Приложение № 5
Към Правила за обработване и защита на лични данни на управляващо дружество „Конкорд Асет Мениджмънт“ АД

РЕГИСТЪР

НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

НА УПРАВЛЯВАЩО ДРУЖЕСТВО „КОНКОРД АСЕТ МЕНИДЖМЪНТ“ АД

Наименование на Дружеството, представител, длъжностно лице по защита на данните	Цели на обработването	Описание на категориите субекти на данни	Описание на категориите лични данни, които се обработват	Категории получатели, пред които са и ще бъдат разкривани лични данни	Срок за съхраняване на лични данни и за тяхното изтриване	Общо описание на технически и организационни мерки за сигурност

„Конкорд Асет Мениджмънт“ АД е акционерно дружество, учредено в съответствие с Търговския закон, което е вписано в регистъра на търговските дружества при Агенцията по вписванията с ЕИК: 131446496, със седалище и адрес на управление гр. София, район „Възраждане“, бул. „Тодор Александров“ № 117, тел.: 02/ 816 43 70, 02/ 816 43 45, e-mail: office@concord-am.bg; интернет страница: http://concord-am.bg/ . Дружеството притежава лиценз № 1–УД	Целите на обработването на лични данни са свързани с осъществяването на дейността на УД по записване и обратно изкупуване на дялове на договорни фондове (ДФ), администриране на дялове, идентифициране на клиенти и контрагенти (пълномощници), извършване на оценка за подходяща услуга (уместност и целесъобразност),	Субектите на лични данни са разделят на пет категории: **А)** Физически лица - клиенти на Дружеството; **Б)** представляващи клиенти - юридически лица или контрагенти; **В)** пълномощници на клиенти и контрагенти; (Такива контрагенти могат да предоставят следните услуги - набиране на клиенти, доставка	Дружеството обработва следните категории лични данни: **А)** Лични данни на клиенти. Видовете обработвани лични данни на клиенти са описани подробно в Приложение № 4 към Правилата за обработване и защита на лични данни на дружеството. Такива данни са: три имена, ЕГН, адрес, други данни от документа за самоличност – място на раждане, ръст, цвят	Получател на лични данни са държавни органи, установени в ЗПФИ, ЗДКИСДПКИ, ЗППЦК, ЗМИП, КТр., КСО, ДОПК, и при обстоятелствата, съдържащи се в цитираните нормативни актове (ДАНС, НАП, КФН, БНБ, НОИ, Инспекция по труда, Служби по трудова медицина). Обработката на лични данни се извършва от служители на дружеството. Достъп до лични данни може да имат юрисконсулти, адвокати, счетоводители, одитори, риск мениджъри, технически специалисти, поддържащи компютрните системи на	Управляващото дружество съхранява за срок от 5 години всички събрани и изготвени по реда на ЗМИП и правилника за неговото прилагане, ЗДКИСДПКИ, ЗПФИ, актовете по прилагането им, и пряко приложимите регламенти документи, данни и информация. В случаите на установяване на делови взаимоотношения с клиенти, както и в случаите на встъпване в кореспондентски отношения срокът на съхранение започва да	**Технически мерки** за гарантиране нивото на сигурност: а) компютърните сървъри за база данни на УД са на съвременно техническо ниво; б) компютърните конфигурации използват лицензирани операционни системи съобразно изискванията на приложния софтуер за работа с лични данни, те са компетентно балансирани и функционално оптимизирани. 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). Минималния набор от системни програмни средства на всяка компютърна конфигурация, на която се обработват лични данни, 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 УД и създаващи предпоставки за идентифициране на IP адрес на потребителя и за достъп на злонамерен софтуер и мобилен код до компютрите.

