# ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В СИСТЕМАТА НА ИНВЕСТБАНК АД

**ИНВЕСТБАНК АД**

**ГЛАВА ПЪРВА**
**ОБЩИ ПОЛОЖЕНИЯ**

В качеството си на администратор на лични данни по смисъла на чл.3 от Закона за защита на личните данни и чл. 4, ал. 7 от Регламент №679 относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, Банката отдава сериозен приоритет за спазване на законовите изисквания относно защита на банкова тайна и лични данни. Инвестбанк АД събира и обработва лични данни на свои служители, администратори, акционери, клиенти, доставчици/контрагенти/ и трети свързани лица, извън кръга на тези, на които предлага финансови услуги. В тази връзка е необходимо да се дефинират механизмите за защита на техните интереси по повод обработката на личните им данни.

**Раздел I**
**Приложимо законодателство**

**Чл.1.** Настоящите Правила отговарят на изискванията на действащото законодателство в България и Европейския съюз (Съюза), което включва:

1. Регламент 2016/679 на Европейския парламент и на Съвета от 27 април 2016 относно защита на физическите лица при обработване на лични данни и свободно придвижване на тези данни, отмяна на Директива 95/46/ЕС(накратко Общ регламент за защита на лични данни).
2. Директива 2002/58/ЕС на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации).
3. Директива 2009/136/ЕС на Европейския парламент и на Съвета от 25 ноември 2009 година за изменение на Директива 2002/22/ЕО относно универсалната услуга и правата на потребителите във връзка с електронните съобщителни мрежи и услуги, Директива 2002/58/ЕО относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации и Регламент (ЕО) № 2006/2004 за сътрудничество между националните органи, отговорни за прилагане на законодателството за защита на потребителите.
4. Закон за защита на лични данни.
5. Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.

**Раздел II**
**Цел и предмет, обхват**

**Чл.2. (1)** Настоящите Правила имат за цел:

1. Да се гарантира неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица срещу неправомерно

обработване на свързаните с тях лични данни във връзка с процеса на свободното движение на данните.

2. Да се осигури обработването на лични данни да бъде приложено в пълно съответствие с изискванията на действащото законодателство.
3. Да се приложи поверителност по професионален начин по отношение на обработването на лични данни на всички субекти на данни.
4. Да се приемат ясни правила и процедури, регламентиращи управлението на лични данни, обработвани от Банката по време на дейността й и всички правоотношения.
5. Да се повиши осведомеността на служителите и да им се предоставят указания как да избегнат всеки акт, който води до неправомерно обработване на лични данни и налагане на административни санкции на Банката.
6. Да се гарантира защита и намали репутационния риск за Банката.
7. Да се установи адекватно ниво на защита на личните данни в поддържаните от Банката регистри чрез осигуряване на необходимите технически и организационни средства и мерки.
8. Да се определят основните задължения на дирекция “Предотвратяване изпирането на пари и специализиран нормативен контрол” /ПИПСНК/ и на ръководните длъжностни лица, отговорни за спазването на законовите норми при обработката на лични данни в системата на Банката и изготвянето на необходимите регистри и уведомления.

**(2)** Тези Правила се прилагат за обработката на лични данни с:

1. неавтоматизирани средства, когато тези данни съставляват или са предназначени да съставляват част от регистър.
2. автоматизирани средства;

**Чл.3. (1)** Правилата, като вътрешно нормативен акт са задължителни за следните категории лица:

1. Всички служители на Инвестбанк, което включва целия мениджърски състав и административен персонал на трудови, граждански договори и други.
2. Всички трети лица, които доставят услуги от свое име или от името на банката, което включва бизнес партньори, посредници, агенции, агенти или други лица, с които банката има договорни отношения за аутсорсинг или други търговски отношения.

**(2)** Правилата обхващат:

1. Всички дейности на банката в страната и чужбина, включително правоотношения с лицата по предходната алинея, други трети лица, действащи от свое име или от името на банката.
2. Всички лични данни на хартиен и на електронен носител, които се обработват във връзка с дейността на банката.
3. Ръчно и автоматизирано обработване на лични данни.

**Раздел III**

**Позиции и отговорности**

**Чл.4.** Управителният съвет на Инвестбанк одобрява настоящите правила и последващите им изменения.

**Чл.5.** Изпълнителните директори на Инвестбанк следят за изпълнението на изискванията на вътрешните правила в банката.

**Чл.6. (1)** Дирекция ПИПСНК има следните основни задължения, свързани с настоящите Правила:

1. отговаря за извършване на анализ за ефективност на законодателството и добрите практики в областта на защита на лични данни, въз основа на който ще извършва периодичен преглед на правилата. При необходимост ще предприема мерки по своевременното им актуализиране и придвижване до УС на банката.
2. организира обучения и информира служителите за задълженията им (подаване на декларации, уведомления, воденето на регистри и др.) съгласно действащото национално и европейско законодателство във връзка с обработване на лични данни. Повишава осведомеността на служителите чрез публикуване на указания чрез вътрешния портал и актуализира знанията на служителите в съответствие с приложимото законодателство и добрите практики в ЕС.
3. извършва периодичен преглед на съществуващите механизми за защита на информацията, свързана с личните данни на физическите лица/субекти на данни и спазването на законовите изисквания.
4. води регистър на заявленията **по чл. 16, ал.2** от настоящите Правила.
5. поддържа кореспонденция с националния регулатор – КЗЛД относно запитвания и разяснения по приложението на действащото законодателство.

