

ПРАВИЛА
ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ
НА УПРАВЛЯВАЩО ДРУЖЕСТВО „КОНКОРД АСЕТ МЕНИДЖМЪНТ“ АД

I. ОБЩИ РАЗПОРЕДБИ И ПРИНЦИПИ

Чл. 1 (1). Настоящите правила се приемат на основание чл. 24, параграф 2 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Регламент 2016/679).

(2) Правилата се изготвят и прилагат с оглед обхвата, мащаба и комплексността на извършваните услуги и дейности от управляващо дружество (УД) „Конкорд Асет Мениджмънт“ АД (наричано по-долу Дружеството или Администраторът) и притежавания от него лиценз.

(3) Настоящите правила се прилагат както спрямо служителите на Дружеството, така и спрямо неговите клиенти, ползващи съответните услуги.

(4) По смисъла на чл. 4, т. 7 от Регламент (ЕС) 2016/679 и настоящите правила Дружеството се явява администратор на лични данни - юридическо лице, което само или съвместно с други определя целите и средствата за обработването на лични данни.

(5) (изм. с решение на СД от 21.11.2018 г.) „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 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.

(6) Целите на обработването на лични данни са свързани с идентифицирането на клиенти и контрагенти на Дружеството съгласно Закон за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране (ЗДКИСДПКИ), извършване на оценка за подходяща услуга (уместност и целесъобразност), сключване и изпълнение на договор/ поръчка за записване/ обратно изкупуване на дялове от договорни фондове (ДФ), упражняване на правото на наследяване на дялове от ДФ, както и за изпълнение на нормативните изисквания, установени в Закона за мерките срещу изпиране на пари (ЗМИП), Закона за мерките срещу финансиране на тероризма (ЗМФТ), Закона за Комисия за финансов надзор (ЗКФН), Закона за публичното предлагане на ценни книжа (ЗППЦК), Закона за пазарите на финансови инструменти (ЗПФИ), Данъчно – осигурително процесуален кодекс (ДОПК), или в нормативни актове по прилагането им.

Чл. 2 (1) Дружеството с оглед извършваната от него дейност и в качеството си на администратор гарантира, че спрямо личните данни се прилагат следните принципи:

а) личните данни са обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“);

б) личните данни са събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели („ограничение на целите“);

в) личните данни подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);

г) личните данни са точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност“);

д) личните данни са съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението“);

е) личните данни са обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

(2) Служителите на Дружеството, които обработват лични данни, преминават първоначално и периодични обучения относно приложимите правни норми и правила по защита на личните данни.

Чл. 3 (1) Водещ принцип при обработването на лични данни е законосъобразността.

(2) Обработването е законосъобразно, само ако и доколкото е приложимо поне едно от следните условия:

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни 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 законово задължение, което се прилага спрямо администратора;

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, които са предоставени на администратора;

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

II. ДАВАНЕ НА СЪГЛАСИЕ

Чл. 4 (1) Когато обработването се извършва въз основа на съгласие, „Конкорд Асет Мениджмънт“ АД винаги следва да е в състояние да докаже, че субектът на данни е дал съгласие за обработване на личните му данни.

(2) „Съгласие на субекта на данните“ означава 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.

(3) Ако съгласието на субекта на данните е дадено в рамките на писмена декларация, която се отнася и до други въпроси, искането за съгласие се представя по начин, който ясно да го отличава от другите въпроси, в разбираема и лесно достъпна форма, като използва ясен и прост език. Някоя част от такава декларация не може да е в нарушение на Регламент 679/2016 и при противоречие тя не е обвързваща.

(4) Субектът на данни има правото да оттегли съгласието си по всяко време. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Преди да даде съгласие, субектът на данни бива информиран за това.

(5) Дружеството не предлага услуги на лица под 18 години, поради което не събира и не обработва лични данни на такива лица, независимо от волята на лицето. Възможно е Дружеството да събере и обработва лични данни на лица под 18 години, или на лица, поставени под запрещение, при извършване на дейността по прехвърляне на дялове от ДФ при наследяване и дарение. При тези случаи обработването се извършва едва след като Дружеството е получило съгласие по реда, предвиден в настоящите правила, от упражняващ родителските права родител или настойник.

III. ОБРАБОТВАНЕ НА СПЕЦИАЛНИ КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 5. (1) Дружеството не обработва лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

(2) Забранява се на всички служители и лица, работещи по договор за него, или негови партньори да обработват лични данни, посочени в ал. 1 по - горе.

Чл. 6 (1) Разпоредбата на чл. 5 не се прилага, ако е налице едно от следните условия:

- а) субектът на данни е дал своето изрично съгласие за обработването на тези лични данни за една или повече конкретни цели, освен когато в правото на ЕС, действащото право на Република България или правото на държава членка се предвижда, че посочената в чл. 5 забрана не може да бъде отменена от субекта на данни;
- б) обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на Дружеството администратор или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила, дотогава, доколкото това е разрешено от правото на Съюза или правото на държава членка, или съгласно колективна договореност в съответствие с правото на държава членка, в което се предвиждат подходящи гаранции за основните права и интересите на субекта на данните;
- в) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;
- г) обработването се извършва при подходящи гаранции в хода на законните дейности на фондация, сдружение или друга структура с нестопанска цел, с политическа, философска, религиозна или синдикална цел, при условие че обработването е свързано единствено с членовете или бившите членове на тази структура или с лица, които поддържат редовни контакти с нея във връзка с нейните цели, и че личните данни не се разкриват без съгласието на субектите на данните;
- д) обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;
- е) обработването е необходимо с цел установяване, упражняване или защита на правни претенции или винаги, когато съдилищата действат в качеството си на правораздаващи органи;
- ж) обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните;
- з) обработването е необходимо за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или социални грижи въз основа на правото на Съюза или правото на държава членка или съгласно договор с медицинско лице.

Обработването по тази буква може да се извършва, когато въпросните данни се обработват от или под ръководството на професионален служител, обвързан от задължението за професионална тайна по силата на правото на Съюза или правото на държавата членка или правилата, установени от националните компетентни органи или от друго лице, също обвързано от задължение за тайна по силата на правото на Съюза или правото на държавата членка или правилата, установени от националните компетентни органи.

и) обработването е необходимо от съображения от обществен интерес в областта на общественото здраве, като защитата срещу сериозни трансгранични заплахи за здравето или осигуряването на високи стандарти за качество и безопасност на здравните грижи и лекарствените продукти или медицинските изделия, въз основа на правото на Съюза или правото на държава членка, в което са предвидени подходящи и конкретни мерки за гарантиране на правата и свободите на субекта на данните, по-специално опазването на професионална тайна;

й) обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните.

Чл. 7. (1) Събирането на лични данни, свързани с присъди и нарушения или със свързаните с тях мерки за сигурност се извършва само за служители на Дружеството, за заемането на чиито позиции се изисква събирането и съхраняването на такива данни от действащото законодателство в

Република България (закони, подзаконовни нормативни актове, регламенти, наредби на регулаторни органи и други).

(2) Категорията такива служители са членовете на управителни и контролни органи, както и заемащите позиции по нормативно съответствие, управление на риска, ръководители на специализирана служба по ЗМИП, главен счетоводител, вътрешен одитор, лицата, които пряко и непосредствено подписват договори с клиенти от името и за сметката на Дружеството.

IV. ИНФОРМАЦИЯ, ПРЕДОСТАВЯНА ПРИ СЪБИРАНЕ НА ЛИЧНИ ДАННИ НА СУБЕКТА НА ДАННИТЕ

Чл. 8 (1). Когато лични данни, свързани с даден субект се събират от него, то в момента на получаване на личните данни Дружеството предоставя на субекта на данните цялата посочена по-долу информация:

- а) данните, които идентифицират Дружеството-администратор и координатите за връзка с него и, когато е приложимо, тези на представителя на Дружеството;
- б) координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;
- в) целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;
- г) когато обработването е необходимо за целите на легитимните интереси на Дружеството или на трета страна, се посочват законните интереси, преследвани от Дружеството или от третата страна;
- д) получателите или категориите получатели на личните данни, ако има такива;
- е) когато е приложимо, намерението на Дружеството да предаде личните данни на трета държава или на международна организация.

Чл. 9 (1). Освен информацията, посочена в чл. 8, ал. 1, в момента на получаване на личните данни Дружеството предоставя на субекта на данните следната допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване:

- а) срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок. Управляващото дружество съхранява личните данни на субект за целия срок на съществуване на отношенията между страните и 5 години след прекратяването им.
- б) съществуването на право да се изиска от Дружеството достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или право да се направи възражение срещу обработването, както и правото на преносимост на данните;
- в) когато обработването се основава на предоставено съгласие от субекта, съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено.
- г) правото на жалба до надзорен орган.
- д) дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последици, ако тези данни не бъдат предоставени. Субектите на лични данни, чиито данни се събират и обработват от Дружеството, се считат уведомени за това обстоятелство с текстове в Общите условия или договорите, сключвани с клиенти и/или контрагенти и за факта, че отказът им да предоставят своите лични данни, изискуеми по ЗПФИ и ЗМИП/ППЗМИП е законово основание Дружеството да откаже предоставянето на съответната търсена услуга.
- е) съществуването на автоматизирано вземане на решения, включително профилиране и съществена информация относно използваната логика, както и значението и предвидените последици от това обработване за субекта на данните.

(2) Когато Дружеството възнамерява по-нататък да обработва личните данни за цел, различна от тази, за която са събрани, то предоставя на субекта на данните преди това по-нататъшно обработване информация за тази друга цел и всякаква друга необходима информация. На субекта на данните се предоставя информация за целта на това последващо обработване преди то да е извършено. Дружеството може да обработва личните данни на клиентите си за целите установени в ЗДКИСДПКИ, ЗПФИ, ЗППЦК, ЗМИП, ППЗМИП, ДОПК, нормативни актове по прилагането им, както и други пряко приложими нормативни актове или актове на европейското право, уреждащи дейността му. Това са нормативно-установени задължения за Дружеството, чието спазване е задължително за извършването на дейност и предоставянето на услуги от управляващо дружество.

