Чл. 3. Настоящите вътрешни правила се прилагат за лични данни по смисъла на Закона за защита на личните данни и се издават на основание Наредба № 1 за минималното ниво на технически и организационни мерки и допустимия вид защита на лични данни на Комисията за защита на личните данни.

Чл. 4. ИП е администратор на лични данни по смисъла на чл.3, ал.1 от Закона за защита на личните данни и е регистриран в Комисията за защита на личните данни.

Чл. 5. (1) Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.

(2) Личните данни се събират за конкретни, точно определени и законни цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

II. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 6. (1) Администраторът възлага обработването на личните данни на негови служители. Обработването може да се възлага на повече от един обработващ данните, съобразно

спецификата на изпълняваните от тях служебни функции и с цел разграничаване на конкретните им задължения.

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

Чл. 7. (1) Личните данни в регистрите се набират от администратора на лични данни, респективно - обработващият лични данни, чрез устен разговор и/или на хартиен носител, както и чрез копиране на лична карта на клиентите на ИП, предвид изискванията на Закона за пазарите на финансови инструменти, актовете по прилагането му и пряко приложимите Делегирани Регламенти на ЕК.

(2) За необходимостта от набирането на данните и целите, за които ще бъдат използвани, обработващият данните информира лицето, съответно клиента на ИП.

(3) Съхраняването на лични данни на хартиен носител се осъществява като данните се съхраняват: в папки в определени заключващи се шкафове и хартиените носители не се изнасят от офиса (адреса на управление) на ИП.

ВИДОВЕ РЕГИСТРИ, КОИТО СЕ ВОДЯТ В ПРИ ИНВЕСТИЦИОННИЯ ПОСРЕДНИК ВИДОВЕ РЕГИСТРИ	**ВИДОВЕ ЛИЧНИ ДАННИ**	**НАПРАВЛЕНИЕ**
1. Регистър „Служители“	Три имена, адрес, телефон, ЕГН, съдимост Хартиен и електронен носител; Предприетите мерки за защита са описани в настоящите правила; Данните се преглеждат на всеки 6 месеца; Предоставянето на трети лица е определено в настоящите Правила.	**„Финансово – счетоводно”**
2. Регистър „Клиенти“	Три имена, адрес, телефон, електронна поща, националност, копие от лична карта (документ за самоличност) Хартиен и електронен носител; Предприетите мерки за защита са описани в настоящите правила; Данните се преглеждат на всеки 6 месеца; Предоставянето на трети лица е определено в настоящите Правила.	**Бек Офис , Нормативно съответствие**

III. ФОРМИ НА ВОДЕНЕ НА РЕГИСТРИТЕ

Чл. 8. Форма на организация и съхраняване на личните данни на хартиен носител:

(1) Папките са разположени в офиса на ИП в специални заключващи се шкафове. Правата и задълженията на служителите са регламентирани в длъжностните им характеристики. Предоставянето, промяната или прекратяването на оторизиран достъп до

регистри се контролира от Изпълнителния директор и Отдел „Нормативно съответствие“ на ИП.

(2) Местонахождението на шкафовете с лични данни на служители и контрагенти е в обособена част от помещение, предназначено за самостоятелна работа на обработващия лични данни.

(3) Носител (форма) за предоставяне на данните от физическите лица -личните данни за всяко лице се набират в изпълнение на нормативно задължение (разпоредбите на закони, подзаконови нормативни актове, кодекси и други) чрез:

- устно интервю с лицето;

- хартиен носител - писмени документи (заявления) по текущи въпроси в процеса на работа, подадени от лицето;

- копия от документи за самоличност, предоставени със съгласието на контрагенти/ клиенти и служители на ИП.

(4) Личните данни от клиенти се подават до ИП, представляван от определени длъжностни лица (брокери и членове на Съвета на директорите).

(5) Възможността за предоставяне другиму (самото лице и оправомощени държавни органи) достъп до личните данни при обработката им е изрично регламентирана в настоящите Вътрешни правила.