**Чл.7. (1)** Длъжностно лице по защита на лични данни има следните задължения:

1. Контролира процеса по разглеждане на молби, свързани с обработването на лични данни на физически лица и упражняване на техните права. Периодично прави преглед на рисковете от неправомерно обработване на лични данни, на принципа на поверителност при изпълнение на задачите си. След това предлага решение за всяко заявление за достъп.
2. Да наблюдава измененията на Регламент за защита на лични данни №679 ЕС и на други разпоредби за защитата на данни на равнище Европейски съюз или държава членка и спазването на политиките на администратора или обработващия лични данни 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.
3. При поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката.
4. Оценява наличието и приоритета на законен интерес на банката спрямо интересите на физическите лица, в случай на искане за достъп до клиентски

данни от трети лица и предлага решение за предоставянето им. Контролира, оказва съдействие при изготвянето и съхранява изготвените от звената-собственици на данните балансиращи тестове в случаите, когато лични данни се обработват на основание законен интерес на банката.

5. Поддържа списък с регистрите, поддържани от банката и видовете данни в тях и периодично ги актуализира след получаване на необходимата информация от другите звена в банката, които са собственици на данните.
6. Предоставя указания за работа с данните във всеки от регистрите и правото на служителите за достъп в банката до информация в съответния регистър. Извършва преглед относно контролиран достъп на служителите в съответствие със спецификите на поддържаните регистри и нивата на въздействие и чувствителност на данните при обработване на лични данни във връзка с техническите и програмно – информационни ресурси използвани за обработка на лични данни.
7. Периодично информира мениджърския състав и административния персонал (на трудови и граждански договори) относно казуси и въпроси, свързани със защита на личните данни в банката.
8. Координира действията на длъжностните лица по прилагане на необходимите технически и организационни мерки за защита на личните данни.
9. Поддържа актуален списък от задължителни и препоръчителни мерки за осигуряване на необходимото ниво на защита на личните данни съобразно вида и чувствителността на данните /**Приложение №2** от настоящите Правила/;
10. Установява обстоятелства, свързани с нарушаване защитата на регистрите и дава препоръки за отстраняването на нарушения.
11. Заедно с Дирекция ПИПСНК предлага мерки за отстраняване на причини, довели до жалби, свързани със защита на лични данни.
12. Действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация, и по целесъобразност да се консултира по всякакви други въпроси. Заедно с Дирекция ПИПСНК оказва съдействие при осъществяване на контролните функции на КЗЛД.

**Раздел IV**

**Основни определения**

**Чл.8.** Основните определения по смисъла на настоящите Правила са:

(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 автоматизирани 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;

(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) „Директен маркетинг“ е предлагане на стоки и услуги на физически лица по пощата, по телефон или по друг директен начин, както и допитване с цел проучване относно предлаганите стоки и услуги.

(14) „Длъжностно лице по защита на личните данни" е физическо или юридическо 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.

(15) „надзорен орган“ означава независим публичен орган, създаден от държава членка съгласно член 51; Комисията за защита на личните данни е независим държавен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Закона за защита на личните данни в България.

## ГЛАВА ВТОРА
## ОБЩИ ПРАВИЛА ОТНОСНО ЗАКОННОСТТА НА ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ В ИНВЕСТБАНК

### Раздел I
### Принципи, отнасящи се до качеството на данните

**Чл.9. (1)** Личните данни трябва да се обработват законосъобразно и добросъвестно. Банката обработва данните на **лицата по чл. 10** като следи данните да бъдат точни и при необходимост да се актуализират, да се заличават или коригират, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват, както и да се поддържат 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)** Данните се събират за конкретни, точно определени цели при условие, че е осигурена подходяща защита и гаранция, че данните не се обработват за други цели и да бъдат съотнасяни, свързани с и не надхвърлящи целите, за които се обработват, което включва, но не само:

1. проверка на общи условия и договори за влизане в договорни отношения
2. изпълнение и изследване на договорни отношения
3. оценка на ефективност на всички видове банкови операции – през алтернативни мрежи, приемане на всички видове заявления през електронни канали на комуникация
4. уведомяване на клиенти през всички комуникационни канали – официален интернет сайт, телефон, текстови съобщения, електронна поща и други
5. управление на заплати на служители в банката в рамките на трудовото законодателство и организацията на работа
6. заплащане на задължения по фактури
7. данъчни цели
8. привеждане в съответствие на задължителни предписания от БНБ
9. защита на интересите и репутацията на банката
10. осигуряване на защита при изпълнение на трансакции.
11. защита на каналите и средствата за отдалечен достъп на клиентите до предлаганите от Банката услуги

**(3)** Забранено е обработването на лични данни, които:

1. разкриват расов или етнически произход;
2. разкриват политически, религиозни или философски убеждения, членство в политически партии или организации, сдружения с религиозни, философски, политически или синдикални цели;
3. се отнасят до сексуалния живот или до човешкия геном.

**(4)** Алинея 3 не се прилага, когато:

1. Обработването е наложително по силата на закон или друг нормативен акт или за спазването на правно задължение, чийто субект е банката;
2. Лицето, за което се отнасят, е дало предварително писменото си съгласие или обработването се отнася до данни, публично оповестени от физическото лице, или то е необходимо за установяването, упражняването или защитата на права на Инвестбанк по съдебен ред.

**(5)** Задължителни условия при предоставяне на съгласие:

1. Когато обработването се извършва въз основа на съгласие, Инвестбанк АД може да докаже, че субектът на данни е дал съгласие за обработване на личните му данни при следните задължителни условия:

а) свободно изразено – не дадено под натиск или заплаха от неблагоприятни последици
б) конкретно отделно съгласие за всяка определена цел
в) информирано – дадено на основата на пълна, точна и лесно разбираема информация
г) недвусмислено – не се извлича или предполага на основата на други изявления или действия на физическото лице/субект на данните

д) изрично изявление или ясно потвърждаващо действие – Банката не прилага мълчаливо съгласие от физическото лице.

