ПОЛИТИКА ЗА ЗАЩИТА НА ДАННИТЕ

НА “ФОНД МЕНИДЖЪР НА ФИНАНСОВИ ИНСТРУМЕНТИ В БЪЛГАРИЯ” ЕАД

I. Въведение

1. Общ регламент за защита на личните данни

Регламент (ЕС) 2016/679 (наричан по-нататък „Общ регламент за защита на данните“ или „Регламентът“) замества Директивата 95/46 / ЕО за защита на данните. Има пряко действие и предполага изменение в законодателството на страните - членки в областта на защитата на личните данни. Неговата цел е да защитава "правата и свободите" на физическите лица и да се гарантира, че личните данни не се обработват без тяхно знание, и когато е възможно, че се обработва с тяхно съгласие.

2. Обхват, очертан от Общия регламент за защита на данните

Материален обхват *(член 2)* –Регламентът се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни (*например ръчно и на хартия*), които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

Териториален обхват *(член 3)* – правилата на Регламента важат за всички администратори на лични данни, които са установени в ЕС, които обработват лични данни на физически лица, в контекста на своята дейност, както и за администратори извън ЕС, които обработват лични данни с цел да предлагат стоки и услуги или ако наблюдават поведението на субектите на данни, които пребивават в ЕС.

3. Понятия

„Лични данни" - 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;

„Специални категории лични данни“ – лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, или членство в синдикални организации и обработката на генетични данни, биометричните данни за уникално идентифициране на физическо лице, данни отнасящи се до здравето или данни относно сексуалния живот на физическо лице или сексуална ориентация;

„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 комбиниране, ограничаване, изтриване или унищожаване;

„Администратор" - всяко 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 ЕС 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;

„Субект на данните“ - всяко живо физическо лице, което е предмет на личните данни, съхранявани от Администратора;

„Съгласие на субекта на данните" - всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

„Дете“ – Общият Регламент определя дете като всеки на възраст под 16 години, въпреки че тази възраст може да бъде намалена от правото на държавата-членка до 13. Обработката на лични данни на едно дете е законна само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или упълномощен да даде съгласието си.

„Профилиране" - 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;

„Нарушение на сигурността на лични данни" - 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;

„Основно място на установяване “ – седалището на администратора в ЕС ще бъде мястото, в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде неговият административен център;

„Получател" - 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;

„Трета страна“ – всяко 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.

II. Декларация относно политиката по защита на личните данни

1. Ръководството на „Фонд мениджър на финансови инструменти в България“ ЕАД („Дружеството“) се ангажира да осигури съответствие със законодателството на ЕС и държавите-членки по отношение на обработването на личните данни и защитата на "правата и свободите" на лицата, чиито лични данни Дружеството събира и обработва съгласно Регламент (ЕС) 2016/679.

2. Тази политика се прилага заедно с други релевантни документи, както и свързани процеси и

процедури в съответствие с Регламента.

3. Регламент (ЕС) 2016/679 и тази политика се отнасят до всички функции по обработването на лични данни, включително тези, които се извършват относно лични данни на крайни получатели, контрагенти, служители, доставчици и партньори и всякакви други лични данни, които Дружеството обработва от различни източници.

4. Длъжностното лице по защита на данните (когато има определено такова в съответствие с настоящата Политика) отговаря за преразглеждането на „Регистъра на дейностите по обработване“ ежегодно в светлината на всякакви промени в дейностите на Дружеството както и всички допълнителни изисквания, оценки на въздействието върху защитата на данните. Този регистър трябва да бъде на разположение по искане на надзорния орган.

5. Тази политика се прилага за всички служители на Дружеството, както и в отношенията с външни доставчици. Всяко нарушение на Регламента ще бъде разглеждано като нарушение на трудовата дисциплина, а в случай че има предположение за извършено престъпление, въпросът ще се предостави за разглеждане на съответните държавни органи.

6. Партньори и трети лица, които работят с или за Дружеството, както и които имат или могат да имат достъп до личните данни, следва да бъдат запознати и да се съобразят с тази политика. Никоя трета страна не може да има достъп до лични данни, съхранявани от Дружеството, без предварително да е сключила споразумение за поверителност на данните, което налага на третата страна задължения, не по-малко обременяващи от тези, които Дружеството е поело, и което дава право на Дружеството да извършва проверки на спазването на наложените със споразумението задължения.