(3) Дружеството предоставя информацията, посочена в чл. 8 и 9 по-горе:

- а) в разумен срок след получаването на личните данни, но не по-късно от един месец, като се отчитат конкретните обстоятелства, при които личните данни се обработват;
- б) ако данните се използват за връзка със субекта на данните, най-късно при осъществяване на първия контакт с този субект на данните; или
- в) ако е предвидено разкриване пред друг получател, най-късно при разкриването на личните данни за първи път.

(4) Описание на конкретната информация по чл. 8 и 9, касаеща дейността на УД е посочена в Приложения № 3 и 4 към настоящите Правила и се предоставя на клиенти и контрагенти срещу подпис или по подходящ начин с оглед установените отношения с насрещната страна.

Чл. 10. (1) Изискванията на чл. 8 и 9 не се прилагат, когато субектът на данните вече разполага с информацията.

(2) Изискванията на чл. 9 не се прилагат, когато и доколкото:

- а) субектът на данните вече разполага с информацията;
- б) предоставянето на такава информация се окаже невъзможно или изисква несъразмерно големи усилия;
- в) получаването или разкриването е изрично разрешено от правото на Европейския съюз или правото на държава – членка, което се прилага спрямо Дружеството и в което се предвиждат същите подходящи мерки за защита на легитимните интереси на субекта на данните;
- г) личните данни трябва да останат поверителни при спазване на задължението за опазване на професионална тайна, което се урежда от правото на Европейския съюз или правото на държава – членка, включително законово задължение за поверителност.

V. ПРОЗРАЧНОСТ И УСЛОВИЯ ЗА ПРОЗРАЧНОСТ

Чл. 11 (1). Дружеството-администратор предприема необходимите мерки за предоставяне на всякаква информация по чл. 13 и 14 и на всяка комуникация по чл. 15-22 и чл. 34 от Регламента, която се отнася до обработването, на субекта на данните в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език. Информацията се предоставя писмено или по друг начин, включително, когато е целесъобразно, с електронни средства.

(2) Ако субектът на данните е поискал това, информацията може да бъде дадена устно, при положение че идентичността на субекта на данните е доказана с други средства. Предоставянето на информацията по този начин се документира надлежно от служител на дружеството, чрез съставяне на писмен протокол, който се подписва и от субекта на данните.

Чл. 12 (1). Дружеството предоставя на субекта на данни информация относно действията, предприети във връзка с искане по 15-22 от Регламента, без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането.

(2) При необходимост срокът по ал. 1 може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията. Администраторът информира субекта на данните за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е поискал друго.

Чл. 13. Ако Дружеството не предприеме действия по искането на субекта на данни, то уведомява субекта на данни без забавяне и най-късно в срок от един месец от получаване на искането за причините да не предприеме действия и за възможността за подаване на жалба до надзорен орган и търсене на защита по съдебен ред.

Чл. 14. (1) Информацията по чл. 13 и 14 и всяка комуникация и действия по чл. 15-22 и чл. 34 от Регламента се предоставят безплатно. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повтораемост, Дружеството може или:

- а) да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия, или
- б) да откаже да предприеме действия по искането.

(2) Дружеството носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.

(3) Когато Дружеството има основателни опасения във връзка със самоличността на физическото лице, което подава искане за право на достъп, коригиране, изтриване, ограничаване на обработката или възражение по отношение на лични данни, Дружеството може да поиска предоставянето на допълнителна информация, необходима за потвърждаване на самоличността на субекта на данните.

VI. ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ

Чл. 15 (1). Право на достъп на субекта на данните. Субектът на данните има право да получи от Дружеството потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация:

- а) целите на обработването;
- б) съответните категории лични данни;
- в) получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави или международни организации;
- г) когато е възможно, предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;
- д) 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;
- е) правото на жалба до надзорен орган;
- ж) когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;
- з) съществуването на автоматизирано вземане на решения, включително профилирането и в тези случаи съществена информация относно използваната логика, както и значението и предвидените последици от това обработване за субекта на данните.

(2) Когато личните данни се предават на трета държава или на международна организация, субектът на данните има право да бъде информиран относно подходящите гаранции във връзка с предаването.

(3) Дружеството предоставя копие от личните данни, които са в процес на обработване. За допълнителни копия, поискани от субекта на данните, Дружеството може да наложи разумна такса въз основа на административните разходи. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя в широко използвана електронна форма, освен ако субектът на данни не е поискал друго.

(4) При предоставянето на копие от лични данни, Дружеството не може да разкрива следните категории данни:

- а) лични данни на трети лица, освен ако същите не са изразили изрично си съгласие за това;
- б) данни, които представляват търговска тайна, интелектуална собственост или конфиденциална информация;
- в) друга информация, която е защитена от действащото законодателство.

(5) Предоставянето на достъп на субекта на данни по настоящия чл. 15 не може да влияе неблагоприятно върху правата и свободите на други лица

Чл. 16. (1) Право на коригиране. Субектът на данни има право да поиска от Дружеството да коригира без ненужно забавяне неточните лични данни, свързани с него. Като се имат предвид целите на обработването субектът на данните има право непълните лични данни да бъдат попълнени, включително чрез добавяне на декларация.

(2) В случаите, когато искане за коригиране от субект на данните бъде удовлетворено, Дружеството уведомява останалите получатели, на които данните са били разкрити, така че да отразят изменението.

Чл. 17. (1) Право на изтриване (право „да бъдеш забравен“) Субектът на данни има правото да поиска от Дружеството изтриване на свързаните с него лични данни без ненужно забавяне, а Дружеството има задължението да изтрие без ненужно забавяне личните данни, когато е приложимо някое от посочените по-долу основания:

- а) личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
- б) субектът на данните оттегля своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването;

- в) субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество;
- г) личните данни са били обработвани незаконосъобразно;
- д) личните данни трябва да бъдат изтрети с цел спазването на правно задължение по правото на ЕС, правото на Република България или правото на държава членка, което се прилага спрямо Дружеството.

(2) Когато “Конкорд Асет Мениджмънт” АД е направил личните данни обществено достояние и е задължен да изтрие личните данни, то, като отчита наличната технология и разходите по изпълнението, 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) Разпоредбите на ал. 1 и 2 не се прилагат, доколкото обработването е необходимо за:

- а) упражняване на правото на свобода на изразяването и правото на информация;
- б) спазване на правно задължение, което изисква обработване, предвидено в правото на ЕС, действащото законодателство на Република България или правото на държавата членка, което се прилага спрямо Дружеството или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;
- в) причини от обществен интерес в областта на общественото здраве;
- г) целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;
- д) установяването, упражняването или защитата на правни претенции.

Чл. 18 (1) Право на ограничаване на обработването. Субектът на данните има право да изиска от Дружеството ограничаване на обработването, когато се прилага едно от следното:

- а) точността на личните данни се оспорва от субекта на данните, за срок, който позволява на Дружеството да провери точността на личните данни;
- б) обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрети, а изисква вместо това ограничаване на използването им;
- в) Дружеството не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;
- г) субектът на данните е възразил срещу обработването в очакване на проверка дали законните основания на Дружеството имат преимущество пред интересите на субекта на данните.

(2) Когато обработването е ограничено съгласно ал. 1, такива данни се обработват, с изключение на тяхното съхранение, само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции или за защита на правата на друго физическо лице или поради важни основания от обществен интерес за ЕС, Република България или държава членка.

Чл. 19. Дружеството съобщава за всяко извършено в съответствие с чл. 16, чл. 17, ал. 1 и чл.18 по – горе коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Дружеството информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

Чл. 20 (1) Право на преносимост на данните. Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на Дружеството, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от Дружеството, на когото личните данни са предоставени, когато:

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

(2) Когато упражнява правото си на преносимост на данните по ал. 1, субектът на данните има право да получи пряко прехвърляне на личните данни от един администратор към друг, когато това е технически осъществимо.

(3) Упражняването на правото, посочено в ал. 1 от настоящия член не засяга чл. 17 по -горе. Посоченото право не се отнася до обработването, необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на Дружеството.

Чл. 21 (1) Право на възражение. Субектът на данните има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него, което се основава на:

а) обработване, което е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора или

б) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, включително профилиране, основаващо се на посочените основания.

Дружеството прекратява обработването на личните данни в случаите по настоящата алинея, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

(2) Когато се обработват лични данни за целите на директния маркетинг, субектът на данни има право по всяко време да направи възражение срещу обработване на лични данни, отнасящо се до него за този вид маркетинг, което включва и профилиране, доколкото то е свързано с директния маркетинг.

(3) Когато субектът на данни възрази срещу обработване за целите на директния маркетинг, обработването на личните данни за тези цели се прекратява.

(4) Най-късно в момента на първото осъществяване на контакт със субекта на данните, той изрично се уведомява за съществуването на правото по ал. 1 и 2, което му се представя по ясен начин и отделно от всяка друга информация.

(5) Субектът на данните може да упражнява правото си на възражение чрез автоматизирани средства, като се използват технически спецификации.

Чл. 22. (1) Право на човешка намеса при автоматизирано вземане на решения. Субектът на данните има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последици за него или по подобен начин го засяга в значителна степен.