2. Съгласието на субекта на данните/физическото лице е дадено в рамките на писмена Декларация за съгласие на клиенти (предоставяно за подпис на настоящи клиенти на Банката – **Приложение №6,** от настоящите правила и в Декларация и анкетен лист за физически лица – Приложение 6А, предоставяно за подпис на нови клиенти - физически лица) в Инвестбанк в разбираема и лесно достъпна форма, в която се използва ясен и разбираем език и са спазени условията по предходната точка.

3. 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 е информиран за това в самата декларация.

**Раздел II**

**Физически лица/Субекти, чиито лични данни се обработват в банката**

**Чл.10.** В Инвестбанк се обработват данни на следните лица:

(1) акционери
(2) настоящи и потенциални клиенти
(3) всички клиенти, включително ползващи платежни услуги, инвестиционни услуги, кредитополучатели, гаранти, други лица, имащи договорни отношения с банката
(4) всички служители на банката (на трудови, граждански и договори за управление, други)
(5) доставчици, посредници, агенти и други бизнес партньори, имащи търговски правоотношения с банката.

**Раздел III**

**Категории получатели на обработваните в банката данни**

**Чл.11.** В позволените от закона случаи, банката предоставя лични данни на следните трети лица:

1.държавни и общински органи и институции

2. надзорни органи, съдебни и други регулаторни органи, отговарящи за надзор върху задълженията на банката: БНБ, КФН, КЗП, КЗК, КЗЛД, ДАНС АФР, други публични държавни органи в страната и чужбина, прокуратура и следствие, нотариуси и други съгласно **Приложение №3** от настоящите правила.

3. Застрахователни и осигурителни дружества

4. Кредитни регистри и бюра, дружества, специализирани в оценка и анализ на риск

5. Колекторски дружества

6. По отношение на извършване на електронни презгранични транзакции, пренос на съпътстващи данни към оператори на платежни системи и други компании за обработване на платежни операции.

**Раздел IV**

**Задължения на Инвестбанк в качеството на администратор на лични данни**

**Чл.12. (1)** Банката въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки, които са разработени с оглед на ефективното прилагане на принципите за защита на данните, интегриране на необходимите контроли в процеса на обработване, за да се осигури защита на правата на субектите на данни.

1. псевдонимизация и криптиране на личните данни;
2. свеждане на данните до минимум;
3. способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;
4. способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;
5. процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

**(2)** Банката 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.

**(3)** При поискване банката и обработващият лични данни (от свое име или от името на банката) и — когато това е приложимо — техните представители си сътрудничат с надзорния орган при изпълнението на неговите задължения.

**(4)** Уведомяване на надзорния орган за нарушение на сигурността на личните данни в случай на нарушение на сигурността на личните данни. Банката, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрала за него, уведомява за нарушението на сигурността на личните данни надзорния орган, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи 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.

**(5)** Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, банката, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

**(6)** Да осигури подходящо обучение за защита на данните за персонала, който постоянно или редовно има достъп до лични данни.

**Раздел V**

**Регистри, водени от администратора**

**Чл.13.(1) При осъществяване на своята дейност банката създава и организира регистри за лични данни в следните направления:**

1. **Регистър за лични данни на клиентите** при извършване на платежни услуги и платежни операции съгласно Закона за платежните услуги и платежните системи и подзаконовите актове по прилагането му; При извършване на кредитиране и други специфични банкови сделки съгласно Закона за кредитните институции /ЗКИ/, Закон за потребителски кредит/ ЗПК/, ЗКНИП; При извършване на дейност като инвестиционен посредник и/или регистрационен агент по смисъла на Закона за пазарите на финансови инструменти /ЗПФИ/ и подзаконовите актове по прилагането му в това число и Наредба № 38/2007г. на КФН за изискванията към дейността на инвестиционните посредници /НИДИП/.
2. **Регистър за лични данни на служители** при сключването на трудови договори и създаване на трудови досиета по реда на Кодекса на труда и всички произтичащи от това задължения за банката като осигурител по смисъла на Кодекса за социалното осигуряване и подзаконовите актове по прилагането му.
3. **Регистър за лични данни за изпълнители на възложени дейности, доставчици и други контрагенти** при осъществяване на вменените й, съгласно Търговския закон, ЗКИ, ЗПФИ задължения за събиране на данни относно членовете на Управителния и Надзорния съвет на свои контрагенти, доставчици и други свързани лица.
4. **Регистър Видеонаблюдение** при извършване на охранителна дейност в публично достъпни места и специални зони на действие.

**(2)** Регистрите се водят документално, на хартиен носител и/или картотечно и автоматизирано на електронен носител чрез компютърна програма. Данните, които се събират и обработват, са съгласно нормативните изисквания и вътрешните актове на банката и се съхраняват в срокове съгласно Закона за държавния архив, Закона за мерките срещу изпиране на пари и специалните закони, регламентиращи банковата и счетоводна дейност.

**(3)** В регистрите се обработват лични данни на физически лица - клиенти на дружеството, служители, лица, които поръчителстват или предоставят друго обезпечение по кредитни сделки, пълномощници, други контрагенти или лица, свързани с дейността на банката.

**Чл.14. (1)** В съответствие с нивото на въздействие на обработваните данни, Инвестбанк прилага подходящи организационни и технически мерки, за да осигури защитата на лични данни от неумишлено или незаконно унищожаване, случайна загуба, преправяне, неоторизирано разкриване или достъп, както всяка друга форма на незаконно обработване. Мерките за защита кореспондират с рисковете, отнасящи се до обработване и чувствителност на данните при обработване и са посочени в **Приложение №1** от настоящите правила, като може да бъдат прилагани и допълнителни мерки.