Чл. 9. Форма на организация и съхраняване на личните данни на технически носител:

(1) Личните данни (три имена, ЕГН, националност) се въвеждат на твърд диск на сървър от компютърната мрежа (в случай, че се обработват от повече от един служител) или на изолиран компютър (в случай, че се обработват само от един служител или от съответното работно място не може да бъде осигурен достъп до сървър). Компютърът е свързан в локалната мрежа, със защитен достъп до личните данни, с който може да работи само обработващият лични данни при мерки за защита от ниско и средно ниво, съобразно изискванията на Наредба № 1 на КЗЛД.

(2) При работа с данните се използват съответните софтуерни продукти за обработка. Те могат да бъдат адаптирани към специфичните нужди на администратора на лични данни. Данните се въвеждат в компютъра от хартиен носител.

(3) Достъп до файловете за обработка на лични данни имат само работещите с нея. Носители с лични данни могат да се разпространяват, само ако данните са криптирани или ако е използван друг механизъм, гарантиращ, че данните не могат да се четат или променят при пренасянето им.

(4) Местонахождение на сървъра е в помещението на ИП, а резервен сървър за бек-ъп (резервно архивно копие, съгласно изискванията на КФН) на данните се поддържа на отделен сървър. Местонахождение на компютрите е в изолирано помещение за самостоятелна работа на обработващия лични данни по регистъра (работно помещение на отдел „Бек офис“).

(5) Достъп до файловете за обработка на лични данни има само определено от Изпълнителния Директор лице/лица обработващо/и лични данни чрез парола за отваряне на тези файлове, известна на него. При ИП това са служителите на Направление „Бек Офис“.

(6) Защита на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните, както и чрез съхраняване на информацията на хартиен носител. Когато данните се намират на сървър, архивирането им се извършва автоматизирано. Когато данните се намират на изолирани компютри архивирането им се извършва от оператора на съответния компютър (обработващия лични данни).

IV. МЕРКИ ЗА ГАРАНТИРАНЕ НА НИВОТО НА СИГУРНОСТ

Чл. 10. (1) Технически мерки за гарантиране нивото на сигурност:

- компютърните сървъри за база данни на Инвестиционния посредник да са на съвременно техническо ниво.

- компютърните работни конфигурации използват лицензирани операционни системи съобразно изискванията на приложния софтуер за работа с лични данни, те са компетентно балансирани и функционално оптимизирани.

(2) За всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите с лични данни, следва да бъдат осигурени непрекъсваеми токозахранващи устройства (UPS).

(3) Минималния набор от системни програмни средства на всяка работна компютърна конфигурация включва:

1. съвременна операционна система съобразно изискванията на ползвания приложен софтуер с инсталирани пакети за сигурност;
2. антивирусен софтуер с включено автоматично обновяване и постоянно сканиране;
3. активирана защитна стена и деинсталирани комуникатори, осигуряващи достъп извън рамките на компютърната мрежа на ИП и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите.

(4) Достъпът до компютърната мрежа и до софтуера за работа с лични данни се осъществява от длъжностни лица със специални пароли, които се предоставят от служител, отговарящ за компютърно-техническото обезпечаване на ИП, съобразно изискванията на Вътрешни правила на ИП и КФН. Системите регистрират времето на достъп. Забранява се обмена и споделянето на лични пароли или пароли за достъп до системи на ИП между служителите.

(5) Всякакво заличаване, модифициране на лични данни, съхранявани на автоматизирани информационни системи се забранява, освен когато това се прави с цел корекция на грешки или при унищожаване на носители на лични данни от ИП при наличие на законовите условия за унищожаване.

Чл. 11. Физически мерки за гарантиране нивото на сигурност:

(1) В помещенията, в които са разположени компютърни и комуникационни средства, се осигурява:

- система за ограничаване на достъпа;

(2) Всички работните помещения се заключват извън рамките на установеното работно време и достъпът до тях е регламентиран.

(3) Всички магнито-оптични носители, които се използват за запис на лични данни в резултат на архивиране и изготвяне на копия на базите данни, се предават и съхраняват в огнеупорен и водоустойчив шкаф, който се заключва, а ключът се съхранява от „Кадри и ТРЗ“ при ИП. Контролът по използването на тези носители се извършва от изпълнителния директор и вътрешния контрол на ИП.