III. Задължения и роли по Регламент (ЕС) 2016/679

1. *ФМФИБ ЕАД е администратор на данни и обработващ данни* съгласно Регламент (ЕС) 2016/679.

2. Всички членове на управителните органи на Дружеството са отговорни за насърчаване на добри практики в областта на обработване на информация във ФМФИБ ЕАД.

3. Съвета на директорите /СД/ взема решение за определяне на Длъжностно лице по защита на данните, с роля определена в Регламент (ЕС) 2016/679[1]. То трябва да бъде отговорно пред висшето ръководство и да се отчита пред Съвета на директорите на Дружеството за управлението на личните данни в рамките на организацията и за гарантирането на възможността за доказване на съответствието със законодателството за защита на данните и добрите практики.

Тази отчетност на ДЛЗД включва:

- внедряване на изискванията на Регламент (ЕС) 2016/679;
- управление на сигурността и риска по отношение на съответствието с политиката и Регламента (ЕС) 2016/679.

4. Длъжностното лице по защита на данните, което СД счита за подходящо, квалифицирано и опитно, е отговорно да гарантира, че както като цяло организацията на Дружеството, така и дейността на всеки член на ръководния състав, която се извършва в рамките на неговата област на отговорност, съответстват на изискванията на Регламент (ЕС) 2016/679.

5. Длъжностното лице по защита на данните, когато е определено, има специфични отговорности по отношение на процедури като „Процедура за управление на исканията от субектите“ и е контактна точка за служителите на администратора, които искат разяснения по всеки аспект на спазването на защитата на данните.

6. Спазването на законодателството за защита на данните е отговорност на всички служители на

[1] *Длъжностно лице по защита на данните (ДЛЗД) - ролята на длъжностното лице по защита на данните, кога неговото назначаване е задължително и какви са изискванията към него са подробно описани в чл. 37-39 от Регламента.*

Дружеството, които обработват лични данни.

7. В Дружеството се провежда политиката за обучение на служителите съобразно техните конкретни роли и правомощия.

IV. Принципи за защита на данните

Цялата обработка на лични данни трябва да се извършва в съответствие с принципите за защита на данните, посочени в член 5 от Регламент (ЕС) 2016/679. Политиките и процедурите на Дружеството имат за цел да гарантират спазването на тези принципи.

1. Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно

Законосъобразно – да идентифицира законна основа, преди да може да обработва лични данни. Те често са посочени като "основания за обработване", например „съгласие“.

Добросъвестно - за да може обработването да бъде добросъвестно, администраторът на данни трябва да предостави определена информация на субектите на данни, доколкото това е практически възможно. Това важи независимо дали личните данни са получени директно от субектите на данни или от други източници.

Регламент (ЕС) 2016/679 увеличава изискванията за това каква информация трябва да бъде на разположение на субектите на данни, която е обхваната от изискването за "прозрачност".

Прозрачно – Общият регламент включва правила относно предоставяне на поверителна информация на субектите на данни в членове 12, 13 и 14 от Регламента. Те са подробни и конкретни, поставяйки акцента върху това, че известията за поверителност са разбираеми и достъпни. Информацията трябва да бъде съобщена на субекта на данните в разбираема форма, като се използва ясен и разбираем език.

Правилата за уведомяване на субекта на данни от Дружеството са определени в Процедура за прозрачност при обработката на лични данни.

Специфичната информация, която трябва да бъде предоставена на субекта на данните, трябва да включва като минимум:

- данни, които идентифицират администратора и данните за контакт на администратора и, ако има такъв, на представителя на администратора;
- контактите на ДЛЗД;
- целите на обработването, за което личните данни са предназначени както и правното основание за обработването;
- периода, за който ще се съхраняват личните данни;
- съществуването на следните права - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както право на възражение срещу условията (или липсата на такива) във връзка с упражняването на тези права;
- категориите лични данни;
- получателите или категориите получатели на лични данни, където това е приложимо;
- където е приложимо, дали администраторът възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на данните;
- всякаква допълнителна информация, необходима да се гарантира добросъвестно обработване.

2. Лични данни могат да се събират само за конкретни, изрично указани и законни цели

Данните, получени за конкретни цели, не трябва да се използват за цел, която се различава от тези, официално обявени на управляващия орган като част от Регистъра на дейностите по обработване на данни (чл. 30 от Регламента) на Дружеството. Съответните правила се определят в Процедура за прозрачност при обработката на лични данни.