(2) Разпоредбата на ал. 1 не се прилага, ако решението:

а) е необходимо за сключването или изпълнението на договор между субекта на данни и администратора („Конкорд Асет Мениджмънт” АД);

б) е разрешено от правото на ЕС, действащото законодателство на Република България или правото на държава членка, което се прилага спрямо Дружеството, и в което се предвиждат също подходящи мерки за защита на правата и свободите, и легитимните интереси на субекта на данните; или

в) се основава на изричното съгласие на субекта на данни.

(3) В случаите, посочени в ал. 2, букви а) и в), „Конкорд Асет Мениджмънт” АД прилага подходящи мерки за защита на правата и свободите и легитимните интереси на субекта на данните, най-малко правото на човешка намеса от страна на администратора, правото да изрази гледната си точка и да оспори решението.

(4) Решенията по ал. 2 не се основават на специалните категории лични данни, посочени в член 9, параграф 1 от Регламент 2016/679, освен ако не се прилага член 9, параграф 2, буква а) или буква ж) от същия Регламент и не са въведени подходящи мерки за защита на правата и свободите и легитимните интереси на субекта на данните.

VII. ОБЩИ ЗАДЪЛЖЕНИЯ И ОТГОВОРНОСТ НА ДРУЖЕСТВОТО В КАЧЕСТВОТО МУ НА АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ

Чл. 23 (1). Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, „Конкорд Асет Мениджмънт” АД въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с Регламент 2016/679. Тези мерки се преразглеждат и при необходимост се актуализират от Съвета на директорите (СД).

(2) Конкретните технически мерки за защита и обработване на лични данни са описани в Приложение към настоящите Правила.

(3) Пропорционално на дейностите по обработване, посочените в ал.1 мерки „Конкорд Асет Мениджмънт” АД прилага на подходящи политики за защита на данните.

Чл. 24 (1). Като взема предвид:

- а) достиженията на техническия прогрес,
- б) разходите за прилагане и естеството, обхвата, контекста и целите на обработването,
- в) породените от обработването рискове с различна вероятност и
- г) тежестта за правата и свободите на физическите лица,

Дружеството въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки.

(2) Мерките по ал. 1 са разработени с оглед на ефективното прилагане на принципите за защита на данните, (например свеждане на данните до минимум) и интегриране на необходимите гаранции в процеса на обработване, за да се спазват изискванията на Регламент 2016/679 и да се осигури защита на правата на субектите на данни.

(3) Дружеството въвежда подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. По-специално, подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице личните данни не са достъпни за неограничен брой физически лица.

Чл. 25 Когато „Конкорд Асет Мениджмънт“ АД (администратор на лични данни) има бизнес отношения с друго дружество, което не е установено в Европейския съюз, но от общите им делови отношения се налага да се обработват лични данни на лица от ЕС, то управляващото дружество изисква данни за:

- а) представителя на партньорското Дружество, който отговаря за дейността в ЕС и за защита на личните данни;
- б) сведения дали обработването на лични данни няма да е спорадично;

Чл. 26 (1) Когато обработването се извършва от името на „Конкорд Асет Мениджмънт“ АД, то „Конкорд Асет Мениджмънт“ АД може да 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 Регламент 2016/679 и да осигурява защита на правата на субектите на данни.

(2) „Конкорд Асет Мениджмънт“ АД осигурява че обработващият данни не включва друг обработващ данни без предварителното конкретно или общо писмено разрешение на „Конкорд Асет Мениджмънт“ АД. В случай на общо писмено разрешение, „Конкорд Асет Мениджмънт“ АД осигурява че обработващият данни винаги ще информира Дружеството за всякакви планирани промени за включване или замяна на други лица, обработващи данни, като по този начин дава възможност на Дружеството да оспори тези промени.

(3) Обработването от страна на обработващия лични данни се урежда с договор или с друг правен акт съгласно правото на ЕС, на Република България или правото на друга държава членка, който е задължителен за обработващия лични данни спрямо „Конкорд Асет Мениджмънт“ АД, и който регламентира 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 „Конкорд Асет Мениджмънт“ АД. В този договор или друг правен акт се предвижда по-специално, че обработващият лични данни:

- а) обработва личните данни само по документирано нареждане на Дружеството, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това по силата на правото на ЕС, правото на Република България или правото на държава членка, което се прилага спрямо обработващия лични данни, като в този случай обработващият лични данни информира Дружеството за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес;
- б) гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;
- в) взема всички необходими технически мерки съгласно член 32 от Регламент 2016/679;
- г) спазва условията по ал. 2 и 4 за включване на друг обработващ лични данни;
- д) като взема предвид естеството на обработването, подпомага Дружеството, доколкото е възможно, чрез подходящи технически и организационни мерки при изпълнението на задължението на „Конкорд Асет Мениджмънт“ АД да отговори на искания за упражняване на предвидените в Регламент 2016/679 и настоящите правила права на субектите на данни;
- е) подпомага Дружеството да гарантира изпълнението на задълженията за сигурност на обработването, уведомяване на надзорни органи, оценка на въздействието и предварителни

консултации, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни;

ж) по избор на Дружеството заличава или връща на „Конкорд Асет Мениджмънт“ АД всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на Съюза, Република България или правото на държава членка не изисква тяхното съхранение;

з) осигурява достъп на „Конкорд Асет Мениджмънт“ АД 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 Дружеството или друг одитор, оправомощен от Дружеството.

С оглед предвиденото в буква „з“ по – горе, „Конкорд Асет Мениджмънт“ АД осигурява, че обработващият лични данни незабавно ще уведоми „Конкорд Асет Мениджмънт“ АД, ако според него дадено нареждане нарушава Регламент 2016/679 или други разпоредби на Съюза, правото на Република България или на държавите членки относно защитата на данни.

(4) „Конкорд Асет Мениджмънт“ АД осигурява, че когато първоначалният обработващ лични данни включва друг обработващ лични данни за извършването на специфични дейности по обработване от името на Дружеството, чрез договор или друг правен акт съгласно правото на Съюза, на Република България или правото на държава членка, на това друго лице се налагат същите задължения за защита на данните, както задълженията, предвидени в договора или друг правен акт между „Конкорд Асет Мениджмънт“ АД и обработващия лични данни, както е посочено в ал. 3, по-специално да предостави достатъчно гаранции за прилагане на подходящи технически и организационни мерки, така че обработването да отговаря на изискванията на Регламент 2016/679. „Конкорд Асет Мениджмънт“ АД осигурява, че когато другият обработващ лични данни не изпълни задължението си за защита на данните, първоначалният обработващ данните продължава да носи пълна отговорност пред „Конкорд Асет Мениджмънт“ АД за изпълнението на задълженията на този друг обработващ лични данни.

(5) Придържането на обработващия лични данни към одобрен кодекс за поведение или одобрен механизъм за сертифициране може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно ал. 1 и 4 от настоящия член.

(6) Без да се засягат разпоредбите на индивидуален договор между „Конкорд Асет Мениджмънт“ АД и обработващия лични данни, договорът или другият правен акт, посочени в ал. 3 и 4 от настоящия член, може да се основават изцяло или отчасти на стандартни договорни клаузи, включително когато са част от сертифициране, предоставено на Дружеството или обработващия лични данни.

(7) Договорът или другият правен акт, посочен в ал. 3 и 4, се изготвят в писмена форма, включително в електронна форма.

Чл. 27. (1) В случаите, когато „Конкорд Асет Мениджмънт“ АД заедно с друг администратор съвместно определя целите и средствата на обработването на лични данни (съвместни администратори) дружеството осигурява, че двамата администратори ще определят по прозрачен начин съответните си отговорности при изпълнение на задълженията си по Регламент 2016/679, и по – специално що се отнася до правата, които има субекта на данните, и съответните им задължения за предоставяне на информацията по чл. 13 и 14 от Регламент 2016/679. Отношенията между съвместните администратори се уреждат със споразумение, освен ако и доколкото съответните отговорности между тях не са определени от правото на Европейския съюз и правото на държава членка, което се прилага спрямо администраторите. В споразумението може да се посочи и обща точка за контакт за субектите на данни.

(2) „Конкорд Асет Мениджмънт“ АД следва да осигури, че споразумението по предходната ал. 1 надлежно урежда съответните роли и връзка на съвместните администратори спрямо субектите на данни. „Конкорд Асет Мениджмънт“ АД осигурява на субекта на данните информация за съществените елементи на споразумението.

(3) Независимо от условията на споразумението между съвместните администратори, субектът на данните може да упражнява правата си по Регламент 2016/679 по отношение на всеки и срещу всеки от администраторите.

Чл. 28. Обработващият лични данни и всяко лице, действащо под ръководството на „Конкорд Асет Мениджмънт“ АД или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на „Конкорд Асет Мениджмънт“ АД, освен ако обработването не се изисква от правото на Съюза или правото на държава членка.

VIII. РЕГИСТРИ НА ДЕЙНОСТИТЕ ПО ОБРАБОТВАНЕ. ИЗКЛЮЧЕНИЯ

Чл. 29 (1) „Конкорд Асет Мениджмънт” АД в качеството му на администратор на лични данни, поддържа регистър на дейностите по обработване, за които отговоря. Този регистър съдържа цялата по-долу посочена информация:

- а) името и координатите за връзка на Дружеството и — когато това е приложимо — на всички съвместни администратори, на представителя на Дружеството-администратор и на длъжностното лице по защита на данните, ако има такива;
- б) целите на обработването;
- в) описание на категориите субекти на данни и на категориите лични данни;
- г) категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;
- д) когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни - документация за подходящите гаранции;
- е) когато е възможно, предвидените срокове за изтриване на различните категории данни;
- ж) когато е възможно, общо описание на техническите и организационни мерки за сигурност.