(4) ИП разполага със специална секретна каса за съхранение на лични данни и магнитни носители с такива данни.

(5) ИП определя зона с контролиран достъп около работните бюра на бек офис служителите и служителят за вътрешен контрол.

(6) ИП разполага с 3 вида пожарогасители, осигуряващи гасене на пожари с вода, прах и газ с оглед потенциални заплахи от пожар. В офиса на ИП има централизирана пожароизвестителна и пожарогасителна система.

(7) Сградата, в която е разположен офиса на ИП, се охранява денонощно и има централизиран контрол на достъпа и видеонаблюдение.

Чл. 12. Организационни мерки за гарантиране нивото на сигурност:

(1) Организира се охрана на работните помещения в рамките на охраната на цялата сграда.

(2) Забранено е използването на преносими лични носители на данни в звената от ИП, в които се обработват лични данни (флаш памети, преносими хардискове и др.).

(3) Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват за служебни цели.

(4) Проверка на всички работни компютърни конфигурации се извършва на всеки 12 месеца от съответно лице, отговарящо за компютърното и техническо обезпечаване на ИП.

(5) Пренасянето на лични данни през (чрез) интернет се забранява, а когато това се осъществява чрез електронна поща, задължително се осигурява криптиране на данните.

(6) При ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни.

(7) Изпълнителният директор на ИП определя обработващите лични данни за различните видове регистри, които се водят в инвестиционния посредник.

(8) ИП осигурява следните основни мерки за персонална защита и по отношение на служителите си осигурява:

1. познаване на нормативната уредба в областта на защитата на личните данни;
2. познаване на вътрешните правила за защита на личните данни;
3. знания за опасностите за личните данни, обработвани от администратора;
4. споделяне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);
5. съгласие за поемане на задължение за неразпространение на личните данни;
6. обучение;
7. тренировка на персонала за реакция при събития, застрашаващи сигурността на данните.

(9) 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”.

(10) Лицата могат да започнат да обработват лични данни след запознаване със:

1. нормативната уредба в областта на защитата на личните данни;
2. политиката и ръководствата за защита на личните данни;
3. опасностите за личните данни, обработвани от администратора.

(11) Служителите на ИП подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

(12) Документалната защита представлява система от организационни мерки при обработването на лични данни на хартиен носител. Основните мерки на документалната защита са:

1. определяне на регистрите, които ще се поддържат на хартиен носител;
2. определяне на условията за обработване на лични данни – лични данни се обработват при сключване на договори с клиенти/контрагенти и при постъпване на работа при ИП. Обработката става в специално отделена част от офиса на ИП от служители от Бек Офис и Фронт Офис;
3. регламентиране на достъпа до регистрите – достъп до регистрите се осъществява от „Бек Офис“ и съответно с отдел „Нормативно съответствие“;
4. контрол на достъпа до регистрите – осъществява се от Изпълнителния Директор и от отдел „Нормативно съответствие“;
5. определяне на срокове за съхранение – съгласно изискванията на ЗПФИ инвестиционният посредник съхранява личните данни за своите клиенти най-малко 5 години от установяване на отношения с клиенти;
6. правила за размножаване и разпространение – лични данни не се размножават и не се разпространяват, освен в предвидените от закона случай към оправомощени държавни институции или към лицата, които са предоставили данните;
7. процедури за унищожаване – носители на лични данни се унищожават от комисия на ИП в състав: член на Съвета на директорите, служител от отдел „Нормативно съответствие“ и служител Бек Офис. Унищожаването става само при наличие на законови предпоставки за това, оценка на регулаторния риск, липса на законови пречки и при съставяне на протокол за унищожаването;
8. процедури за проверка и контрол на обработването – контролът за обработването на личните данни се осъществява от изпълнителния директор и от отдел „Нормативно съответствие“ регулярно и/или инцидентно.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ

Чл. 13. Служителите на ИП са длъжни да спазват и изпълняват Вътрешните правила, в съответствие с длъжностните им характеристики.

Чл. 14. При обработване на личните данни служителят подписва декларация, че е запознат със ЗЗДЛ, както и с настоящите Вътрешни правила.

Чл. 15. (1) Администраторът предоставя лични данни в изпълнение на нормативно установени задължения.