**(2)** При водене на **регистрите на хартиен носител** се спазват следните изисквания, като списъка не е изчерпателен:

1. всички оригинали на документи се съхраняват в заключващи се метални шкафове, разположени на места, предназначени за самостоятелна работа на служители.

2. документи, съдържащи по-чувствителна информация се съхраняват регулярно в огнеупорни сейфове със специален достъп до служебна зона.
3. обособени са архивохранилища, предназначени за съхраняване на документи.
4. сградите се охраняват с физическа охрана в работно време и сигнално охранителна техника (СОТ) извън работно време, оборудвани със системи за контрол на достъпа и пожароизвестяване и са под денонощен мониторинг.
5. при обработване на данни от служители се спазват принципите „необходимо да се знае“ и „необходимо да се ползва“.
6. копия от документи, размножени документи и чернови се унищожават след постигане на целта, за която са били използвани.
7. след изтичане на сроковете за съхранение на всички документи от финансовите центрове и Централно управление се предават за траен архив по решения на ръководните им органи.

**(3)** При водене на **регистрите на технически носител** се спазват следните изисквания за защита, но не само:

1. В процеса на обработка, данните се въвеждат, обработват и съхраняват в предварително подготвени компютърни системи, . Компютрите са свързани в локалната мрежата за обработка на данни на Банката с контролиран и защитен чрез пароли достъп до личните данни, който е непосредствен от страна на служителите.

2. Правата за достъп на всеки служител се предоставят съгласно утвърдени Типови карти и обезпечават нормалната работа на служителите при спазване на основни принципи като „втори контрол“ и „даване само на необходимите права за изпълнение на възложените функции и задължения на служителя“. Системите регистрират всеки достъп от страна на служители.

3. Сървърите с бази данни на регистрите са разположени дейта център/сървърно помещение с контролиран достъп.

4. Инвестбанк е въвела в експлоатация следните системи за осигуряване защитата на обработваните данни:

а) система за контрол за мрежовия достъп (firewalls) за защита на външния периметър с изградена DMZ зона за услуги, като web приложенията на банката.

б) система за откриване и предотвратяване на DDoS атаки през ТАТА.

вб) система за защита от вируси и вредоносен код (малуеър) на Kaspersky, с централизирано управление и обхваща всички работни станции и сървъри, съхраняващи информация.

в) достъпът до Интернет в банката се ограничава с продукта BlueCoat, предоставящ възможност за анализ на трафика към интернет и позволяващ филтриране на web страници, по съдържание и протоколи. .

г) система за антиспам защита Barracuda, предоставяща защита от спам и нежелани съобщения, разпространявани по електронна поща от Банката към интернет и обратно.
.

д) безжична комуникация (wireless) е разрешена само за мобилни компютри с криптиране на връзката.

е) системи за събиране, анализ и мониторинг на събития от основните мрежови компоненти и сървъри.

5. Обменът на информация и защитата на каналите за пренос на информация са определени в “Политика за информационна сигурност на „Инвестбанк“ АД“.

6. Унищожаване/заличаване/изтриване на данни върху технически (респ. електронни) носители са регламентирани в “Политика за информационна сигурност на „Инвестбанк“ АД“.

7. За всички служители, които са потребители в инфраструктурата на Инвестбанк, се използва PKI (Public key infrastructure). За достъп до електронни услуги на държавни органи и регистри се използват КЕП (квалифицирани електронни подписи), издадени от доставчик на удостоверителни услуги. За всички уеб базирани публични финансови електронни услуги, които се предоставят от Банката, е задължително използване на защитена комуникация чрез SSL/TLS/. Цифровите сертификати/удостоверения за идентичност, които са инсталирани на сървърите, предоставящи публични електронни услуги, са издадени от специализирани компании за издаване на цифрови (SSL) сертификати.

8. За осигуряване на непрекъсваемост на критични бизнес процеси в Инвестбанк, информационните системи които ги обезпечават, са дублирани, като са разположени в основен и резервен център за обработка на данни в банката.

**(4)** В клонова мрежа и централно управление са разработени планове за непрекъсваемост на бизнеса и за възстановяване на след бедствия. Те са изготвени с цел минимизиране на последици от евентуални бедствия чрез разработване на принципи за смекчаване на въздействието, съобразени с естеството, интензитета и предполагаемата честота на възникване на оперативни рискове. Защита на персонала, опазване и приоритизиране на технологичната и оперативна инфраструктура, стимулиране на нуждата за защита на работна среда по време на и след бедственото събитие, елиминиране на липсата на координация, постигане на възстановяване на бизнеса в рамките на приемливи срокове, обучения и тренировки за действие при бедствия са уредени подробно в „План за непрекъсваемост на бизнеса на „Инвестбанк” АД“.

**Чл.15. (1)** Длъжностните лица, осъществяващи достъп до лични данни, ги обработват съобразно длъжностните си характеристики и на принципите „необходимост да се ползва“ и „необходимост да се знае“, както и съгласно подписана Декларация за опазване тайната на личните данни, отнасяща се за служители, администратори (мениджърски състав) и лица, с които е сключен граждански договор в „Инвестбанк” АД

– **Приложение №4 от настоящите правила**. Възможността за предоставяне на достъп до данните на друго лице, е ограничена и изрично регламентирана в настоящите правила.

**(2)** Обработващи са всички служители в клонова мрежа, с достъп съгласно Картите за достъп до информационните и счетоводните системи в зависимост от функционалните задължения при осъществяване на служебните си задължения.

**(3)** Обработващи в централно управление са служители от определени дирекции, съгласно възложените им функционални задължения.