(2) В случаите, когато „Конкорд Асет Мениджмънт” АД действа като обработващ на лични данни и — когато това е приложимо — представителят на дружеството като обработващ лични данни, поддържа регистър на всички категории дейности по обработването, извършени от името на администратора, съгласно договор сключен с него. В регистъра се съдържат:

- а) името и координатите за връзка на обработващия или обработващите лични данни и на Дружеството, от чието име действа обработващият лични данни и — когато това е приложимо — на представителя на Дружеството или обработващия лични данни и на длъжностното лице по защита на данните;
- б) категориите обработване, извършвано от името на Дружеството;
- в) когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни - документация за подходящите гаранции;
- г) когато е възможно, общо описание на техническите и организационни мерки за сигурност.

(3) Регистрите, посочени в ал. 1 и 2, се поддържат в писмена форма, включително в електронен формат.

(4) При поискване, Дружеството и — когато това е приложимо — представителят на Дружеството, осигуряват достъп до регистъра на надзорния орган.

(5) Задълженията, посочени в ал. 1 и 2, не се прилагат когато дружеството е с по-малко от 250 служители, освен ако има вероятност извършването от тях обработване да породи риск за правата и свободите на субектите на данни, ако обработването не е спорадично или включва специални категории данни по Регламент 2016/679.

IX. СИГУРНОСТ НА ЛИЧНИТЕ ДАННИ

Чл. 30 (1) Като се вземат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, Дружеството и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, *inter alia*, когато е целесъобразно:

- а) псевдонимизация и криптиране на личните данни;
- б) способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;
- в) способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;
- г) процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

(2) При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

(3) Придържането към одобрен кодекс за поведение или одобрен механизъм за сертифициране, съобразно правилата на Регламент 2016/679 може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно ал. 1 от настоящия член.

(4) Дружеството предприема стъпки всяко физическо лице, действащо под негово ръководство, което има достъп до лични данни, да обработва тези данни само по указание на Дружеството, освен ако от въпросното лице не се изисква да прави това по силата на правото на ЕС, приложимото право на Република България или правото на държава членка.

Чл. 31 (1) В случай на нарушение на сигурността на личните данни „Конкорд Асет Мениджмънт” АД, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрало за него, уведомява за нарушенията на сигурността на личните данни компетентния надзорен орган, освен ако не съществува вероятност нарушенията на сигурността на личните данни да породят риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

(2) „Конкорд Асет Мениджмънт” АД осигурява че обработващите лични данни ще уведомяват дружеството без ненужно забавяне, след като узнаят за нарушаване на сигурността на лични данни.

(3) В уведомлението, посочено в ал. 1, се съдържа най-малко следното:

- а) описание на естеството на нарушенията на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
- б) 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;
- в) описание на евентуалните последици от нарушенията на сигурността на личните данни;
- г) описание на предприетите или предложените от Дружеството мерки за справяне с нарушенията на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

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

(5) „Конкорд Асет Мениджмънт” АД документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушенията на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Документирането се извършва посредством съставяне на протокол, който се подписва от изпълнителния директор на дружеството и ръководителят на отдел „Нормативно съответствие“.

Чл. 32 (1) Когато има вероятност нарушенията на сигурността на личните данни да породят висок риск за правата и свободите на физическите лица, „Конкорд Асет Мениджмънт” АД, без ненужно забавяне, съобщава на субекта на данните за нарушенията на сигурността на личните данни.

(2) В съобщението до субекта на данните, посочено в ал. 1 от настоящия член, на ясен и прост език се описва естеството на нарушенията на сигурността на личните данни и се посочват най-малко информацията и мерките, посочени в член 31, ал. 3, букви б), в) и г) по-горе.

(3) Посоченото в ал. 1 съобщение до субекта на данните не се изисква, ако някое от следните условия е изпълнено:

- а) „Конкорд Асет Мениджмънт” АД е предприело подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушенията на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;
- б) „Конкорд Асет Мениджмънт” АД е взело впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни, посочен в ал. 1 по-горе;
- в) съобщаването 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.

Чл.33 (1) Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породят висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, „Конкорд Асет Мениджмънт” АД извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. В една оценка може да

бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове.

(2) При извършването на оценка на въздействието върху защитата на данните „Конкорд Асет Мениджмънт“ АД иска становището на длъжностното лице по защита на данните.

(3) Оценката на въздействието върху защитата на данните, посочена в ал. 1, се изисква по-специално в случай че:

а) налице е систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице;

б) мащабно обработване на специални категории данни, посочени в член 9, параграф 1 от Регламент 2016/679 или на лични данни за присъди и нарушения по член 10 от Регламент 2016/679; или

(4) Оценката съдържа най-малко:

а) системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;

б) оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

в) оценка на рисковете за правата и свободите на субектите на данни, посочени в ал. 1 по-горе; и

г) мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

(5) Когато е целесъобразно, „Конкорд Асет Мениджмънт“ АД се обръща към субектите на данни или техни представители за становище относно планираното обработване, без да се засягат търговските или обществените интереси или сигурността на операциите по обработване.

(6) Когато обработването на лични данни е необходимо за спазването на законово задължение на „Конкорд Асет Мениджмънт“ АД съгласно правото на ЕС или приложимото право в Република България, и това право регулира конкретната операция по обработване или набор от такива операции, и вече е извършена оценка на въздействието върху защитата на личните данни като част от общата оценка на въздействието в контекста на приемането на това правно основание, ал. 1—4 по – горе не се прилагат.

(7) При необходимост Дружеството прави преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни, най-малкото когато има промяна в риска, с който са свързани операциите по обработване.

(8) „Конкорд Асет Мениджмънт“ АД се консултира с надзорния орган преди обработването, когато оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако „Конкорд Асет Мениджмънт“ АД не предприеме мерки за ограничаване на риска.

Х. ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Чл. 34 (1) Дружеството определя длъжностно лице по защита на данните в следните случаи:

а) основните дейности на Дружеството се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни; или

б) основните дейности на Дружеството се състоят в мащабно обработване на специалните категории данни съгласно член 9 от Регламент 2016/679 и на лични данни, свързани с присъди и нарушения, по член 10 от Регламент 2016/679.

При условие, че описаните хипотези не са налице, Дружеството не определя длъжностно лице по защита на данните.

(2) Длъжностното лице по защита на данните се определя въз основа на неговите професионални качества, и по-специално въз основа на експертните му познания в областта на законодателството и практиките в областта на защитата на данните и способността му да изпълнява задачите.

(3) Длъжностното лице по защита на данните може да бъде служител на Дружеството или да изпълнява задачите въз основа на договор за услуги.

В случай че възникне основание за определяне на длъжностно лице по защита на данните, „Конкорд Асет Мениджмънт“ АД определя, че функциите ще се изпълняват от ръководителя на отдел „Нормативно съответствие“.

(4) При възникване на основание за определяне на длъжностно лице по защита на данните „Конкорд Асет Мениджмънт“ АД публикува данните за контакт с длъжностното лице по защита на данните и ги съобщава на надзорния орган.

Чл. 35 (1) „Конкорд Асет Мениджмънт“ АД гарантира, че длъжностното лице по защита на данните участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни.

(2) Управителния органи и всички служители на „Конкорд Асет Мениджмънт“ АД подпомагат длъжностното лице по защита на данните при изпълнението на неговите задачи, като дружеството осигурява ресурсите, необходими за изпълнението на тези задачи, и достъп до личните данни и операциите по обработване, а така също поддържа неговите експертни знания.

(3) Управителният орган на „Конкорд Асет Мениджмънт“ АД прави необходимото длъжностното лице по защита на данните да не получава никакви незаконосъобразни указания или влияния във връзка с изпълнението на неговите задачи по ал. 2. Длъжностното лице по защита на данните не може да бъде освобождавано от длъжност, нито санкционирано от „Конкорд Асет Мениджмънт“ АД за изпълнението на своите задачи. Длъжностното лице по защита на данните се отчита пряко пред най-висшето ръководно ниво на Дружеството - Съвета на директорите.

(4) Субектите на данни могат да се обръщат към длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните лични данни и с упражняването на техните права съгласно действащото законодателство и Регламент 2016/679.

(5) Длъжностното лице по защита на данните е длъжно да спазва пълна професионална тайна или поверителност на изпълняваните от него задачи в съответствие с правото на ЕС, правото на Република България или правото на държава членка.

(6) Длъжностното лице по защита на данните може да изпълнява и други задачи и задължения. Управителния орган на „Конкорд Асет Мениджмънт“ АД предприема необходимите стъпки тези задачи и задължения да не водят до конфликт на интереси.

Чл. 36. (1) Длъжностното лице по защита на данните изпълнява най-малко следните задачи:

- а) информира и съветва управителния орган и всички служители на „Конкорд Асет Мениджмънт“ АД, които извършват обработване, за техните задължения по силата на Регламент 2016/679 и на други разпоредби за защитата на данни на равнище ЕС или съгласно правото на Република България;
- б) наблюдава спазването на настоящия Регламент 2016/679 и на други разпоредби за защитата на данни на равнище ЕС или съгласно правото на Република България и на политиките на „Конкорд Асет Мениджмънт“ АД по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;
- в) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката;
- г) сътрудничи с надзорния орган;
- д) действа като точка за контакт за надзорния орган по въпроси, свързани с обработването и по целесъобразност да се консултира по всякакви други въпроси.

(2) При изпълнението на своите задачи длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.

XI. ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ДЪРЖАВИ ИЛИ МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

Чл. 37. Предаването на лични данни, които се обработват или да предназначени за обработване след предаване на трета държава или на международна организация, се извърша само при условие че са спазени всички изисквания на Регламент 2016/679, и при спазване на изискванията на глава V от Регламент 2016/679, включително при последващо предаване а на данните от третата държава или международната организация на друга трета държава или международна организация. „Конкорд Асет Мениджмънт“ АД осигурява също така, че нивото на защита на физическите лица,

осигурено от цитирания регламент, да не се излага на риск и да се запази и при предаване на данните.