3. Личните данни трябва да бъдат адекватни, релевантни, ограничени до това, което е необходимо за обработването им със съответната цел. *(принцип на минимално необходимото**)***

- Дружеството не следва да събира информация, която не е строго необходимо за целта, за която тя е получена.
- Всички формуляри за събиране на данни (електронни или на хартиен носител), включително изискванията за събиране на данни в новите информационни системи, трябва да включват декларация или уведомление за поверително третиране на личните данни.
- Дружеството гарантира, че на годишна основа всички способи за събиране на данни се преглеждат от ДЛЗД/вътрешен одит/външни експерти, за да се гарантира, че събраните данни продължават да бъдат адекватни, релевантни, не са прекомерни съобразно Процедура за оценка на въздействието върху защитата на данните.

4. Личните данни трябва да бъдат точни и актуализирани във всеки един момент, и да са положени необходими усилия, за да е възможно незабавно (в рамките на възможните технически решения) изтриване или коригиране.

- Данните, които се съхраняват от Дружеството, трябва да бъдат прегледани и актуализирани при необходимост. Не трябва да се съхраняват данни, в случаите, когато има вероятност да не са точни.
- Ръководството на Дружеството следва да осигури обучение на целия персонал в значението на събирането на точни данни и поддържането им.
- Също така, задължение на субекта на данните е да декларира, че данните, които предава за съхраняване от Дружеството са точни и актуални. Попълването на формуляр от субекта на данни, предназначени за администратора, ще включва изявление, че съдържащите се в него данни са точни към датата на подаване.
- От субектите на данни (служителите / контрагенти / крайни получатели/ други) трябва да се изисква, да уведомяват Дружеството за всякакви промени в обстоятелствата, за да могат да се актуализират записите на лични данни. Отговорността на Дружеството е да гарантира, че всяко уведомление относно промяната на обстоятелствата е записано и се предприемат действия.
- Ръководството на Дружеството носи отговорност да се гарантира, че са налице подходящи процедури и политики за поддържане на точност и актуалност на личните данни, като се отчита обемът на събраните данни, скоростта, с която може да се промени, други относими фактори.
- Най-малко на годишна база в Дружеството се извършва преглед на сроковете на съхранение на всички лични данни и идентифициране на всички данни, които вече не се изискват в контекста на регистрираната цел. Тези данни следва да бъдат надеждно унищожени в съответствие с процедурите и правилата на Дружеството.
- Длъжностното лице за защита на данните взема подходящи мерки, в случаите когато установи, че организациите на трети страни имат неточни или остарели лични данни, да ги информира, че информацията е неточна или остаряла и да не се използва за вземане на решения относно лицата, да информира съответните страни.

5. Личните данни трябва да се съхраняват в такава форма, че субектът на данните може да бъде идентифициран само толкова дълго, колкото е необходимо за обработването.

- Лични данни ще бъдат пазени в съответствие с Процедура за съхраняване и унищожаване на данните и след като е преминал срокът им на съхранение, те трябва да бъдат надеждно унищожени по указания в тази процедура ред;
- Допустимо е личните данни да се запазват след датата на обработването, като в тези случаи те ще бъдат съхранявани по подходящ начин – *криптирани или псевдонимизирани,* за да се защити самоличността на субекта на данните в случай на нарушение на данните.
- Длъжностното лице за защита на данните специално трябва да одобри всяко запазване на данни, което надхвърля срока на съхранение, дефиниран в Процедура за съхраняване и унищожаване на данните и трябва да гарантира, че обосновката е ясно определена и е в съответствие с изискванията на законодателството за защита на данните. Това одобрение трябва да бъде писмено.

6. Личните данни трябва да бъдат обработени по начин, който гарантира подходяща сигурност (чл. 24 , чл. 32 от ОРЗД)

Длъжностното лице за защита на данните следва да извърши оценка на въздействието, като вземе предвид всички обстоятелства, свързани с операциите по управление или обработване на данни от Дружеството.

При определянето на това доколко уместно е обработването, Длъжностното лице по защита на данните трябва също така да разгледа степента на евентуална вреда или загуба, която може да бъде причинена на физически лица (напр. персонал или контрагенти), ако възникне нарушение на сигурността, както и всяка вероятна вреда за репутацията на Дружеството, включително евентуална загуба на доверие на контрагентите.