## ГЛАВА ТРЕТА
## ПРАВА НА ФИЗИЧЕСКИТЕ ЛИЦА, СУБЕКТИ НА ЛИЧНИ ДАННИ ПРИ ОБРАБОТВАНЕ В ИНВЕСТБАНК

### Раздел I

### Комуникация и условия за упражняване правата на физическите лица (субекти на данните)

**Чл.16. (1)** Инвестбанк осигурява изследване на поддържаната информация, съдържаща лични данни на физически лица. Всяко физическо лице има право да получи информация, която включва право за получаване за предходни периоди и право за достъп до настоящ период (преди, по-време на и след обработване).
**(2)** Съобщението до субекта на данни се изпраща в кратка, прозрачна, разбираема и лесно достъпна форма. Информацията се предоставя писмено или по друг начин, включително, когато е целесъобразно, с електронни средства, съдържа личните му данни, които се обработват, както и всяка налична информация за техния източник.
**(3)** За изпълнението на своите информационни задължения, банката в случай на необходимост предоставя допълнително релевантни документи, свързани с обработваните данни.
**(4)** Банката предоставя на субекта на данни информация относно действията, предприети във връзка с подадено заявление/искане по **членове 17—25**, без ненужно забавяне и във всички случаи **в срок от един месец** от получаване на искането/заявлението. При необходимост този срок може да бъде удължен **с още два месеца**, като се взема предвид сложността и броя на исканията.
**(5)** Банката информира субекта на данните за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето.
**(6)** Банката отказва да предприеме действия по искане на субекта на данните за упражняване на правата му по **членове 17—25**, когато не е в състояние да идентифицира субекта на данните.
**(7)** Банката предоставя информацията по **ал.2** безплатно. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, Инвестбанк може или:

1. да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или

предприемането на исканите действия съгласно Тарифа за такси и комисионни на банката,

или

2. да откаже да предприеме действия по искането.

**(8)** При смърт на физическото лице правата му се упражняват от неговите наследници.

**Раздел II**

**Право на информация и право на достъп на физическите лица, чиито лични данни се обработват от Банката в качеството и на администратор**

**Чл.17. (1)** Информация, предоставяна от длъжностните лица в Банката, при събиране на лични данни от субекта на данните :

1. данните, които идентифицират администратора, координатите за връзка с него и, когато е приложимо, тези на представителя на администратора;
2. координатите за връзка с длъжностното лице по защита на данните;
3. целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;
4. информация за обработването когато то 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;
5. получателите или категориите получатели на личните данни, ако има такива;
6. когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни, позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични.

Посочената по-горе информация се предоставя на субекта на данните, при поискване от негова страна, по ясен и недвусмислен начин и съгласно Декларация за поверителност – Приложение №5 от настоящите правила, освен в случаите, когато той вече я притежава.

**(2)** Освен информацията, посочена в ал. 1, в момента на получаване на личните данни банката предоставя на субекта на данните следната допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване:

1. срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;
2. съществуването на право да се изиска от администратора 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;

3. когато обработването се основава на съгласие, дадено от субектът на данните за обработване на личните му данни за една или повече конкретни цели, 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;
4. правото на жалба до надзорен орган;
5. 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 последствия, ако тези данни не бъдат предоставени;
6. съществуването на автоматизирано вземане на решения, включително профилирането, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

(3) Когато банката възнамерява по-нататък да обработва личните данни за цел, различна от тази, за която са събрани, тя предоставя на субекта на данните, преди това по-нататъшно обработване, информация за тази друга цел и всякаква друга необходима информация, както е посочено в ал. 2.

**Чл.18. (1)** Когато личните данни не са получени от субекта на данните, банката предоставя на субекта на данните информацията по **чл. 17, ал.1, т.1-6.**

**(2)** Освен информацията, посочена в ал. 1, банката предоставя на субекта на данните следната информация, необходима за осигуряване на добросъвестно и прозрачно обработване на данните по отношение на субекта на данните съгласно **чл. 17, ал.2, т.1-6**, включително източника на личните данни и, ако е приложимо, дали данните са от публично достъпен източник.

**(3)** Банката/Администраторът предоставя информацията, посочена в алинеи 1 и 2 чрез Декларацията за поверителност – **Приложение №5**, която се публикува и се актуализира на интернет страницата на Банката:

1. в разумен срок след получаването на личните данни, но най-късно в срок до един месец, като се отчитат конкретните обстоятелства, при които личните данни се обработват;
2. ако данните се използват за връзка със субекта на данните, най-късно при осъществяване на първия контакт с този субект на данните; или
3. ако е предвидено разкриване пред друг получател, най-късно при разкриването на личните данни за първи път.
4. Когато банката/администраторът възнамерява да обработва личните данни по-нататък за цел, различна от тази, за която са събрани, той предоставя на субекта на данните преди това по-нататъшно обработване информация за тази друга цел и всякаква друга необходима информация, както е посочено в **алинея 2**.

**(4)** За Инвестбанк отпадат задълженията по ал. 1-3, когато и доколкото субектът на данните вече разполага с информацията.

**Чл.19.** (1) Правото на достъп на физическите лица (субекти на данни). Субектът на данните има право да получи от банката потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация:

1. целите на обработването;
2. съответните категории лични данни;
3. получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави или международни организации;
4. когато е възможно, предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;
5. 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;
6. правото на жалба до надзорен орган;
7. когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;
8. съществуването на автоматизирано вземане на решения, включително профилирането, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия 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)** Банката предоставя копие от личните данни, които са в процес на обработване. За допълнителни копия, поискани от субекта на данните, банката може да наложи такса въз основа на административните разходи съгласно Тарифа за такси и комисионни. 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)** Заявлението за осъществяване на достъп е по образец на банката (Приложение №7). При подаването му от страна на субект на данни, служителят от ФЦ го завежда в програма Архимед и го насочва към Дирекция ПИПСНК. **Във ФЦ не се извършват справки и не се дават разяснения за обработваните лични данни.**

**(5)** Дирекция ПИПСНК организира съвместно с Дирекция ИТ съставянето на справката с лични данни, обработвани в банката за лицето, подало заявлението.