Чл. 38. Предаване на лични данни на трета държава или международна организация може да има, ако „Конкорд Асет Мениджмънт“ АД извърши проверка и надлежно установи, че Европейската Комисия е решила, че тази трета държава, територия или един или повече конкретни сектори в тази трета държава, или международна организация, осигуряват адекватно ниво на защита. За такова предаване не се изисква специално разрешение и „Конкорд Асет Мениджмънт“ АД може да го извърши.

Чл. 39 (1) При липса на специален акт на Европейската Комисия по чл. 38 по - горе за адекватно ниво на защита, „Конкорд Асет Мениджмънт“ АД може да предава лични данни на трета държава или на международна организация, само ако е предвидило подходящи гаранции и при условие, че са налице приложими права на субектите на данни и ефективни правни средства за защита.

(2) Подходящите гаранции, посочени в ал. 1, могат да бъдат предвидени, без да се изисква специално разрешение от надзорния орган, посредством:

- а) задължителни фирмени правила по чл. 47 от Регламент 2016/679;
- б) стандартни клаузи за защита на данните;
- в) стандартни клаузи за защита на данните, приети от надзорен орган;
- г) одобрен кодекс за поведение, заедно със задължителни ангажименти с изпълнителна сила на администратора в третата държава да прилага подходящите гаранции, включително по отношение на правата на субектите на данни; или
- д) одобрен механизъм за сертифициране, заедно със задължителни и изпълними ангажименти на администратора в третата държава да прилага подходящите гаранции, включително по отношение на правата на субектите на данни.

Чл. 40 (1) „Конкорд Асет Мениджмънт“ АД не предава лични данни на свои клиенти или служители на трети лица, от които и да е държави, ако тези лица не отговарят на изискванията, установени в Регламент 2016/679.

(2) При липса на решение относно адекватното ниво на защита или на подходящи гаранции съгласно член 39 по-горе, включително задължителни фирмени правила, предаване или съвкупност от предавания на лични данни на трета държава се извършва само при едно от следните условия:

- а) субектът на данните изрично е дал съгласието си за предлаганото предаване на данни, след като е бил информиран за свързаните с предаването възможни рискове за субекта на данните поради липсата на решение относно адекватното ниво на защита и на подходящи гаранции.
- б) предаването е необходимо за изпълнението на договор между субекта на данните и „Конкорд Асет Мениджмънт“ АД или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните.
- в) предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;
- г) предаването е необходимо поради важни причини от обществен интерес;
- д) предаването е необходимо за установяването, упражняването или защитата на правни претенции;
- е) предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;
- ж) предаването се извършва от регистър, който съгласно правото на Съюза или правото на държавите членки, е предназначен да предоставя информация на обществеността и е достъпен за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

ХІІ. ОБУЧЕНИЕ

Чл. 41 (1) Звеното за „Нормативно съответствие“ на „Конкорд Асет Мениджмънт“ АД извършва обучение на всички служители на Дружеството с оглед спазване на изискванията на Закона за защита на личните данни и Регламент 2016/679, за което се съставя съответния протокол.

(2) Обучение се извършва при влизане в сила на Регламент 2016/679 и при всяка съществена промяна на действащото и приложимо законодателство, касаещо събирането, обработването, защитата, съхранението и предоставянето на лични данни.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите правила влизат в сила от 25.05.2018г.. Неразделна част от тези Правила са и съответните приложения към тях.

§ 2. Понятията и термините, използвани в настоящите Правила имат съдържанието, установено за тях в Регламент (ЕС) 2016/679 и са изброени в Приложение към правилата.

§ 3. Конкретните процедури, действия на задължени звена и служители, касаещи обработването на лични данни при „Конкорд Асет Мениджмънт“ АД са посочени в отделно приложение към настоящите Правила.

§ 4. Тези Правила са приети с Решение на Съвета на директорите от 23.05.2018г. на основание чл. 24, параграф 2 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни.

§ 5. Всички служители и лица, работещи по договор за УД, са уведомени за настоящите Правила, приложенията към тях и за задължението си да ги спазват.

Неразделна част от настоящите правила са и следните приложения:

Приложение № 1: Определения;

Приложение № 2: Вътрешни процедури за обработване на лични данни на УД „Конкорд Асет Мениджмънт“ АД;

Приложение № 3: Видове обработвани лични данни;

Приложение № 4: Уведомление до клиентите на УД „Конкорд Асет Мениджмънт“ АД във връзка със обработването на лични данни;

Приложение № 5: Регистър лични данни на дейностите по обработване на лични данни на УД „Конкорд Асет Мениджмънт“ АД.

Приложение № 1

Към Правила за обработване и защита на лични данни на управляващо дружество „Конкорд Асет Мениджмънт“ АД

ОПРЕДЕЛЕНИЯ

За целите на Правилата за обработване и защита на лични данни на управляващо дружество „Конкорд Асет Мениджмънт“ АД и съобразно изискванията на Регламент 2016/679 се прилагат следните определения:

1) „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;

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

3) „ограничаване на обработването“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

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

5) „псевдонимизация“ означава обработването на лични данни по такъв начин, че личните данни 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;

6) „регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

7) „администратор“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

8) „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

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

10) „трета страна“ означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

11) „съгласие на субекта на данните“ означава 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;

12) „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

13) „генетични данни“ означава лични данни, свързани с наследени или придобити генетичните белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице;

14) „биометрични данни“ означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилооскопични данни;

15) „данни за здравословното състояние“ означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;

16) „основно място на установяване“ означава:

а) по отношение на администратор, установен в повече от една държава членка — мястото, където се намира централното му управление в Съюза, освен в случаите, когато решенията по отношение на целите и средствата за обработването на лични данни се вземат на друго място на установяване на администратора в Съюза и на това място на установяване има правомощия за прилагане на тези решения, в който случай мястото на установяване, където са взети тези решения, се счита за основно място на установяване;

б) по отношение на обработващ лични данни, установен в повече от една държава членка — мястото, където се намира централното му управление в Съюза, или ако обработващият лични данни няма централно управление в Съюза, мястото на установяване на обработващия лични данни в Съюза, където се осъществяват основните дейности по обработването в контекста на дейностите на дадено място на установяване на обработващия лични данни, доколкото обработващият има специфични задължения съгласно настоящия регламент;

17) „представител“ означава физическо или юридическо лице, установено в Съюза, което, назначено от администратора или обработващия лични данни в писмена форма, представлява администратора или обработващия лични данни във връзка със съответните им задължения по настоящия регламент;

18) „дружество“ означава физическо или юридическо лице, което осъществява икономическа дейност, независимо от правната му форма, включително партньорствата или сдруженията, които редовно осъществяват икономическа дейност;

19) „група предприятия“ означава контролиращо предприятие и контролираните от него предприятия;

20) „задължителни фирмени правила“ означава политики за защита на личните данни, които се спазват от администратор или обработващ лични данни, установен на територията на държава членка, при предаване или съвкупност от предавания на лични данни до администратор или обработващ лични данни в една или повече трети държави в рамките на група предприятия или група дружества, участващи в съвместна стопанска дейност;

21) „надзорен орган“ означава независим публичен орган, създаден от държава членка съгласно член 51 от Регламент 2016/679;

21) „засегнат надзорен орган“ означава надзорен орган, който е засегнат от обработването на лични данни, тъй като:

а) администраторът или обработващият лични данни е установен на територията на държава членка на този надзорен орган;

б) субектите на данни с местопребиваване в държавата членка на този надзорен орган са засегнати съществено или е вероятно да бъдат засегнати съществено от обработването; или до този надзорен орган е подадена жалба.

23) „трансгранично обработване“ означава или:

а) обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обработващ лични данни в

Съюза, като администраторът или обработващият лични данни е установен в повече от една държава членка; или

б) обработване на лични данни, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, но което засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка;

24) „относимо и обосновано възражение“ означава възражение срещу проект на решение относно това дали е налице нарушение на Регламент 2016/679, или не, или дали предвиданото действие по отношение на администратора или обработващия лични данни отговаря на изискванията на Регламент 2016/679, което ясно доказва, че проектът за решение води до значителни рискове за основните права и свободи на субектите на данни, и където е приложимо, за свободното движение на лични данни в рамките на съюза;

25) „услуга на информационното общество“ означава услуга по смисъла на член 1, параграф 1, точка б) от Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета);

26) „международна организация“ означава организация и нейните подчинени органи, регламентирани от международното публично право, и/ или друг орган, създаден чрез или въз основа на споразумение между две или повече държави.

ВЪТРЕШНИ ПРОЦЕДУРИ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ НА УПРАВЛЯВАЩО ДРУЖЕСТВО „КОНКОРД АСЕТ МЕНИДЖМЪНТ“ АД

I. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 1. (1) „Конкорд Асет Мениджмънт“ АД (Дружеството/Управляващото Дружество/УД) възлага обработването на личните данни на негови служители. Обработването може да се възлага на повече от един служител в различни отдели/звена, съобразно спецификата на изпълняваните служебни функции и с цел разграничаване на конкретните им задължения. При възлагането на обработването се прилага принципът достъп до данните да имат само служители, които непосредствено изпълняват конкретни дейности.

(2) Служителите, които обработват лични данни, действат само по указание на УД освен ако в закон не е предвидено друго.

Чл. 2. (1) Личните данни се събират от клиенти на Дружеството чрез получаване на електронна поща от клиента, чрез устен разговор и/или на хартиен носител, както и чрез копиране на лична карта на клиентите на УД, предвид изискванията на Закон за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране, актовете по прилагането му, Закона за пазарите на финансови инструменти, актовете по прилагането му и пряко приложимите Делегирани Регламенти на ЕК, Закона за мерките срещу изпирането на пари и правилника за приложението му, а също и съобразно изискванията на Данъчно-осигурително процесуалния кодекс.