При оценяването на подходящи технически мерки, длъжностното лице по защита на данните ще разгледа следното:

- Защита с парола;
- Автоматично заключване на бездействащи работни станции в мрежата;
- Ограничаване на права на достъп за USB и други преносими носители с памет;
- Антивирусен софтуер и защитни стени;
- Правата за достъп основани на длъжности, включително тези, на назначен временно персонал;
- Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;
- Сигурност на локални и широкообхватни мрежи;
- Технологии за подобряване на поверителността, като например криптиране или псевдонимизиране;
- Идентифициране на подходящи международни стандарти за сигурност подходящи за Дружеството.

При оценяването на подходящите организационни мерки Длъжностното лице за защита на данните ще вземе предвид следното:

- Нивата на подходящо обучение в Дружеството;
- Мерките, които отчитат надеждността на служителите;
- Включването на защитата на данните в трудовите договори;
- Идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни;

- Редовна проверка на персонала за спазване на съответните стандарти за сигурност;
- Контрол на физическия достъп до електронни и хартиено базирани записи;
- Спазването на политика на „чисто работно място“[2];
- Съхраняване на хартия на базата данни в заключващи се шкафове/архив;
- Ограничаване на използването на портативни електронни устройства извън работното място;
- Спазване на правилата за създаване и ползване на пароли;
- Редовно създаване на резервни копия на личните данни и физическо съхраняване на носителите с копия извън офиса / резервен център за съхранение на данни;
- Налагане на договорни задължения на контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни (вкл. извън ЕС).

Тези контроли следва да бъдат избрани въз основа на идентифицираните рискове за лични данни, както и потенциала за нанасяне на вреди, на лицата, чиито данни се обработват.

7. Спазване на принципа на отчетност

Регламент (ЕС) 2016/679 включва разпоредби, които насърчават отчетността и управляемостта и допълват изискванията за прозрачност. Принципът на отчетност в изисква от администратора да докаже, че спазва останалите принципите от Регламента и изрично заявява, че това е негова отговорност.

Дружеството ще доказва спазването на принципите за защита на данните чрез прилагане на политики по защита на данните, като внедрява подходящи технически и организационни мерки, както и чрез приемане на техники по защита на данните на етапа на проектирането и защита на данните, оценка на въздействието върху защитата на личните данни, процедура за уведомяване за нарушаване на лични данни и т.н.

V. Права на субектите на данни

1. Субектите на данни имат следните права по отношение на обработването на данни, както и на данните, които се записват за тях:

- Да отправя искания за потвърждаване дали се обработват лични данни, свързани с тях, и ако това е така, да получат достъп до данните, както и информация кои са получателите на тези данни.
- Да поискат копие от своите лични данни от администратора;
- Да искат от администратора коригиране на лични данни, когато те са неточни, както и когато не са вече актуални;
- Да изискат от администратора изтриване на лични данни (право „да бъдеш забравен");
- Да искат от администратора ограничаване на обработването на лични данни като в този случай данните ще бъдат само съхранявани, но не и обработвани.;
- Да направят възражение срещу обработване на лични данни;
- Да се обърнат с жалба до надзорен орган ако смятат, че някоя от разпоредбите на Регламента е нарушена;
- Да поискат и да им бъдат предоставени личните данни в структуриран, широко използван и

[2] При напускане на работното място, цялата работна документация е премахната или прибрана в подходящи за това и с ограничен достъп места - специални шкафове, заключени помещения, унищожаване на вече ненужни документи.

пригоден за машинно четене формат;

- Да оттеглят съгласието си за обработката на личните данни по всяко време с отделно искане, отправено до Дружеството;
- Да не бъдат обект на автоматизирано взети решения, които ги засягат в значителна степен, без възможност за човешка намеса;
- Да се противопоставят на автоматизирано профилиране, което се случва без тяхно съгласие;

2. Дружеството осигурява условия, които да гарантират упражняването на тези права от субекта на данни:

- Субектите на данни могат да направят искания за достъп до данни, както е описано в процедурата за Процедура за управление на исканията от субектите.
- Субектите на данни имат право да подават жалби до Дружеството, свързани с обработването на личните им данни, обработването на искане от субекта на данни и обжалване от страна на субекта на данни, относно начина на обработване на жалбите в съответствие с Процедура за начините на комуникация при жалби и искания от субекта на данни.