**Раздел III**

**Право на коригиране и право на изтриване на лични данни на физическите лица/субекти на данни**

**Чл.20.** Право на коригиране на събраните данни на физическите лица (субекти на данни). Всеки субект на данни има право да поиска от банката 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.

**Чл.21. (1)** Право на изтриване (право „да бъдеш забравен“) е правна възможност на субекта на данни да поиска от банката изтриване на свързаните с него лични данни без ненужно забавяне, а банката има задължението да изтрие без ненужно забавяне личните данни, когато е приложимо някое от посочените по-долу основания:

1. личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
2. субектът на данните оттегля своето съгласие, върху което се основава обработването на данните, **и няма друго правно основание за обработването**;
3. субектът на данните възразява срещу обработването съгласно **чл. 24, ал. 1** и няма законни основания за обработването, които да имат преимущество, или субектът на данните възразява срещу обработването съгласно **член 24, ал. 2**;
4. личните данни са били обработвани незаконосъобразно;
5. личните данни са били събрани във връзка с прякото предлагане на услуги на деца. Обработването на данни на дете е законосъобразно, ако детето е поне на 16 години. Ако детето е под 16 години това обработване е законосъобразно само ако и доколкото такова съгласие е дадено или разрешено от носещия родителска отговорност за детето.

**(2)** Когато банката е направила личните данни обществено достояние и е задължена съгласно алинея 1 да изтрие личните данни, като отчита наличната технология и разходите по изпълнението, предприема технически мерки, за да уведоми други администратори, обработващи личните данни, че субектът на данните е поискал изтриване от тези администратори на всички връзки, копия или реплики на тези лични данни.

**(3)** Алинеи 1 и 2 **НЕ** се прилагат, доколкото обработването е необходимо:

1. за целите на трудовата медицина и за оценка на трудоспособността на служителя;
2. за целите на архивирането, за научни или исторически изследвания или за статистически цели. В тези случаи обработването подлежи на подходящи гаранции, които осигуряват наличието на технически и организационни мерки, по-специално с оглед на спазването на принципа на свеждане на данните до минимум. Мерките могат да включват псевдонимизация, при условие че посочените цели могат да бъдат постигнати по този начин. Когато посочените цели могат да бъдат постигнати чрез по-нататъшно обработване, което не позволява или повече не позволява идентифицирането на субектите на данни, целите се постигат по този начин, доколкото съществува вероятност правото на изтриване да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или
3. за установяването, упражняването или защитата на правни претенции.

**Чл.22. (1)** Субектът на данните има право да изиска от банката **ограничаване** на обработването, в следните случаи:

1. точността на личните данни се оспорва от субекта на данните. В този случай ограничаването на обработването е за срок, който позволява на банката да провери точността на личните данни;
2. обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрити, а изисква вместо това ограничаване на използването им;
3. банката 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;
4. субектът на данните е възразил срещу обработването в очакване на проверка (тест за балансиране) дали законните основания на банката имат преимущество пред интересите на субекта на данните.

**(2)** Когато обработването е ограничено съгласно алинея 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.

**(3)** Когато субект на данните е изискал ограничаване на обработването съгласно ал. 1, банката го информира преди отмяната на ограничаването на обработването.

**Чл.23. (1)** Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на банката, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли (**право на преносимост**) тези данни на друг администратор без възпрепятстване от банката, когато:

1. обработването е основано на съгласие или на договорно задължение, 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 и

2. обработването се извършва по автоматизиран начин.

**(2)** Когато упражнява правото си на преносимост на данните по алинея 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 алинея 1 от настоящия член не засяга правото на изтриване на данните.

**(4)** Правото, посочено в алинея 1, не влияе неблагоприятно върху правата и свободите на други лица.

**Раздел IV**

**Право на възражение и автоматизирано вземане на индивидуални решения**

**Чл.24. (1)** 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, включително профилиране. Банката прекратява обработването на личните данни, 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 алинеи 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.

**(6)** Когато лични данни се обработват за целите на научни или исторически изследвания или за статистически цели, субектът на данните има право, въз основа на конкретното си положение, да възрази срещу обработването на лични данни, отнасящи се до него, освен ако обработването е необходимо за изпълнението на задача, осъществявана по причини от публичен интерес.

**Чл.25.(1)** Субектът на данните има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за субекта на данните или по подобен начин го засяга в значителна степен.
**(2)** Алинея 1 не се прилага, ако решението:
1. е необходимо за сключването или изпълнението на договор между субект на данни и банката;
2. се основава на изричното съгласие на субекта на данни.
**(3)** В случаите, посочени в алинея 2, т.1 и 2, банката 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 банката, правото да изрази гледната си точка и да оспори решението.

