ИНСТРУКЦИЯ от 31.07. 2013 г.

ЗА МЕРКИТЕ И СРЕДСТВАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ,

ОБРАБОТВАНИ ОТ ЦКБ АСЕТС МЕНИДЖМЪНТ ЕАД

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) С тази инструкция се уреждат редът и условията за обработването на лични данни от ЦКБ АСЕТС МЕНИДЖМЪНТ ЕАД /по-долу ЦКБ АМ ЕАД, Дружеството/, както и мерките и средствата за защита на поддържаните от ЦКБ АМ ЕАД регистри на лични данни.

(2) Инструкцията не урежда обработването на лични данни, представляващи класифицирана информация.

(3) Инструкцията се приема, допълва, изменя и отменя от Съвета на директорите на ЦКБ АМ ЕАД.

Чл. 2. (1) (изм. 14.04.2016г.) ЦКБ АМ ЕАД е администратор на лични данни с адрес: гр. София, бул. „Цариградско шосе" № 87. Дружеството се представлява заедно от неговите изпълнителни директори. ЦКБ АМ ЕАД е вписано под идентификационен № 0036415 в регистъра на администраторите на лични данни, воден от Комисията за защита на личните данни (КЗЛД).

(2) (доп. 14.04.2016г.) ЦКБ АМ ЕАД обработва лични данни за конкретни цели, определени в Закон за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране, Валутен закон, Закон за публичното предлагане на ценни книжа, Закон за пазарите на финансови инструменти, Закон за мерките срещу изпирането на пари, Закон за мерките срещу финансирането на тероризма, Кодекс за социално осигуряване, Кодекс на труда, Данъчно-осигурителен процесуален кодекс /ДОПК/, Закон за данъците върху доходите на физическите лица, Закон за здравословни и безопасни условия на труд, Закон за счетоводството и други нормативни актове, при спазване изискванията на Закона за защита на личните данни /ЗЗЛД/.

(3) Дружеството обработва личните данни чрез различни служители, съобразно спецификата на изпълняваните от тях служебни функции и в зависимост от конкретните им задължения.

(4) Дружеството предоставя достъп до обработваните от нея лични данни на физическите лица, за които се отнасят данните, и на трети лица, в съответствие с изискванията на ЗЗЛД. Осъществяване правото на достъп до лични данни не може да бъде насочено срещу правата и доброто име на друго физическо лице, обществения ред и морала.

Глава втора
РЕГИСТРИ НА ЛИЧНИ ДАННИ

РАЗДЕЛ I
ВИДОВЕ РЕГИСТРИ

Чл. 3. (1) (доп. 14.04.2016г.) ЦКБ АМ ЕАД поддържа следните видове регистри на лични данни, вписани по реда на ЗЗЛД в Комисията за защита на личните данни:

1. регистър „Клиенти";
2. регистър „Персонал";
3. (нова 14.04.2016г.) регистър „Автоматичен обмен на финансова информация по ДОПК"

(2) (изм. 14.04.2016г.) Описание на регистрите, в т.ч. категории физически лица, за които се обработват лични данни, групи обработвани данни, източници и средства за събирането им, форма за водене на регистъра, ред за съхраняване и унищожаване на информационни носители, служители, обработващи лични данни, техническите ресурси, прилагани за обработване на данните в електронните регистри и други се съдържа в Приложения № 3; №3А; №4; № 5 към настоящата Инструкция.

(3) Създаването на нови регистри и извършването на промени, в т.ч. преустановяване обработването на лични данни в съществуващите регистри, се извършва с решение на Съвета на директорите или заповед на изпълнителните директори на ЦКБ АМ ЕАД. Въз основа на решението/заповедта се предприемат действия по чл. 18, ал. 3 от ЗЗЛД за уведомяване на Комисията за защита на лични данни.

