ПОЛИТИКА
ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ
НА „ЕКСПАТ АСЕТ МЕНИДЖМЪНТ“ ЕАД

Раздел I
Правно основание

Чл. 1. Настоящата политика е в съответствие с изискванията на Закона за защита на личните данни, чл. 19, ал.1 от Наредба № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), (ОВ, L119/1 от 4 май 2016 г.), наричан по наричан по-нататък „Регламент (ЕС) 2016/679“.

Раздел II
Цели на политиката

Чл. 3. (1) Настоящата политика има за цел да регламентира:

1. Минималното ниво на технически и организационни мерки при обработване на лични данни и допустимия вид защита прилагани от „Експат Асет Мениджмънт“ ЕАД (Дружеството) като администратор на лични данни;
2. Осигуряването на адекватно ниво на защита на личните данни в поддържаните регистри с лични данни от случайно или незаконно унищожаване, или от случайна загуба, от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване;
3. Организационни мерки в Дружеството, прилагани спрямо служителите, които обработват лични данни, осигуравящи спазването на нормативните изисквания и прилагането на тази Политика;
4. Оценка и нива на въздействие и определяне на ниво на защита в дейността на Дружеството.

(2) Настоящата политика има за цел и да информира клиентите и потенциалните клиенти на „Експат Асет Мениджмънт“ ЕАД, неговите служители, както и всички останали заинтересовани лица, че:

1. Данните, които идентифицират администратора, и координатите за връзка с него са: „Експат Асет Мениджмънт“ ЕАД, ЕИК 175431340, гр. София 1000, ул. „Г. С. Раковски“ № 96А.
2. Като управляващо дружество, извършващо дейност по управление на клиентски портфейли и на колективни инвестиционни схеми, Дружеството извършва обработване на лични данни, необходимо за изпълнение на договор и за спазване на законови задължения (законосъобразно обработване на лични данни по чл. 6, т. 1., б. „б“ и „в“ от Регламент (ЕС) 2016/679) – на основание на Закона за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране, Закона за пазарите на финансови инструменти, Закона за мерките срещу изпирането на пари, Закона за счетоводството и останалите законови и подзаконови нормативни актове, уреждащи дейността на дружеството.
3. Личните данни се съхраняват от Дружеството за срок, не по-дълъг от необходимия за изпълнение на целите, за които личните данни се обработват, и не по-дълъг от предвидените срокове за всяко едно от законовите основания, на които Дружеството извършва обработване на лични данни – съгласно Закона за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране, Закона за пазарите на финансови инструменти, Закона за мерките срещу изпирането на пари, Закона за счетоводството и останалите законови и подзаконови нормативни актове, уреждащи дейността на дружеството.
4. Дружеството не разкрива пред трети страни събраните лични данни освен в случаите, когато това се изисква по силата на нормативен акт, или е необходимо за извършване дейността на управляващото дружество – на трети страни като съдебни органи, надзорни органи, депозитари, платежни системи и институции, контрагенти, с които дружеството влиза в договорни отношения за целите на дейността си.

5. Дружеството може да извършва и обработване на лични данни на основание на съгласие, предоставено от субектите на лични данни (законосъобразно обработване на лични данни по чл. 6, т. 1., б. „а“ от Регламент (ЕС) 2016/679). Съгласието трябва да е свободно изразено от субекта на личните данни, а ако се дава в писмена форма, трябва да е в разбираема и лесно достъпна форма, като използва ясен и прост език. В този случай субектът на данните има правото да оттегли съгласието си по всяко време.
6. Във всички случаи субектът на личните данни има и следните права: право да изиска от Дружеството достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на данните; право да се направи възражение срещу обработването; право на преносимост на данните; право на жалба до надзорен орган.

Раздел III
Принципи при обработването на лични данни

Чл. 4. Дружеството спазва основните принципи при обработване на лични данни:
1. Законосъобразно, добросъвестно и по прозрачен начин обработване по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“);
2. Събирани са за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели („ограничение на целите“);
3. Събират се подходящи и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);
4. Точни и поддържани в актуален вид; предприемат се 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“);
5. Съхранявани са 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 („ограничение на съхранението“);
6. Обработвани са 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“).

Чл. 5. Дружеството носи отговорност и е в състояние да докаже спазването на чл. 4 („отчетност“).

Видове защита

Чл. 6. Видовете защита на личните данни са:
1. Физическа – система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.
2. Персонална – система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.
3. Документална – система от организационни мерки при обработването на лични данни на хартиен носител.
4. Защита на автоматизираните информационни системи и/или мрежи представлява система от технически и организационни мерки за защита от незаконни форми на обработване на личните данни.