**Чл.26. (1)** Заявлението от клиента за получаване на **съобщението за упражняване на права по чл. 16, ал. 2** съдържа следните реквизити:

1. име, адрес и други данни за идентифициране на съответното физическо лице;
2. описание на искането;
3. предпочитана форма за предоставяне на информацията;
4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

**(2)** При подаване на заявление от упълномощено лице към заявлението се прилага и нотариално заверено пълномощно.

## ГЛАВА ЧЕТВЪРТА
## СПЕЦИАЛНИ ПРАВИЛА И ПРИНЦИПИ ПРИ УПРАВЛЕНИЕ НА ЛИЧНИ ДАННИ ВЪВ ВРЪЗКА С ТЯХНОТО ОБРАБОТВАНЕ В ХОДА НА ОСЪЩЕСТВЯВАНЕ ДЕЙНОСТТА НА ИНВЕСТБАНК

### Раздел I
### Контрол на достъпа на служители до документи, съдържащи лични данни в системата на банката

**Чл.27. (1)** Служителите на Инвестбанк, които имат достъп до документи на хартиен и електронен носител, съдържащи лични данни, дефинирани в настоящите правила, използват достъпа си само в рамките на изпълнение на техните служебни задължения. Следва да се отбележи, че нарушение на законовите изисквания включва не само изтичане на информация, но и всяко изследване или възстановяване на информация без законно основание (доказателство за предоставено съгласие или уведомление от субекта на данни или служебна свързана причина във връзка с изпълнение на договорно задължение).

**(2)** Всяко проучване на данни, което не е адекватно обосновано или оторизирано, е абсолютно забранено и може да бъде открито от системите на банката.

**(3)** Всеки достъп до лични данни, който не е оторизиран или не е обоснован за конкретна цел, е забранен, освен ако не бъде приведен в съответствие с вътрешните правила на банката в конкретния случай.

**(4)** За да бъде елиминирана възможността от нерегламентирано ползване на електронните системи на банката от служители за извличане на лични данни на клиенти или други служители (информация за салда по сметки, детайли по транзакции, друга информация, представляваща банкова тайна и съответно лични данни за финансова идентичност) се използват включително и следните механизми: 1. указания, предоставяни на регулярна база от компетентни длъжностни лица по защита на лични данни, 2. повишен мониторинг от Специализирана служба за вътрешен одит със съдействието на Дирекция ПИПСНК, които следва да откриват нередности. При никакви обстоятелства тези данни не бива да бъдат използвани за лични цели и знание, както и да бъдат предавани на трети лица в/извън банката, освен когато обработваните лични данни се използват единствено за целите на работния процес.

### Раздел II
### Предоставяне на информация във връзка с данъчни служби, съдебни, разследващи и други органи с държавни правомощия

**Чл.28.(1)** В рамките на текущи разследвания, извършвани от различни регулаторни органи съгласно **Приложение №3** от настоящите правила, Инвестбанк е задължена по специален закон да предоставя включително лични данни за салда, наличности по сметки и детайли по транзакции на свои клиенти – информация, представляваща банкова тайна и лични данни за финансова идентичност.

(2) Цялата свързана информация по ал.1 е конфиденциална и освен че се предоставя на субектите на данни, при изрични обстоятелства може да бъде предоставяна и на трети

лица, спазвайки реда за предоставяне и разкриване на банкова тайна (респективно разследващи органи, БНБ, Комисия за отнемане на незаконно придобито имущество, икономическа полиция, данъчни служби /НАП/ и други). В тези случаи, субекта на разследване не бива да бъде уведомяван за разкриване на негови данни, отнасящи се до финансовата му идентичност към органи, разследващи финансови престъпления.

**Раздел III**

**Забрана за уведомяване на субекта на лични данни във връзка с разследване по повод изпиране на пари**

**Чл.29.(1)** От първостепенно значение за всички служители на банката, отговарящи за конфиденциалността в хода на всяко разследване във връзка с изпиране на пари, е да се въздържат от оповестяване на информация за заподозрени лица, които са субекти на данните.

**(2)** Строго забранено е служителите на Инвестбанк да предупреждават клиенти, които са обект на разследване, както и други трети лица, когато информацията е изискана и разкрита на компетентните органи, без значение дали разследването във връзка с изпиране на пари или финансиране на тероризъм е текущо или потенциално.

**(3)** Строги административни санкции се налагат на всеки служител при нарушение на неговите задължения, отнасящи се до правната рамка за изпиране на пари или финансиране на тероризъм.

**Раздел IV**

**Обработване на лични данни при работа с Централния кредитен регистър (ЦКР)**

**Чл.30. (1)** При взаимодействие с Централният кредитен регистър на БНБ, на Инвестбанк е предоставен обособен достъп до услугите като вписана кредитна институция. Достъпът е свързан със специфични изисквания, определени с Наредба №22 на БНБ за дейността на ЦКР.

**(2)** Правилното документиране на всяка проверка и получаване на информация от базата данни на регистъра се позволява само в предвидените от наредбата случаи.

**Раздел V**

**Забрана за разкриване на данни, извлечени от системите на банката, към трети лица**

**Чл.31. (1)** Строго забранено е разкриване на трети лица на информация (съдържаща лични данни), получена/извлечена от системите на банката за целите на предлагане и управление на услугите към клиенти, без значение дали е свързана с клиентите или трети лица.

**(2)** Ръководители на звена (в ЦУ и КМ), информират техните служители, които обработват лични данни, съдържащи финансова идентичност на клиенти, че:

1. всички данни, които се записват в системите на банката, се проверяват внимателно и се верифицират преди това, с цел да се избегне прехвърляне на грешни данни.

2. всяко изтичане на данни на физически лица може да доведе до значителни щети и вредно въздействие върху банката.

**Чл.32.(1)** Необходимост от унищожаване на документи на хартиен носител, съдържащи лични данни, генерирани всекидневно при осъществяване дейността на банката, се основава на указания, съобразени със изпълнението на законови срокове за съхранение. Оценката се извършва с оглед на запазване на документите с цел упражняване или защита на правни претенции, независимо дали това е в рамките на съдебна, административна или друга извънсъдебна процедура.
**(2)** Документи, съдържащи лични данни, определени за унищожаване, се съхраняват от всяко звено от отговорен служител, определен от ръководител на звеното.