(2) За необходимостта от събирането на данните и целите, за които ще бъдат използвани, служителят на УД информира лицето, съответно клиента на УД, устно или писмено с предоставяне на съответния договор, общи условия към него, поръчка за записване/ обратно изкупуване на дялове от договорен фонд (ДФ) както и изрично уведомление за обработваните лични данни.

Чл. 3. (1) Съхраняването на лични данни на хартиен носител се осъществява като данните се съхраняват: в папки/ класъори в определени заключващи се шкафове и хартиените носители не се изнасят от служебните помещения (офиса на адреса на управление) на УД.

1. Правата и задълженията на служителите за достъп до такава информация са регламентирани в длъжностните им характеристики.
2. Предоставянето, промяната или прекратяването на оторизиран достъп до регистри и архив, съдържащ лични данни, се контролира от Изпълнителния директор и Отдел „Нормативно съответствие“ на УД.

(2) Местонахождението на шкафовете с лични данни на служители и клиенти 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 регламенти, закони, подзаконовни нормативни актове, кодекси и други правни норми) чрез:

- устно интервю с лицето;
- хартиен носител - писмени документи (заявления и апликационни форми, анкетни и информационни карти, декларации, тестове, поръчки, и др.) по текущи въпроси в процеса на работа и по предоставяне на съответната услуга, подадени от лицето;
- копия от документи за самоличност, предоставени от контрагенти/ клиенти и служители на УД.
- копия от банкови документи, пълномощни, данни за адресна регистрация, финансови възможности, опит, образование, професия, относима професия и други изискуеми съгласно законодателството лични данни.

(4) Личните данни от клиенти се подават до УД, чрез определени длъжностни лица. Тези лица, служители на УД, или членове на СД, разясняват на клиента/контрагента/пълномощника целта на обработване на данните, съгласно приложимото законодателство - ЗДКИСДПКИ, ЗПФИ, ЗМИП, ППЗМИП, ДОПК, Регламенти на ЕК, и други закони и подзаконовни нормативни актове, за което на

Клиента се предоставя отделен информационен документ (Приложение към Правилата за обработване и защита на лични данни).

(5) Личните данни, предоставяни от служители на Дружеството се подават до УД, чрез определени длъжностни лица (членове на СД, прокуристи, ръководител на звено човешки ресурси или счетоводство). Тези лица, служители на УД или членове на СД, разясняват на настоящия или бъдещ служител на УД целта на обработване на данните, съгласно приложимото законодателство – Кодекс на труда, Кодекс за социално осигуряване, ЗДКИСДПКИ, ЗПФИ, ЗМИП, ППЗМИП, ДОПК, Регламенти на ЕК, и други закони и подзаконовни нормативни актове.

Чл. 4. Форма на организация и съхраняване на личните данни на технически носител:

(1) Личните данни се въвеждат на твърд диск (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 локална служебна мрежа, със защитен достъп до личните данни, която може да се достъпва и да работи само служителят, обработващ лични данни при мерки за защита от средно ниво (парола и потребителско име).

(2) При работа с данните се използват съответните софтуерни продукти за обработка. Те могат да бъдат адаптирани към специфичните нужди на Дружеството. Данните се въвеждат на твърд диск/сървър от хартиен носител, освен ако не са били подадени от клиента/контрагента/бъдещия или настоящ служител на УД, чрез друго електронно средство за комуникация. Подаването по електронен начин от контрагента/бъдещия или настоящ служител на УД, става чрез изпращане на лични данни до УД чрез електронна поща на УД, тази възможност може да бъде изключена по решение на СД.

Електронната поща на УД, в която постъпват лични данни от което и да било лице се ползва с висока степен на техническа защита (пароли за достъп, ограничен достъп до пароли, честа смяна, техническа защита от вируси др.)

(3) Достъп до файловете за обработка на лични данни имат само работещите с тях, съобразно функционалното разпределение по звена в УД. При отсъствие на служителите, които са пряко ангажирани с изпълнението на определени функции, същите се заместват от друг служител, определен със заповед на изпълнителния директор.

(4) Местонахождение на сървъра е в помещението на УД, 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 УД това са служителите на отдел „Бек Офис“.

(6) За целите на осигуряване на непрекъсваемост на дейността на дружеството (back - up) при извънредни събития, природни бедствия технически причини, попадане на вируси в системата, и др. се снемат копия на съхраняваните в електронна форма документи на CD/DVD носители. CD/DVD носителите се съхраняват в заключващи се шкафове, достъп до които имат единствено системния администратор на дружеството и ръководството.

(7) 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 от автоматизирано под надзора на служител, отговарящ за компютърно-техническото обезпечение на УД. Когато данните се намират на изолирани компютри архивирането им се извършва от оператора на съответния компютър (обработващия лични данни).

II. МЕРКИ ЗА ГАРАНТИРАНЕ НА НИВОТО НА СИГУРНОСТ

Чл. 5. (1) Технически мерки за гарантиране нивото на сигурност:

- компютърните сървъри за база данни на УД 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, 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.

(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 УД, съобразно изискванията на вътрешни правила на УД 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.

(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 УД при наличие на законовите условия за унищожаване.

(6) УД извършва периодично тестове на системите си за техническа сигурност, за което провежда специализирани технически проверки на всеки 6 месеца с оглед спазване на изискванията за защита на лични данни.

Чл. 6. 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 работни 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 Главния счетоводител на УД. Контролът по използването на тези носители се извършва от изпълнителния директор и отдел Нормативно съответствие на УД.

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

(5) УД определя зона с контролиран достъп около работните бюра на бек офис служителите и служителят от отдел Нормативно съответствие и вътрешен контрол.

(6) При осъществяване на функциите си, служителите прилагат принципа на „чистото бюро“.

(7) 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.

(8) Сградата, в която е разположен офиса на УД, се охранява денонощно и има централизиран контрол на достъпа.

Чл. 7. 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 УД, 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 шест месеца от съответно лице, отговаряща за компютърното и техническо обезпечаване на УД.

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

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

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

(8) УД 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 процедури за защита на личните данни;
3. знания за опасностите за личните данни, обработвани от администратора;
4. несподеляне 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. процедурите и ръководствата за защита на личните данни;
3. опасностите за личните данни, обработвани от администратора.

(11) Служителите на УД 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 условията за обработване на лични данни – лични данни се обработват при сключване на договори с клиенти/контрагенти и при постъпване на работа при УД. Обработката става в специално отделена част от офиса на УД от служители на отделите Бек Офис и Фронт Офис;

2. регламентиране на достъпа до личните данни – достъп до лични данни се осъществява от служители от отдел „Фронт офис“, „Бек Офис“ и „Нормативно съответствие“;

4. контрол на достъпа – осъществява се от Изпълнителния Директор и отдел „Нормативно съответствие“;

5. определяне на срокове за съхранение – съгласно изискванията на ЗДКИСДПКИ, ЗПФИ, ЗМИП, КСО, КТр, ЗСч., пряко приложимите Регламенти на ЕК, други закони и подзаконовни нормативни актове, УД съхранява личните данни за своите клиенти докато траят отношенията с клиента и най-малко 5 години от прекратяване на отношения с клиента;

6. правила за размножаване и разпространение – лични данни не се размножават и не се разпространяват, освен в предвидените от приложимите закони и Регламент 2016/679 случаи към оправомощени държавни институции, към лицата, които са предоставили данните или трети лица от други държави при определени условия по Регламентата;

7. процедури за унищожаване – носители на лични данни се унищожават от комисия на УД 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 и правен риск, липса на законови пречки и при съставяне на протокол за унищожаването; 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. Унищожаването се извършва по следния начин:

а) при хартиен носител - чрез нарязване или изгаряне на хартиения носител без възможност за последващо възстановяване;

б) при електронен носител - чрез изтриване на електронните записи и всички архиви или резервни копия или копия на тези данни у други обработващи лични данни, без да има възможност за тяхното възстановяване.

в) унищожаването на лични данни се извършва и на всички съхранени копия от тях при трети лица, ако такива са били предоставени на някакво законово основание или въз основа на съгласие на клиента, освен ако няма друго законово основание, което препятства унищожаването на данните.

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. При унищожаване на носители на лични данни контролът за законосъобразното им унищожаване се осъществява от СД и отдел „Нормативно съответствие“.

III. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ

Чл. 8. Служителите на УД са длъжни да спазват и изпълняват Вътрешните правила, в съответствие с длъжностните им характеристики.

Чл. 9. При обработване на личните данни служителят подписва декларация, че е запознат със ЗЗДЛ, Регламент 2016/679, както и с настоящите процедури.

Чл. 10. (1) Дружеството предоставя достъп на служители си до лични данни на клиенти в изпълнение на нормативно установени задължения на служителите на УД.

(2) Лични данни се предоставят служебно между отделите в УД след обосновано искане, в съответствие с функционалните задължение на даден служител или звено и при уведомяване на Отдел „Нормативно съответствие“.

Чл. 11. (1) Всеки клиент (контрагент) на УД, който е физическо лице, има право на достъп до отнасящи се за него лични данни, съхранявани и обработвани при УД.

(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 УД или от изрично упълномощено от него лице, чрез нотариално заверено пълномощно.

(3) Заявлението следва да съдържа следната информация:

- а) идентификация на лицето – име, ЕГН, клиентски номер;
- б) контакти за обратна връзка – адрес, телефон, електронна поща;
- в) изложение на искането.

(4) Подаването на заявлението е бесплатно. УД има право да не отговори на заявлението, ако не е в състояние да идентифицира субекта на данните.

(5) Заявлението се завежда във входящия регистър на УД.

(6) Дружеството може да поиска писка допълнителна информация, ако са налице основателни съмнения относно самоличността на лицето, което подава искането.