VI. Съгласие

1. Под „съгласие“ Дружеството ще разбира 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. Субектът на данните може да оттегли своето съгласие по всяко време.

2. Дружеството разбира под "съгласие" само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

3. Съгласието не може да бъде изведено от липсата на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. Дружеството в качеството му на администратор трябва да може да докаже, че е получено съгласие за дейностите по обработване (например когато нов клиент подписва договор или по време на набиране на нов персонал).

4. За специални категории данни трябва да се получи изрично писмено съгласие, съгласно Процедура по получаване на съгласие за обработване на лични данни на субектите на данни, освен ако не съществува алтернативно законно основание за обработване.

5. Когато Дружеството обработва лични данни на деца, трябва да бъде получено разрешение от упражняващите родителските права (родители, настойници и т. н.). Това изискване се прилага за деца на възраст под 16 години (освен ако с национален закон не е предвидена по-ниска възрастова граница, която не може да бъде по-ниска от 13 години).

VII. Сигурност на данните

1. Всички служители са отговорни за гарантирането на сигурността при съхраняването на данните, за които те отговарят и които Дружеството държи, както и, че данните се съхраняват сигурно и не се разкриват при каквито и да било обстоятелства на трети страни, освен ако Дружеството не е дало такива права на тази трета страна , като е сключен договор.

2. Всички лични данни трябва да бъдат достъпни само за тези, които се нуждаят от тях, а достъпът може да бъде предоставен само в съответствие с изградените правила за контрол на достъпа. Всички лични данни трябва да се третират с най-голяма сигурност и трябва да се съхраняват:

- в самостоятелна стая с контролиран достъп; и/или в заключен шкаф или в картотека; и/или

- ако е компютъризирана, защитена с парола в съответствие с вътрешните изисквания посочени в организационните и технически мерки за контролиране на достъпа до информация (*например правила за контрол на достъпа*) ; и / или
- съхранявани на преносими компютърни носители, които са защитени в съответствие с организационните и технически мерки за контролиране на достъпа до информация.

3. В Дружеството следва да се създаде организация, която да гарантира, че компютърните екрани и терминалите не могат да бъдат гледани от друг, освен от оторизираните служители. Всички служители следва да бъдат обучени и да се запознаят и декларират спазване на организационните и технически мерки за достъп, както и правилата за заключване на работните станции, преди да им бъде предоставен достъп до информация от всякакъв вид.

4. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни от неоторизирани лица и не могат да бъдат изваждани от определените офисни помещения без изрично разрешение. Веднага щом хартиените документи вече не са необходими за текущата работа, те трябва да бъдат унищожени в съответствие със създадена за това процедура/правила и съответен протокол.

5. Личните данни могат да бъдат изтривани или унищожавани само в съответствие с Процедура за съхраняване и унищожаване на данните. Записите на хартиен носител, които са достигнали датата на съхранение, трябва да бъдат нарязани и унищожени. Данните върху твърдите дискове на излишните персонални компютри трябва да бъдат изтрити или дисковете унищожени, съгласно изградените правила/процедури.

6. Обработването на лични данни "извън офиса" представлява потенциално по-голям риск от загуба, кражба или нарушение на лични данни. Персоналът трябва да бъде специално упълномощен да обработва данните извън обекти на администратора.

VIII. Разкриване на данни

1. Дружеството трябва да осигури условия, при които личните данни не се разкриват на неупълномощени трети страни, което включва членове на семейството, приятели, държавни органи, дори разследващи такива, ако има основателно съмнение, че не се изискват по установения ред. Всички служители трябва да бъдат предпазливи, когато им поискат да разкрият съхранявани лични данни за друго лице на трета страна. Важно е да се има предвид, дали разкриването на информацията е свързано или не с нуждите на дейността, извършвана от Дружеството.

Необходимо е на служителите да се извърши специално обучение и периодични инструктажи с цел да се избегне рискът от такова нарушение.

2. Всички искания от трети страни за предоставяне на данни трябва да бъдат подкрепени с подходяща документация и всички такива разкривания на данни трябва да бъдат специално разрешени от Длъжностното лице за защита на данните.