РАЗДЕЛ II
ГРУПИ ОБРАБОТВАНИ ДАННИ

Чл. 4. (1) В зависимост от нормативното основание за събирането и предназначението им в регистрите се набират, обработват и съхраняват лични данни за:

1. (доп. 14.04.2016г.) физическата идентичност на лицето – имена; ЕГН/ЛНЧ; номер на документ за самоличност; дата и място на издаването му; адрес; месторождение; телефони за контакт; адрес по местоживеене; дата на раждане; всяка юрисдикция, на която лицето е местно лице за данъчни цели; данъчен номер за всяка юрисдикция, на която лицето е местно лице за данъчни цели; всяко гражданство, което лицето притежава;

2. семейна идентичност – семейно положение;

3. социална идентичност – трудова дейност, образование /вид на образованието, място, номер и дата на издаване на дипломата, допълнителна квалификация и др./;

4. икономическа идентичност – имотно състояние, финансово състояние, участие и/или притежаване на дялове или ценни книжа в дружества;

(2) (доп. 14.04.2016г.) Личните данни в регистрите се събират:

1. на хартиен или електронен носител от физическите лица, за които се отнасят данните;

2. от публични и други регистри;

3. (нова 14.04.2016г.) от трети лица /като пълномощници, законни представители/

Глава трета
ДОСТЪП ДО ЛИЧНИ ДАННИ

РАЗДЕЛ I
ДОСТЪП НА ЛИЦАТА ДО ЛИЧНИТЕ ИМ ДАННИ

Чл. 5. (1) Всяко физическо лице има право на достъп до отнасящите се до него лични данни, обработвани от ЦКБ АМ ЕАД.

(2) В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, Дружеството предоставя на съответното физическо лице достъп само за частта от данните, отнасяща се него.

(3) При упражняване на правото си на достъп физическото лице има право да поиска от Дружеството:

1. потвърждение за това, дали отнасящи се до него данни се обработват, информация за целите на това обработване, за категориите данни и за получателите или категориите получатели, на които данните се разкриват;

2. съобщение до него в разбираема форма, съдържащо личните му данни, които се обработват, както и всяка налична информация за техния източник.

(4) При смърт на физическото лице право на достъп до личните му данни имат неговите наследници.

Чл. 6. (1) Правото на достъп по чл. 5 се осъществява с писмено заявление до ЦКБ АМ ЕАД.

(2) Заявление може да бъде отправено и по електронен път по реда на Закона за електронния документ и електронния подпис.

(3) Заявлението по ал. 1 се отправя лично от физическото лице или от изрично упълномощен с нотариално заверено пълномощно пълномощник.

Чл. 7. (1) Заявлението по чл. 6 съдържа:

1. трите имена, ЕГН/ЛНЧ, адрес за контакт и телефон на заявителя;

2. трите имена и ЕГН/ЛНЧ, месторождение на починало лице; в случай, че заявлението се подава от наследник на починалото лице, към него се прилага заверено копие на удостоверение за наследници или друг документ, удостоверяващ качеството на наследник;

3. описание на искането;

4. предпочитана форма за предоставяне на достъп до личните данни;

5. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) При подаване на заявление от пълномощник към заявлението се прилага и изричното нотариално заверено пълномощно в оригинал.

Чл. 8. (1) Информацията по чл. 5, ал. 3 може да бъде предоставена под формата на устна или писмена справка.

(2) Физическото лице може да поиска копие на обработваните лични данни на предпочитан носител или предоставянето им по електронен път, освен в случаите, когато това е забранено от закон.

(3) Дружеството е длъжно да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията по чл. 5, ал. 3.

(4) Дружеството предоставя исканата информация във форма, различна от заявената, когато:

1. за исканата форма няма техническа възможност;

2. исканата форма е свързана с необосновано увеличаване на разходите по предоставянето.

Чл. 9. (1) ЦКБ АМ ЕАД разглежда заявлението по чл. 6 и се произнася в 14-дневен срок от неговото постъпване.

(2) Срокът по ал. 1 може да бъде удължен от Дружеството до 30 дни в случаите, когато обективно се изисква по-дълъг срок за събирането на всички искани данни и това сериозно затруднява нейната дейност.

Чл. 10. С решението си Дружеството предоставя пълна или частична информация на заявителя или мотивирано отказва предоставянето й.