**Раздел VI**
**Директен маркетинг при предлагане на услуги**
**Чл.33.(1)** Във връзка с изготвяне и провеждане на промоционални кампании при предлагане на продукти и услуги на банката и с цел да се осигури задължителното спазване на действащото законодателство, е необходимо да се изпълнят следните условия:
1. получателите на рекламни материали на хартиен носител, както и чрез телефон, SMS, MMS, електронна поща/e-mail/, с човешка намеса или по автоматизиран начин, следва да са предоставили предварително своето съгласие при спазване на условията на **чл. 9, ал. 5 от настоящите правила**. Съгласията се съхраняват в доказателствен вид в специален регистър на принципа за отчетност.
2. всички получатели, които са изключени от регистъра за съгласия относно целите на предоставяне на директен маркетинг, следва да не бъдат оферирани за в бъдеще до получаване на надлежно събрано съгласие.
3. всички получатели могат да предоставят своето съгласие чрез всички налични канали за връзка с банката.
**(2)** Когато клиент, предоставил свое съгласие по законен начин чрез каналите на банката, пожелае да възрази по реда на **Раздел IV Право на възражение и автоматизирано вземане на индивидуални решения на Глава трета от настоящите правила**, банката безплатно и без неоснователно забавяне, отписва клиента от бъдещи промоционални кампании и го отписва от Регистъра на съгласията, като запазва и съхранява **съобщението по чл. 16, ал. 2** от настоящите правила.

**Раздел VI**
**Мерки за защита срещу фишинг измами**
**Чл.34.(1)** За защита на своите клиенти, служители и други физически лица от злонамерени атаки, наречени фишинг (т.е. злонамерен опит за придобиване на чувствителна информация като потребителско име, парола и детайли на платежни инструменти чрез създаването на дубликат на съществуваща уеб страница на банката, прихващане на потребителска електронна поща и извършителят е приел чужда клиентска самоличност при електронни комуникации) банката подготвя и публикува

уведомления и указания с инструкции кои са най-популярните измами и как да бъдат избегнати.

**(2)** Инвестбанк уведомява по недвусмислен начин своите клиенти чрез официалните канали за комуникация, че не изпраща съобщения с искания за допълнително предоставяне на информация по телефон, имейл, или друг канал за комуникация, съдържаща данни по лична карта, IBAN на сметки, клиентски номера и пароли, извън регламентираните канали за комуникация с клиенти. В случай на получаване на подобни електронни съобщения, същите следва да се изтрият незабавно и да се потърси връзка с банката.

**(3)** Банката поддържа постоянен контакт със Специализиран сектор "Киберпрестъпност" при ГДБОП-МВР.

**Раздел VII**

**Инсталиране на охранителна система за видеонаблюдение**

**Чл.35.(1)** С цел превенция срещу кражба на собственост и други нарушения, както и защита от престъпления, наблюдение за служителите, посетителите в сгради на банката, контрол на дейността в помещенията, Инвестбанк е инсталирала, където е необходимо, системи за организация на видеоконтрол както на локални, така и на териториално-разпределени обекти.

**(2)** Запис и съхранение на събраната информация чрез системите за наблюдение се ползва в банката в съответствие с приложимото законодателство, а данните могат да бъдат предоставяни само и единствено на компетентни съдебни или разследващи органи за целите на наказателно преследване по конкретни случаи и след становище на Дирекция Сигурност и охрана. Достъпът до данните е уреден в Процедура.

**ГЛАВА ПЕТА**

**ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ**

**§1.** За неуредените в тези Правила въпроси се прилагат разпоредбите на действащото българско законодателство.

**§2. Приложения**:

1. Справка за регистрите с лични данни в системата на „Инвестбанк” АД и длъжностните лица ангажирани с тяхното поддържане и опазване. Описание на съществуващите мерки за защита на личните данни;

2. Списък от задължителни и препоръчителни мерки за осигуряване на необходимото ниво на защита на личните данни съобразно техния вид и чувствителност;

3. Списък на институциите, които получават от „Инвестбанк” АД регулярна информация съдържаща лични данни на служители или клиенти по силата на специални закони.

4. Декларация за опазване тайната на личните данни, отнасяща се за служители, администратори (мениджърски състав)и лица, с които е сключен граждански договор в „Инвестбанк” АД ;

5. Декларация за поверителност.

6. Декларация за съгласие на клиенти.

6А. Декларация и Анкетен лист.

7. Заявление за достъп до лични данни от клиенти.

**§3.** Изменения и допълнения на вътрешния нормативен акт:

**(1)** Вътрешни правила за защита на личните данни на „Инвестбанк“ АД, приети на заседание на Управителния съвет на ТБ "ИНВЕСТБАНК" АД с протокол № 14 от 05.04.2007г. и изменени с решение по протокол № 19 от 23.04.2010.г. на Управителния съвет, което е одобрено и от Надзорния съвет.

**(2)** Настоящите Правила са приети с Протокол №43а/14.07.2017г. на Управителния съвет на „Инвестбанк” АД, отменят Правилата с №19/23.04.2010 г. и съставляват Приложение V към Правилника за осъществяване на специализиран нормативен контрол в „Инвестбанк” АД.

**(3) Настоящите Правила са изменени с Протокол №26/22.05.2018 г. на Управителния съвет на „Инвестбанк“ АД и съставляват Приложение V към Правилника за осъществяване на специализиран нормативен контрол в „Инвестбанк“ АД.**

**(4) Настоящите Правила са изменени с Протокол № 18/28.04.2020 г. на Управителния съвет на „Инвестбанк“ АД и съставляват Приложение V към Правилника за осъществяване на специализиран нормативен контрол в „Инвестбанк“ АД.**