(2) Лични данни се предоставят служебно между служителите в ИП след обосновано искане, в съответствие с функционалните задължение на даден служител или звено и при уведомяване на отдел „Нормативно съответствие“. Искането може и да е в устна форма, когато служебните задължения на лицето налагат обработване на лични данни или когато правото на дъстъп е част от длъжностната характеристика на служителя.

Чл. 16. (1) Всеки клиент (контрагент) на ИП, който е физическо лице има право на достъп до отнасящи се за него лични данни, съхранявани и обработвани при ИП.

(2) Правото на достъп се осъществява с писмено заявление/или заявление по електронен път по реда на Закона за електронните документи и електронния подпис/ до Изпълнителния Директор на ИП или от изрично упълномощено от него лице, чрез нотариално заверено пълномощно. Подаването на заявлението е безплатно.

(4) Заявлението се завежда при ИП.

(5) Достъп до данните на лицето се осигурява под формата на: устна справка; писмена справка; преглед на данните от самото лице или от упълномощеното такова; копие от обработваните лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

(6) При подаване на заявление за осигуряване на достъп до лични данни, представляващият Инвестиционния посредник или упълномощено от него лице, разглеждат заявленията и разпореждат на обработващия лични данни да осигури искания достъп от лицето в предпочитаната от него форма.

(7) Срокът за разглеждане на заявлението и произнасянето по него е 14-дневен от деня на подаването му.

(8) Инвестиционният посредник уведомява писмено заявителя за решението си - то може да бъде за предоставяне на достъп или отказ за достъп. Уведомяването става лично срещу подпис или по пощата с обратна разписка.

(9) Отказът на достъп до лични данни трябва да бъде мотивиран. Основанията за отказ са: 1. когато данните не съществуват; 2. когато данните не могат да бъдат предоставяни на определено правно основание.

Чл. 17. (1) Лични данни се предоставят на трети лица само след получаване на писмено съгласие от лицето, за което се отнасят данните.

(2) При неполучаване на съгласие от лицето или при изричен отказ да се даде съгласие, данните не се предоставят.

(3) Не е необходимо съгласие на лицето в случаите, когато ИП е задължен субект по закон и данните са поискани от държавни органи и институции в рамките на техните правомощия

VI. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ, УПРАВЛЯВАНЕ И РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ

Чл. 18. (1) При възникване и установяване на инцидент веднага се докладва на лицето, отговорно за защита на личните данни;

(2) 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.

(3) След анализ от Изпълнителния директор и от отдел „Нормативно съответствие“ в дневника се записват последствията от инцидента и мерките, които са предприети за отстраняването им.

(4) В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на лицето по защита на личните данни, като това се отразява в дневника по архивиране и възстановяване на данни.

(5) В случаите на компрометирането на парола тя се подменя с нова, като събитието се отразява в дневника за инциденти.

Чл. 19 (1) Всеки служител на ИП се счита уведомен за рисковете при изтичане на лични данни за клиент и за отговорността, която се носи при такова събитие. Рискът от изтичане на лични данни е свързан с нарушаване на личната неприкосновеност на клинт/ контрагент, тъй като така биха станали известни данни за имена, адрес и ЕГН на даден клиент.

(2) Всеки служител на ИП разбира, съгласява се и приема да спазва забраната за неразпространение на лични данни на клиенти и/или контрагенти на ИП, станали му известни при или по повод на изпълняваните функции.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

По смисъла на тези Вътрешни правила:

§1. „Администратор на лични данни” е ИП “ФАКТОРИ” АД представлявано от Изпълнителния директор

§2. „Обработващ лични данни” са длъжностни лица при ИП “ФАКТОРИ” АД.

§3. Вътрешните правила влизат в сила от деня на тяхното приемане от Съвета на директорите на ИП. Неразделна част от тези Правила е оценката на нивото на въздействие на всеки регистър.

§4. Тези Правила са приети с Решение на Съвета на директорите на ИП “ФАКТОРИ” АД на основание чл. 23 от Закона за защита на личните данни.

Всички служители и лица, работещи по договор за ИП, са уведомени за настоящите Правила и за задължението си да ги спазват.