РАЗДЕЛ II
ДОСТЪП НА СЛУЖИТЕЛИ НА ЦКБ АМ ЕАД ДО РЕГИСТРИТЕ, СЪДЪРЖАЩИ ЛИЧНИ ДАННИ

Чл. 11. (1) Право на достъп до данните в поддържаните от ЦКБ АМ ЕАД регистри на лични данни имат:

1. служителите на Дружеството, на които е възложено приемането и обработването на лични данни върху хартиен и електронен носител (обработващите лични данни – например, служителите в отдели „Управление на портфейли”, „Продажби, отношения с клиенти и маркетинг”, „Финансово-счетоводен” и др.);

2. служителите, на които е възложено да:

а) да изготвят становища и отговори по сигнали и жалби;

б) да разработват и тестват програмни средства за обработване на лични данни;

в) да изготвят статистическа информация.

(2) Служителите имат оторизиран достъп само до тези регистри и данни, които са необходими за изпълняване на конкретните им задължения, съобразно спецификата на изпълняваните от тях служебни функции. Предоставянето, промяната или прекратяването на права за обработка и достъп до регистрите на лични данни се извършва по нареждане на представляващите ЦКБ АМ ЕАД или определени от тях лица, по предложение на преките ръководители на съответните служители на Дружеството.

(3) Дружеството създава механизми за предотвратяване на достъп до регистрите на служители, различни от оторизираните.

Чл. 12. (1) Служителите с оторизиран достъп са длъжни:

1. да обработват лични данни законосъобразно и добросъвестно;

2. да използват личните данни, до които имат оторизиран достъп, съобразно целите, за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели;

3. да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.

(2) Във връзка със задълженията си по тази инструкция лицата по чл. 11, ал. 1 подписват декларация по образец – приложение № 6.

РАЗДЕЛ III
ДОСТЪП НА ТРЕТИ ЛИЦА ДО РЕГИСТРИТЕ, СЪДЪРЖАЩИ ЛИЧНИ ДАННИ

Чл. 13. (1) Достъп до обработваните от администратора лични данни имат:

1. органите на съдебната власт и други държавни органи във връзка с изпълнение на техните правомощия по закон;

2. трети лица – съконтрагенти на администратора, при наличие на изрично съгласие на лицето, чиито лични данни се обработват;

3. други лица за упражняване на правомощия, предоставени им със закон или с оглед защита на техни законни интереси.

(2) (доп. 14.04.2016г.) Правото на достъп се осъществява въз основа на писмено заявление до Дружеството, в което се посочва основанието за предоставяне на лични данни, или въз основа и при условията на пряко прилагане на закона /напр. ДОПК/.

(3) Дружеството се произнася по заявлението в 14-дневен срок от постъпването му, като с решението си предоставя или мотивирано отказва поисканата информация.

(4) Срокът по предходната алинея може да бъде удължен от Дружеството до 30 дни в случаите, когато обективно се изисква по-дълъг срок за предоставяне на исканата информация или предоставянето й сериозно затруднява нейната дейност. Когато достъпът до лични данни е поискан от орган на съдебната власт или особена юрисдикция, ЦКБ АМ ЕАД предоставя поисканата информация в указан от органа/юрисдикцията или предвиден в съответния закон срок.

Глава четвърта
ВИДОВЕ ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 14. С цел недопускането на неправомерен достъп, изменение или разпространение, случайно или незаконно унищожаване, случайна загуба и всички други незаконни форми на обработване на личните данни, ЦКБ АМ ЕАД предприема мерки, съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 15. (1) Видове защита:

1. Физическа защита на личните данни представлява система от технически и организационни мерки за предотвратяване на нерегламентиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни.

2. Персонална защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора.

3. Документална защита представлява 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.

5. Криптографската защита представлява система от технически и организационни мерки, които се прилагат с цел защита на личните данни от нерегламентиран достъп при предаване, разпространяване или предоставяне.

(2) Мерките по различните видове защита се определят съгласно приложение № 2 от настоящата инструкция.

Глава пета
ОЦЕНКА И НИВА НА ВЪЗДЕЙСТВИЕ И ЗАЩИТА

РАЗДЕЛ I
ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ОБРАБОТВАНИТЕ ЛИЧНИ ДАННИ

Чл.16. (1). Оценката на въздействието е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, цялостността или наличността на личните данни.