(7) 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.

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

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

(10) УД уведомява писмено заявителя за решението си. Уведомяването става лично срещу подпис или по пощата с обратна разписка или в предпочитаната от заявителя форма.

Чл. 12. (1) Лични данни се предоставят на трети лица след получаване на писмено съгласие от лицето, за което се отнасят данните, както и при наличие на предпоставките за това, установени в Регламент 2016/679 и другите действащи и приложими за дейността на Дружеството нормативни

актове (ЗМИП, ЗДКИСДПКИ, ЗПФИ, ЗППЦК, Регламенти на ЕК, Наредби на КФН, Правила и насоки на ESMA и ЕВА).

(2) Не е необходимо съгласие на лицето в случаите, когато УД е задължен субект по закон и данните са поискани от държавни органи и институции в рамките на техните правомощия. В такива случаи субектът на данните следва да се информира поне за категориите получатели.

IV. ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ, УПРАВЛЕНИЕ И РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ

Чл. 13. (1) При възникване и установяване на инцидент, свързан с лични данни веднага се докладва на лицето, отговорно за защита на личните данни и на изпълнителния директор;

(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.

(6) Прилагат се и процедурите за уведомяване на субекта на личните данни и регулаторния орган, ако това се изисква съгласно нормите на Регламент 2016/679.

Чл. 14 (1) Всеки служител на УД се счита уведомен за рисковете, произтичащи от изтичане на лични данни на клиент, контрагент или служител, и за отговорността, която се носи при такова събитие. Рискът от изтичане на лични данни е свързан с нарушаване на личната неприкосновеност на клиент/ контрагент/служител, тъй като така биха станали известни различни лични данни обработвани от УД за съответния клиент/контрагент/служител.

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

V. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 15. Настоящите Вътрешни процедури са неразделна част от Правилата на за обработване и защита на лични данни на управляващо дружество „Конкорд Асет Мениджмънт“ АД.

Приложение № 3

Към Правила за обработване и защита на лични данни на управляващо дружество „Конкорд Асет Мениджмънт“ АД

ВИДОВЕ ОБРАБОТВАНИ ЛИЧНИ ДАННИ

За целите на Правилата за обработване и защита на лични данни и съобразно изискванията на Регламент 2016/679 „Конкорд Асет Мениджмънт“ АД (Дружеството/ Управляващото дружество/УД), в качеството си на администратор на лични данни, обработва следните лични данни на свои клиенти/контрагенти (пълномощници) и служители.

Изброяването посочва конкретните данни и законовото основание за обработването им.

Настоящото Приложение се предоставя на клиентите на Дружеството, за да се запознаят с данните, за чието обработване за Дружеството е установено нормативно задължение.

I. Лични данни обработвани съгласно изискванията на ЗМИП и ППЗМИП

1. имена на клиента; [чл. 53, ал. 2, т. 1 ЗМИП]
2. дата на раждане; [чл. 53, ал. 2, т. 2 ЗМИП]
3. място на раждане; [чл. 53, ал. 2, т. 2 ЗМИП]
4. ЕГН (официален личен идентификационен номер или друг уникален елемент за установяване на самоличността); [чл. 53, ал. 2, т. 3 ЗМИП]
5. данъчен номер (ако има такъв); [ДОПК]
6. всяко гражданство, което лицето притежава; включително ако има повече от едно или зелена карта [чл. 53, ал. 2, т. 4 ЗМИП]
7. държава на постоянно пребиваване; [чл. 53, ал. 2, т. 5 ЗМИП]
8. държава/и, на която/ито лицето е местно за данъчни цели [ДОПК]
9. адрес; [чл. 53, ал. 2, т. 5 ЗМИП; ДОПК]
10. вид на документа за самоличност; [чл. 53, ал. 2 ЗМИП]
11. номер на документ за самоличност; [чл. 53, ал. 2 ЗМИП]
12. издател на документа за самоличност; [чл. 53, ал. 2 ЗМИП]
13. валидност; [чл. 53, ал. 2 ЗМИП]
14. снимка; [чл. 53, ал. 2, т. 3 ЗМИП]
15. копие от официален документ за самоличност на клиента, заверено „вярно с оригинала“, поставена дата и подпис на клиента (чл. 53, ал. 1 ЗМИП и Наредба № 38 за изискванията към дейността на инвестиционните посредници, приета от КФН);
16. адрес за кореспонденция;
17. телефон, факс и адрес на електронна поща;
18. професия;
19. заемана длъжност;
20. работодател;
21. други валидни официални документи за самоличност, със снимка на лицето, за попълване на липсващи данни [чл. 53, ал. 5 ЗМИП].
22. данни за действителен собственик на юридически лица [чл. 59 ЗМИП];
23. информация от клиента за основната му дейност, включително за действителния и очаквания обем на деловите взаимоотношения и на операциите или сделките, които се очаква да бъдат извършвани в рамките на тези взаимоотношения, чрез попълване на въпросник или по друг подходящ начин [чл. 66, ал. 1 ЗМИП];
24. данни свързани с категоризирането на клиента като видна политическа личност (PEP) [чл. 36 ЗМИП].

Последици от отказ да се предоставят лични данни: В случаите, при които УД не може да изпълни изискванията за комплексна проверка по ЗМИП, то УД е длъжен да откаже извършването на операцията или сделката или установяването на делови взаимоотношения [чл. 17, ал. 1 ЗМИП].

Срок за съхранение на лични данни: Управляващото дружество съхранява за срок от 5 години всички събрани и изготвени по реда на ЗМИП и правилника за неговото прилагане, ЗДКИСДПКИ 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 тече от началото на календарната година, следваща годината на прекратяването на отношенията [чл. 67 ЗМИП].

II. Лични данни обработвани съгласно изискванията на Наредба № 44 за изискванията към дейността на колективните инвестиционни схеми, управляващите дружества, националните инвестиционни фондове и лицата, управляващи алтернативни инвестиционни фондове, във връзка с Наредба № 38 за изискванията към дейността на инвестиционните посредници

1. банково удостоверение, че клиентът е титуляр на съответната банкова сметка;
2. документ за платени комунални услуги като ток или вода;
3. нотариално заверено пълномощно от клиента към неговия пълномощник за извършване на управителни и/или разпоредителни действия с финансови инструменти.

III. Лични данни обработвани съгласно изискванията на Закона за пазарите на финансови инструменти (ЗПФИ) и Делегиран Регламент (ЕС) 2017/565.

1. опит и знания на клиента, за присъщите рискове, свързани с предлагания или искания инвестиционен продукт или инвестиционна услуга (чл. 56 от Делегиран регламент 2017/565);
2. образователно равнище и професия или значима предишна професия на клиента или на потенциалния клиент (чл. 55, параграф 1, б. „в“ от Делегиран регламент 2017/565);
3. видове услуги, сделки и финансови инструменти, с които клиентът е запознат (чл. 55, параграф 1, б. „а“ от Делегиран регламент 2017/565);
4. естество, обем и честота на сделките на клиента с финансови инструменти и период, през който те са сключвани (чл. 55, параграф 1, б. „б“ от Делегиран регламент 2017/565);
5. финансово положение на клиента - съдържа източника и размера на неговия редовен доход, неговите активи, включително ликвидни активи, инвестиции и недвижима собственост, както и неговите редовни финансови задължения (чл. 54, параграф 4 от Делегиран регламент 2017/565);
6. инвестиционните цели на клиент или потенциален клиент - съдържа информацията относно продажливостта от време, през което клиентът желае да държи инвестицията, неговите предпочитания по отношение на поемането на риск, неговия рисков профил и целите на инвестицията (чл. 54, параграф 5 от Делегиран регламент 2017/565);
7. данни за IP адрес и електронна поща на клиента (чл. 3, параграф 3 от Делегиран регламент (ЕС) 2017/565);
8. информация за сключените сделки с финансови инструменти за сметка на клиент трябва да съдържа данни най-малко за самоличността на клиента и за предприетите действия по изпълнението на Закона за мерките срещу изпирането на пари и Закона за мерките срещу финансирането на тероризма. (чл. 85, ал. 2 ЗПФИ).

Обработваната информация е законово установена и задължително се събира от УД с оглед извършване на оценка за уместност и целесъобразност, както и определяне на рисков профил на клиента.

IV. Лични данни събирани съгласно изискванията на чл. 142т от Данъчно-осигурително процесуален кодекс (ДОПК)

При откриване на нова сметка с декларация от титуляря на сметката УД събира данни, които да му позволят да извърши процедурите за комплексна проверка и да определи дали титулярят на сметката е лице, за което се предоставя информация, както следва:

1. по отношение на финансова сметка с титуляр физическо лице:
 - а) име;
 - б) адрес по местоживееене;
 - в) дата и място на раждане;
 - г) всяка юрисдикция, на която лицето е местно лице за данъчни цели;
 - д) данъчен номер за всяка юрисдикция, на която лицето е местно лице за данъчни цели;
 - е) всяко гражданство, което лицето притежава;

- ж) задължение за уведомяване при промяна в обстоятелствата;
- з) отговорност при деклариране на неверни данни;
- и) потвърждение за уведомяване, че информацията може да е обект на автоматичен обмен на финансова информация;
- к) дата и подпис на лицето.

V. Лични данни събирани по Кодекса на труда от служители на УД

Със съгласие на лицето: адрес, три имена, ЕГН, копие на лична карта, телефон, електронна поща, данни за банкова сметка, ниво на завършено образование, професионална квалификация. Със съгласие на служителя и когато е необходимо, съобразно изискванията на нормативен акт за заемане на определена длъжност, се събират и данни за липса или наличие на предишна съдимост и служителят изрично уведомява за данни за здравен статус (това може да не бъде събирано като информация, ако служителят декларира, че няма физически заболявания, които му пречат да извърша дейността си в УД.