3. Дружеството има право да разкрива и предава личните данни на трети лица, позиционирани на територията на ЕС/ЕИП, доколкото съществува легитимен интерес, свързан с обработка на личните данни за вътрешни административни цели. Това и всяко друго предаване се извършва при стриктно спазване на конфиденциалност и сигурност на личните данни.

IX. Съхраняване и унищожаване на данните

1. Дружеството не съхранява лични данни във вид, който позволява идентифицирането на субектите за по-дълъг период отколкото е необходимо, по отношение на целите, за които са били събрани данните.

2. Дружеството може да съхранява данни за по-дълги периоди единствено ако личните данни ще бъдат обработвани за целите на архивиране, за цели в обществен интерес, научни или исторически изследвания и за статистически цели, и само при изпълнението на подходящи технически и

организационни мерки за гарантиране на правата и свободите на субекта на данните.

3 Периодът на съхранение за всяка категория на лични данни ще бъде посочен в Процедура за съхраняване и унищожаване на данните както и на критериите, използвани за определяне на този период.

4. Процедура за съхраняване и унищожаване на данните, Дружеството ще се прилага във всички случаи.

5. Личните данни трябва да бъдат унищожени сигурно, съгласно принципа за гарантиране подходящо ниво на сигурност – включително чрез защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“);

X. Трансфер на данни

1. Всеки износ на данни от рамките на ЕС към страни извън ЕС (посочени в Общия регламент като "трети страни") са незаконни, освен ако няма подходящо "ниво на защита на основните права на субектите на данни“.

2. Решение за адекватност

Европейската комисия може да оцени трети страни, територия и/или специфични сектори в трети страни, за да прецени дали има подходящо ниво на защита на правата и свободите на физическите лица. В тези случаи не се изисква разрешение.

Държавите, които са членки на Европейското икономическо пространство (ЕИП), но не и на ЕС, се приемат като отговарящи на условията за решение за адекватност.

XI. Регистър на обработванията на данни (инвентаризация на данните)

1. Дружеството е създало процес на инвентаризация на данните като част от своя подход за справяне с рисковете и възможностите в процеса на спазване на политиката за съответствие с Регламент (ЕС) 2016/679. При инвентаризацията на данните и в работния поток от данни се установяват:

- бизнес процесите, които използват лични данни;
- източниците на лични данни;
- броя на субектите на данни;
- описание на категориите лични данни и елементите на във всяка категория;
- дейностите по обработване;
- целите на обработването, за което личните данни са предназначени;
- правното основание за обработването;
- получателите или категориите получатели на личните данни;
- основните системи и места за съхранение;
- всички лични данни, които подлежат на трансфери извън ЕС;
- сроковете за съхранение и заличаване.

2. Дружеството следва да е наясно с рисковете, свързани с обработването на определени видове лични данни.

3. Дружеството оценява нивото на риска за лицата, свързани с обработването на личните им данни. Извършват се оценки на въздействието върху защитата на данните във връзка с обработването на лични данни и във връзка с обработването, предприето от други организации от името на Дружеството.

4. Дружеството управлява всички рискове, идентифицирани от оценката на въздействието, с цел да се намали вероятността от несъответствие с тези правила.

Когато вид обработване може да доведе до висок риск за правата и свободите на физическите лица, по-специално с използване на нови технологии и като се вземат предвид естеството, обхвата, контекста и целите на обработването, преди да пристъпи към обработване Дружеството следва да извърши оценка на въздействието на предвидените операции по обработване върху защитата на личните данни. Една обща оценка на въздействието може да разглежда набор от подобни операции по обработване, които представляват подобни високи рискове.

5. Когато в резултат на Оценката на въздействието е ясно, че Дружеството ще започне да обработва лични данни, които поради висок риск биха могли да причинят вреди на субектите на данни, решението дали обработването да продължи или не, трябва да бъде предадено за преглед от страна на Длъжностното лице за защита на данните.

6. Ако ДЛЗД има сериозни опасения или относно потенциалната вреда или опасност, или относно количеството на съответните данни, то следва да ескалира въпроса пред Съвета на директорите.

7. Длъжностното лице по защита на данните прави ежегоден преглед на първоначално инвентаризираните данни, преразглежда вписаната информация в „Регистъра на дейностите по обработване“ в светлината на всякакви промени в дейностите на Дружеството.