(2) 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. 17. При оценката на въздействието Дружеството отчита характера на обработваните лични данни, както следва:

1. систематизиране и оценка на лични 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.

РАЗДЕЛ II
НИВА НА ВЪЗДЕЙСТВИЕ

Чл. 18. Определят се следните нива на въздействие:

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. 19. (1) ЦКБ АД извършва оценка на въздействие за всички поддържани регистри, съгласно приложение № 1.

(2) Всеки отделен регистър се оценява по критериите поверителност, цялостност и наличност.

(3) Най-високото ниво на въздействие, определено по всеки от критериите по ал. 2, определя нивото на въздействие на съответния регистър.

РАЗДЕЛ III

НИВА НА ЗАЩИТА

Чл. 20. В зависимост от нивото на въздействие се определя и съответно ниво на защита.

Чл. 21. (1) Нивата на защита са ниско, средно, високо и изключително високо.

(2) 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. 22. Нивото на технически и организационни мерки, които се осигуряват в ЦКБ АМ ЕАД, са посочени в приложение № 2 от настоящата инструкция.

Глава шеста
ПРОЦЕДУРИ ЗА ДОКЛАДВАНЕ, УПРАВЛЯВАНЕ И РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ

Чл. 23. (1) При възникване и установяване на инцидент, свързан с нарушаване защитата или загуба на лични данни, незабавно се докладва на изпълнителните директори на ЦКБ АМ ЕАД.

(2) За инцидентите се води регистър, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада.

(3) В регистъра 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 изпълнителните директори на ЦКБ АМ ЕАД, като това се отразява в регистър по архивиране и възстановяване на данни.

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

Глава седма
ОТГОВОРНОСТ

Чл. 24. За нарушаване на разпоредбите на тази инструкция на виновните лица се налагат дисциплинарни наказания по Кодекса на труда, независимо от имуществената, административнонаказателната или наказателната отговорност, ако такава отговорност се предвижда по закон.

Чл. 25. (1) За вреди, причинени в резултат на незаконосъобразно обработване на лични данни от служители на ЦКБ АМ ЕАД, засегнатите лица могат да търсят отговорност от виновните лица по реда на общото гражданско законодателство или наказателна отговорност, ако извършеното представлява престъпление.

(2) Ако в резултат на незаконосъобразно обработване на лични данни, в т.ч незаконното им разкриване или разпространение, са причинени щети на администратора на виновните лица се търси имуществена отговорност по Кодекса на труда.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§1. По смисъла на тази инструкция:

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

2. „Носител на лични данни“ е физически обект, на който могат да се запишат данни или могат да се възстановят от същия.

3. „Обработване на лични данни” е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.

4. „Регистър на лични данни” е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален принцип.

5. „Достъп до лични данни” е предоставената по надлежен ред възможност за използване на поддържаните от администратора регистри на лични данни, без данните да бъдат коригирани, заличавани или унищожавани.

6. „Лице по защита на личните данни” е физическо лице, притежаващо необходимата компетентност, което е упълномощено или назначено от администратора със съответен писмен акт, в който са уредени правата и задълженията му във връзка с осигуряване на минимално необходимите технически и организационни мерки за защита на личните данни при тяхното обработване.

7. „Ниво на защита” 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.

8. „Поверителност“ е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.

9. „Цялостност“ е изискване данните да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване и изискване да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.

10. „Наличност“ е изискване за осигуряване непрекъсната възможност за обработване на личните данни на оторизираните лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване.

11. „Инцидент” е непредвидимо обстоятелство, което би могло да засегне сигурността на данните.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 2. Настоящата инструкция е приета на 31.07.2013г. от Съвета на директорите на ЦКБ АМ ЕАД, на основание чл. 23, ал. 4 от Закона за защита на личните и чл. 19, т. 2 от Наредба № 1 от 30 Януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, изм. на 28.04.2016г. /в сила от 01.05.2016г/.

§ 3. Инструкцията влиза в сила от 01.08.2013 г.