Приложение № 4

Към Правила за обработване и защита на лични данни на управляващо дружество „Конкорд Асет Мениджмънт“ АД

УВЕДОМЛЕНИЕ

ДО КЛИЕНТИ НА УПРАВЛЯВАЩО ДРУЖЕСТВО „КОНКОРД АСЕТ МЕНИДЖМЪНТ“ АД ВЪВ ВРЪЗКА С ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Настоящото уведомление се предоставя на клиентите на управляващото дружество (УД) на основание чл. 13, параграфи 1 и 2 от Регламент 2016/679 и разкрива информацията, касаеща обработването на лични данни.

1. Данни за администратора „Конкорд Асет Мениджмънт“ АД

„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 от 19.09.2005 г. и лиценз № 46 – УД/21.06.2012 г. за извършване на дейност като управляващо дружество. Лице за контакт по отношение на защитата на лични данни – 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.

2. Видове обработвани лични данни

Категориите личните данни, които се събират и обработват при осъществяване на дейността на УД са следните:

- имена, единен граждански номер (ЕГН);
- адрес;
- други данни от документа за самоличност – място на раждане, пол, ръст, цвят на очите;
- данни за контакт: телефонен номер, електронна поща;
- клиентски номер;
- банкова информация: номер на банкова сметка;
- данни за финансово състояние: данни за притежаваните от клиента финансови инструменти;

3. Цели на обработването на лични данни и правни основания за обработването

Целите на обработването на лични данни са свързани с осъществяването на дейността на управляващото дружество, вкл. по записване и обратно изкупуване на дялове на договорни фондове (ДФ) и администриране на дялове, и са както следва:

- идентифициране на клиенти, контрагенти и пълномощници;
- извършване на оценка за подходяща услуга (уместност и целесъобразност);
- изпълнение на сключен с клиента договор/ 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;
- изпълнение на нормативни или регулаторни изисквания, установени в Закона за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране, Закона за мерките срещу изпиране на пари, Закона за мерките срещу финансиране на тероризма, Данъчно – осигурителния процесуален кодекс, Закона за пазарите на финансови инструменти, Закона за Комисията за финансов надзор, Закона за прилагане на мерките срещу пазарните злоупотреби с финансови инструменти, Закона за публичното прилагане на ценни книжа, наредби и други актовете по прилагането им, пряко действащите Регламенти и други актове на ЕК, или на други действащи нормативни актове.

„Конкорд Асет Мениджмънт“ АД събира и обработва лични данни на следните основания:

- Обработването е необходимо за сключване и изпълнение на договор/ поръчка за записване или обратно изкупуване на дялове от ДФ;
- Обработването е необходимо за спазване на законово задължение, което се прилага спрямо дружеството (администратор), при осъществяване на дейността му;
- Дружеството може да обработва лични данни на клиенти и на основание предоставено изрично съгласие от субекта на данните;
- Обработването е необходимо за целите на легитимния интерес на дружеството или на трето лице, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по – специално когато субектът на данните е дете.

„Конкорд Асет Мениджмънт“ АД има право и задължение да обработва личните данни на клиентите си за целите установени в ЗДКИСДПКИ, ЗПФИ, ЗМИП, ЗМФТ, ДОПК, ЗППЦК, ЗПМСПЗФИ, ЗКФН, наредбите и други актове по прилагането им, както и други пряко приложими Регламенти и други актове на ЕК, уреждащи дейността му или други подзаконовни нормативни актове, приложими в Република България. В цитираните нормативни актове са установени задължения за „Конкорд Асет Мениджмънт“ АД (администратор лични данни), чието спазване е задължително за извършването на дейност и предоставянето на съответните услуги, включително чрез обработването и съхраняването на лични данни.

„Конкорд Асет Мениджмънт“ АД събира лични данни на клиентите си чрез служителите, които работят по договор за дружеството, които са обвързани с декларации за конфиденциалност. Лични данни на клиента може да се събират и чрез електронни платформи, в които клиентът сам попълва регистрационните форми и съответните лични данни, в който случай електронните платформи са ползват с най-висока степен на техническа защита.

3. Получатели/ Категории получатели на лични данни

При осъществяването на дейността си като управляващо дружество „Конкорд Асет Мениджмънт“ АД може да разкрива събраните и обработвани лични данни на следните категории трети лица:

- Държавните органи, установени в ЗДКИСДПКИ, ЗПФИ, ЗПМСПЗФИ, ЗКФН, ЗППЦК, ЗМИП, ЗМФТ, ДОПК, съответните наредби по прилагането им и директно приложимите Регламенти и други актове на ЕК. Личните данни се разкриват при обстоятелствата и по ред, съдържащи се в цитираните нормативни актове. Такива получатели могат да бъдат – Комисия за финансов надзор, Българска народна банка, Национална агенция за приходите, Държавна Агенция „Национална сигурност“, одитори и др. Обработката на лични данни се извършва от служители на „Конкорд Асет Мениджмънт“ АД. Достъп до лични данни може да имат адвокати, счетоводители, одитори, риск мениджъри, технически специалисти, поддържащи компютърните системи на дружеството, както и доставчици на информационни услуги за съответните специфични дейности, извършвани от посочените категории лица.
- „Конкорд Асет Мениджмънт“ АД може да предостави лични данни и на свои партньори, доставчици на финансови услуги, или други контрагенти, необходими за осъществяване на дейността му като управляващо дружество, изпълнение на поръчките от клиенти или администриране на дялове от ДФ. Лични данни на клиенти могат да се предоставят на банката – депозитар на ДФ, на „Централен депозитар“ АД, регулиран пазар на финансови инструменти, доставчици на електронни платформи за търговия (МСТ, ОСТ), При изпълнение на поръчки от клиенти е възможно лични данни да бъдат предоставени на 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.
- Дружеството може да предостави лични данни и на финансови, данъчни, правни или други консултанти.

В качеството си на администратор на лични данни „Конкорд Асет Мениджмънт“ АД няма намерение да предава личните данни на трета държава или на международна организация, освен ако Клиентът не е дал изрично съгласие за това.

5. Срок на съхранение на лични данни

Управляващото дружество съхранява за срок от 5 години всички събрани и изготвени по реда на ЗМИП и актовете по 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 тече от началото на календарната година, следваща годината на прекратяването на отношенията. Критерият за посочения срок е законоустановен в чл. 67 ЗМИП. Всички сключени договори се съхраняват 5 години след тяхното прекратяване.

6. Права на клиентите спрямо личните данни, обработвани от „Конкорд Асет Мениджмънт“ АД

Клиентите имат следните права спрямо „Конкорд Асет Мениджмънт“ АД при обработване на лични данни:

- право на достъп до своите лични данни, които дружеството обработва, както и да получи копие от тях;
- право личните данни да бъдат коригирани, в случаите когато същите са непълни или неточни;
- право на поискат личните им данни да бъдат изтрити, когато са налице предвидените в действащата нормативна уредба предпоставки за това. Такива случаи са: ако е постигната целта, за която данните са събрани; клиентът е оттегил съгласието си за обработване на данните, когато не е налице друго основание за обработването; данните на клиента се обработват незаконосъобразно и т.н.;
- право на ограничаване на обработването на лични данни и право на възражение срещу обработването, в предвидените в Регламент 2016/679 или на друго законово основание случаи;
- право на преносимост на данните и да поискат същите да бъдат предоставени в структуриран, общоупотребяван и машинно-четим формат, в случаите когато това не противоречи на законоустановено задължение на „Конкорд Асет Мениджмънт“ АД или на друг нормативен акт на ЕС;
- когато обработването на лични данни се основава на предоставено съгласие, Клиентите имат право да оттеглят съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено;
- Клиентите имат право да подават жалби до надзорен орган, във връзка с обработване на негови лични данни. Субектите на лични данни, чиито данни се събират и обработват от УД, могат да подават жалби до Комисията за защита на личните данни, на адрес: гр. София 1592, бул. „Проф. Цветан Лазаров“ № 2, тел. 02/91-53-518, приемна - работно време: 9:00 - 17:30 ч., електронна поща: kzld@cpdp.bg, интернет страница: www.cpdp.bg.

Предоставянето на лични данни е нормативно задължително изискване предвид осъществяваната дейност от управляващото дружество. Основанията за това са посочени в ЗДКИСДПКИ, ЗПФИ, ЗМИП, ДОПК, актовете по прилагането им, други нормативни актове, пряко уреждащи дейността на дружеството, пряко приложими Регламенти на ЕК, подзаконовни нормативни актове на КФН, правила на ESMA, ЕВА, правилници на депозитарни институции, и указания на КФН. При евентуален отказ от страна на клиент/ контрагент/ пълномощник да предостави своите лични данни, изискуеми на нормативно основание, като последствие от това „Конкорд Асет Мениджмънт“ АД следва да откаже предоставянето на съответната услуга на клиента.

Други последици от отказа да се предоставят лични данни: В случаите, при които управляващото дружество не може да изпълни изискванията по ЗМИП, тъй като клиентът отказва да предостави лични данни, дружеството е задължено да откаже да извърши операцията, сделката или да установи делови отношения.

При осъществяването на своята дейност УД „Конкорд Асет Мениджмънт“ АД не прилага автоматизирано вземане на решения, включително профилиране, и поради това не предоставя информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

Допълнителна информация за начина, по който могат да се упражняват правата на клиентите, е налична в Правилата за обработване и защитна на личните данни на управляващо дружество „Конкорд Асет Мениджмънт“ АД, които са публикувани на интернет страницата на дружеството <http://concord-am.bg/>, както в офиса на дружеството в гр. София, бул. „Тодор Александров“ № 117.

Дата:

.....

Три имена и подпис на клиента:

.....