от 19.09.2005 г. и лиценз № 46 – УД/21.06.2012 г. за извършване на дейност като управляващо дружество. Лице за контакт за УД „Конкорд Асет Мениджмънт" АД: гр. София – Николай Пламенов Механджийски, Главен юрисконсулт и Ръководител отдел „Нормативно съответствие", e-mail за контакт: mehandzhiyski@concord-am.bg, на който може да се подават жалби и сигнали, свързани с обработването на лични данни.	изпълнение на подадена поръчка за записване/ обратно изкупуване на дялове от ДФ, прехвърляне на дялове от ДФ при дарение или при наследяване, извършване на проверка и контрол на дейността по записване и обратно изкупуване на дялове от ДФ, както и за изпълнение на нормативни или регулаторни изисквания, установени	на финансови услуги, изпълнение на нареждания, счетоводни услуги, консултантски услуги, правни услуги, регистрационни услуги, депозитарни услуги и други, които са относими към предмета на дейноста на Дружеството. **Г)** Кандидати за работа; **Д)** Служители на Дружеството, които предостав	на очите, данни за контакт: телефонен номер, електронна поща, клиентски номер; номер на банкова сметка; данни за притежаваните от клиента финансови инструменти. **Б)** За кандидати за работа се обработват следните видове лични данни – три имена, адрес, дата на раждане, телефонен номер, електронна поща, данни за образование и професиона	„Конкорд Асет Мениджмънт" АД, както и доставчици на информационни услуги за съответните специфични дейности, извършвани от посочените категории лица. Личните данни се предоставят и на банката – депозитар на договорните фондове, както и на депозитарна институция – „Централен депозитар" АД. Със съгласие на клиента „Конкорд Асет Мениджмънт" АД може да предоставя лични данни и на свои партньори или доставчици на финансови услуги. При изпълнение на поръчки от клиенти е възможно лични данни да бъдат предоставени на	тече от началото на календарната година, следваща годината на прекратяването на отношенията. Критерият за посочения срок е законоустановен в чл. 67 ЗМИП. Съгласно чл. 12 от Закона за счетоводството - Счетоводната информация се съхранява на хартиен и/или на технически носител в Дружеството в следните срокове: 1. ведомости за заплати - 50 години, считано от 1 януари на отчетния период,	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 УД, съобразно изискванията на вътрешни правила и КФН. Системите регистрират времето на достъп. Забранява се обмена и споделянето на лични пароли или пароли за достъп до системи на УД между служителите. 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 УД при наличие на законовите условия за унищожаване. УД извършва периодично тестове на системите си за техническа сигурност, за което провежда специализирани технически проверки на всеки 6 месеца с оглед спазване на изискнаията за защина на лични данни. **Физически мерки** за гарантиране нивото на сигурност: В помещенията, в които са разположени компютърни и комуникационни средства, се осигурява система за ограничаване на достъпа; Всички работни помещения се заключват извън

	в ЗДКИСДПКИ, ЗМИП, ЗМФТ, ДОПК, ЗПФИ, ЗКФН, ЗПМСПЗФИ, ЗППЦК, наредби и други актовете по прилагането им, пряко действащите Регламенти и други актове на ЕК, или на други действащи нормативни актове;	ят лични данни въз основа на договора, сключен с Дружеството, законовите изисквания за това, установени в ЗПФИ, Регламент 2017/565, Наредба № 44 на КФН, КТ, КСО, ТЗ, а също и с изричното си съгласие на лицето.	лна квалификация, професионален опит, снимка, място на раждане. **В)** За служители се обработват следните видове лични данни - три имена, адрес, дата на раждане, телефонен номер, електронна поща, данни за образование и професионална квалификация, професионален опит, място на раждане, данни за статус на лицето – осъждан/	контрагенти (брокери), лицензирани в трети държави или в държави от ЕС, когато това се изисква от приложимото за сделката законодателство, и без такова предоставяне не може да се изпълнят договорни задължения по изпълнение на нареждания на сделки с финансови инструменти. „Конкорд Асет Мениджмънт“ АД може да предостави лични данни и на финансови, данъчни, правни или други консултанти. Разкриването на лични данни в този случай се извършва след получаване на съгласие от клиента, освен ако	следващ отчетния период, за който се отнасят; 2. счетоводни регистри и финансови отчети, включително 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; 3. всички останали носители на счетоводна информация - три години, считано от 1 януари на отчетния период, следващ	рамките на установеното работно време и достъпът до тях е регламентиран. 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 Главния счетоводител на УД. Контролът по използването на тези носители се извършва от изпълнителния директор и отдел Нормативно съответствие на УД. УД разполага със специална секретна каса за съхранение на лични данни и магнитни носители с такива данни. УД определя зона с контролиран достъп около работните бюра на бек офис служителите и служителят от отдел Нормативно съответствие и вътрешен контрол. При осъществяване на функциите си, служителите прилагат принципа на „чистото бюро“. УД разполага с пожарогасители, осигуряващи гасене на пожари с вода, прах и газ с оглед потенциални заплахи от пожар. В офиса на УД има централизирана пожароизвестителна и пожарогасителна система. Сградата, в която е разположен офиса на УД, се охранява денонощно и има централизиран контрол на достъпа. **Организационни мерки** за гарантиране нивото на сигурност:

			неосъждан (когато това се изисква от нормативен акт), ръст, цвят на очи и други данни от документа за самоличност, данни за здравословно състояние, данни за изплатени обезщетения, финансово състояние. Обхващат законово изискуемите събирани и обработвани лични данни по ЗМИП, ППЗМИП, ДОПК, ЗДКИСДПКИ, ЗКФН, ЗПФИ, ЗПМСПЗФИ, наредби на КФН, КТр., КСО, други	не е налице легитимен интерес на дружеството или трето лице, съобразно изискванията на Регламент 2016/679.	отчетния период, за който се отнасят. Счетоводната информация може да се съхранява в частни или държавни архиви по реда на Закона за Националния архивен фонд при спазване на изискванията по ЗСч. След изтичането на срока за съхранението им носителите на счетоводна информация (хартиени или технически), които не подлежат на предаване в Националния архивен фонд или в Националния осигурителен институт,	Организира се охрана на работните помещения в рамките на охраната на цялата сграда. Забранено е използването на преносими лични носители на данни в звената от УД, в които се обработват лични данни (флаш памети, преносими хардискове и др.). Работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват за служебни цели. Проверка на всички работни компютърни конфигурации се извършва на всеки шест месеца от съответно лице, отговаряща за компютърното и техническо обезпечаване на УД. Пренасянето на лични данни през (чрез) интернет се забранява, а когато това се осъществява чрез електронна поща, задължително се осигурява техническа защита на данните.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. Изпълнителният директор на УД определя обработващите лични данни за различните видове регистри, които се водят в УД. УД осигурява **следните основни мерки за персонална защита** и по отношение на служителите си осигурява: а) познаване на норма-

			пряко приложими Регламенти на ЕК и нормативни актове, както и изискуеми съгласно подзаконови актове на КФН и Насоки на ESMA и EBA		могат да се унищожават. Съгласно Кодекса на труда - Трудовото досие на работника или служителя се създава при постъпване на работа и в него се съхраняват документите във връзка с възникването, съществуването, изменението и прекратяването на трудовото правоотношение.	тивната уредба в областта на защитата на личните данни; б) познаване на вътрешните процедури за защита на личните данни; в) знания за опасностите за личните данни,обработвани от администратора; г) несподеляне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.); д) съгласие за поемане на задължение за неразпространение на личните данни; е) обучение; ж) тренировка на персонала за реакция при събития, застрашаващи сигурността на данните. 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". Служителите могат да обработват лични данни след запознаване с: а) нормативната уредба в областта на защитата на личните данни; б) процедурите и ръководствата за защита на личните данни; в) опасностите за личните данни, обработвани от администратора. Служителите на УД подписват декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си. **Документалната защита** предста-

						влява система от организационни мерки при обработването на лични данни на хартиен носител. Унищожаване е допустимо и в хипотезите на Регламент 2016/679, ако това не противоречи на други действащи и относими към дейността на УД нормативни актове. Подробно описание на всички технически, организационни и персонални мерки за сигурност се съдържат в Приложение № 2 към Правилата за обработване и защита на личните данни.