Чл. 7. Дружеството прилага система от мерки, съответстващи на различните видове защита, които осигуряват адекватно ниво на защита в поддържаните регистри с лични данни.

Раздел IV
Оценка и нива на въздействие. Определяне на ниво на защита

Чл. 8. За да определи нивото на техническите и организационните мерки и допустимия вид защита, Администраторът извършва оценка на въздействието върху обработваните лични данни в съответствие с чл. 13 от Наредба № 1. Оценка на въздействие се извършва за всички поддържани регистри. Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.

Чл. 9. Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

Чл. 10. При оценка на въздействието, се вземат предвид:

1. Личните аспекти, свързани с дадено физическо лице (профилиране), за анализиране или прогнозиране, по-специално на неговото икономическо положение, местоположение, лични предпочитания, надеждност или поведение, която се основава на автоматизирано обработване и на чието основание се вземат мерки, които пораждат правни последици за лицето или го засягат в значителна степен;
2. Данни, които разкриват расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, или данни, които се отнасят до здравето, сексуалния живот или до човешкия геном;
3. Лични данни чрез създаване на видеозапис от видеонаблюдение на публично достъпни райони;
4. Лични данни в широкомащабни регистри на лични данни;
5. Данни, чието обработване съгласно решение на Комисията за защита на личните данни застрашава правата и законните интереси на физическите лица.

Чл. 11. Анализът на оценката на въздействие, определя нивото за въздействие за всеки един от водените регистри, както следва:

1. „Изключително високо“ – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на особено голяма група физически лица или трайни здравословни увреждания или смърт на група физически лица;
2. „Високо“ – в случаите, когато неправомерното обработване на лични данни би могло да доведе до възникване на значителни вреди или кражба на самоличност на голяма група физически лица или лица, заемащи висши държавни длъжности, или трайни здравословни увреждания или смърт на отделно физическо лице;
3. „Средно“ – в случаите, когато неправомерното обработване на лични данни би могло да създаде опасност от засягане на интереси, разкриващи расов или етнически произход, политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели, здравословното състояние, сексуалния живот или човешкия геном на отделно физическо лице или група физически лица;
4. „Ниско“ – в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Чл. 12. На база оценката на нивото на въздействие, Администраторът определя съответното ниво на защита, което представлява съвкупност от технически и организационни мерки за физическа, персонална, документална защита и защита на автоматизираните информационни системи и/или мрежи, както и криптографска защита на личните данни.
Нивата на защита са, както следва:

1. При ниско ниво на въздействие – ниско ниво на защита;
2. При средно ниво на въздействие – средно ниво на защита;
3. При високо ниво на въздействие – високо ниво на защита;
4. При изключително високо ниво на въздействие – изключително високо ниво на защита.

Чл. 13. След определяне на съответното ниво на защита, Администраторът следва да осигури минималното ниво на технически и организационни мерки, отговарящи на определеното ниво и съответстващи на изискванията на нормативната уредба по отношение на видовете защита на личните данни – физическа, персонална, документална, защита на автоматизирани информационни системи и/или мрежи и криптографска защита.

Раздел V
Организационни мерки спрямо служителите, които обработват лични данни

Чл. 14. Прилагането на необходимите технически и организационни мерки за защита на личните данни се осъществява от Администратора.

Чл. 15. Служителите, които обработват лични данни, трябва:

1. Да са запознати с нормативната уредба в областта на защитата на личните данни и настоящата Политика и Инструкцията по чл. 23 ал. 4 от ЗЗЛД и чл. 19 ал. 2 от Наредба No. 1;
2. Да познават опасностите при обработка на личните данни;
3. Да спазват различните нива на достъп, изградени в дейността на Администратора при обработка на лични данни
4. Да не разпространяват и споделят данни, идентификатори, пароли и други с помежду си и пред трети лица;
5. Да подпишат декларация за неразгласяване на лични данни, до които са получили достъп при и по повод изпълнение на задълженията си.

Чл. 16. Ръководителят на отдел „Вътрешен контрол и нормативно съответствие" отговаря за координирането при прилагане на мерките за защита на лични данни в Дружеството и провежда обучение на служителите, които обработват лични данни по отношение на нормативната уредба и настоящата Политика, както и за реакция при събития, застрашаващи сигурността на данните.

Допълнителни разпоредби

По смисъла на настоящата Политика:

§1. „Администратор на лични данни" 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. „Администратор на лични данни" е „Експат Асет Мениджмънт" ЕАД;

§2. „Обработващ лични данни" означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

§3. Настоящата Политика е приета от „Експат Асет Мениджмънт" ЕАД на заседание на Съвета на директорите, проведено на 18 юни 2013 г. и актуализирана на заседание на Съвета на директорите, проведено на 21 май 2018 г.