ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «СТРАХОВА КОМПАНІЯ «ЕТАЛОН»

ЗАТВЕРДЖЕНО
Рішенням Наглядової Ради
Приватного акціонерного товариства
«Страхова компанія «Еталон»
від 31.07.2025 р. № 108
Голова Наглядової Ради

_____ Н. Піацца

ПОЛІТИКА
ЗАХИСТУ ТА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ
ПрАТ «СК «Еталон»

Київ - 2025

Зміст

I.	ЗАГАЛЬНІ ПОЛОЖЕННЯ	4
II.	ВИЗНАЧЕННЯ ТЕРМІНІВ ТА СКОРОЧЕННЯ	4
III.	ПРЕДМЕТ ТА ЗАВДАННЯ ПОЛІТИКИ	6
IV.	ЗАХИСТ ТА ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ	6
V.	ПРИКІНЦЕВІ ПОЛОЖЕННЯ	12

І.ЗАГАЛЬНІ ПОЛОЖЕННЯ

1. Політика захисту та обробки персональних даних Приватного акціонерного товариства «Страхова компанія "Еталон" (далі – **Політика**) визначає загальні вимоги до організації обробки та забезпечення захисту персональних даних суб'єктів персональних даних у ПрАТ «СК «Еталон» (далі – **Товариство**) на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів.
2. Забезпечення захисту персональних даних є невід'ємною частиною діяльності Товариства. Стан захищеності являє собою вміння та здатність Товариства надійно протистояти будь-яким спробам завдати шкоди його законним інтересам.
3. Товариство забезпечує захист персональних даних, які обробляються під час надання платіжних послуг та в усіх можливих випадках обробки інформації, які не пов'язані з наданням платіжних послуг. Заходи захисту відповідають законодавству у сфері захисту інформації та обробки персональних даних.
4. Керівництво Товариства усвідомлює важливість та необхідність вдосконалення заходів і засобів забезпечення захисту персональних даних в контексті розвитку законодавства та норм регулювання діяльності, а також розвитку реалізованих технологій та очікувань клієнтів Товариства та інших зацікавлених сторін.
5. Політика розроблена з урахуванням вимог законодавства України, зокрема Закону України «Про інформацію», Закону України «Про доступ до публічної інформації», Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», Закону України «Про платіжні послуги», Закону України «Про захист персональних даних» (далі – **Закон**), нормативно-правових актів Національного банку України, національних стандартів України з питань інформаційної безпеки ДСТУ ISO/IEC 27001 та ДСТУ ISO/IEC 27002, міжнародного стандарту PCI DSS.
6. Політика поширюється на всі підрозділи і всіх штатних працівників Товариства а також на всіх повірених, яких Товариство уповноважило на укладання договорів страхування, на працівників таких повірених та інших осіб, яких повірений залучив для виконання своїх повноважень на користь Товариства.
7. Політика має бути опублікована на офіційному сайті Товариства та надаватись третім сторонам в рамках контрактних або партнерських зобов'язань Товариства.

ІІ.ВИЗНАЧЕННЯ ТЕРМІНІВ ТА СКОРОЧЕННЯ

8. Терміни в цьому Положенні вживаються в таких значеннях:

1) **База персональних даних** – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;
2) **Володілець персональних даних** – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.
3) **Відповідальний виконавець** – особа, яка відповідно до внутрішніх документів Товариства безпосередньо здійснює обробку персональних даних, в тому числі, формує та веде відповідні бази персональних даних, отримує та зберігає згоди суб'єктів персональних даних на обробку персональних даних тощо.
4) **Згода суб'єкта персональних даних** – добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.
5) **Знеособлення персональних даних** – вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу.
6) **Інформаційна система (ІС)** – сукупність інформаційних ресурсів, середовища передачі даних, обслуговуючого персоналу та організаційних заходів, які використовуються Товариством для задоволення своїх інформаційних потреб.

7) **Інформація** – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

8) **Категорії** – узагальнені групи персональних даних відповідних суб'єктів.

9) **Клієнт** – суб'єкт персональних даних (фізична особа або представник такої особи), який виступає споживачем фінансових послуг, що надаються Товариством та персональні дані якого обробляються Товариством.

10) **Контрагент** – суб'єкт персональних даних (фізична особа, фізична особа – підприємець, представник юридичної особи), який діє у цивільно-правових та господарсько-правових відносинах з Товариством.

11) **Конфіденційна інформація (КІ)** – інформація, щодо якої встановлено режим конфіденційності. До КІ відноситься інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. КІ може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

12) **Користувач** – особа, що залучається Товариством для виконання відповідних функцій або працівник Товариства, що використовує інформаційні ресурси ІС Товариства для виконання посадових обов'язків.

13) **Обробка персональних даних** – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

14) **Персональні дані (ПД)** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Персональними даними згідно цього Положення вважаються:

- прізвище, ім'я, по батькові;
- дата і місце народження;
- адреса проживання;
- паспортні дані;
- ідентифікаційний код;
- дані про освіту, професію, роботу;
- номер телефону, email;
- фото або відео, на яких можна впізнати людину;
- медична інформація;
- біометричні або генетичні дані;
- IP-адреса, якщо її можна прив'язати до особи.

15) **Правочин** – будь-який договір, стороною якого є Товариство, не залежно від його форми та предмету, в тому числі додатки, доповнення до них, угоди про внесення змін до них, документи, що підтверджують дії, спрямовані на укладення, виконання, зміну та припинення будь-яких з цих правочинів.

16) **Працівник** – фізична особа, яка безпосередньо власною працею виконує трудову функцію згідно з укладеним з Товариством трудовим договором (контрактом) та/або фізична особа, яка виконує операції щодо укладення договорів страхування для Товариства на підставі укладеного з іншим суб'єктом господарювання договору доручення.

17) **Розпорядник персональних даних** – фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.

18) **Суб'єкт персональних даних** – фізична особа, персональні дані якої обробляються.

19) **Строк обробки персональних даних** – строк, протягом якого Товариство здійснює обробку персональних даних суб'єкта персональних даних, який обчислюється з моменту отримання Товариством персональних даних та згоди на обробку персональних

даних (укладання правочину, умови якого передбачають обробку Товариством персональних даних) та не перевищує строк, необхідний для реалізації мети обробки та строк, визначений законодавством України у сфері архівної справи та діловодства.

20) **Третя особа** – будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений), якій Товариством чи розпорядником персональних даних здійснюється передача персональних даних.

Інші терміни, визначення та скорочення, що не визначені у цьому розділі, вживаються у значеннях, наведених далі по тексту Політики, а у разі відсутності такого визначення – відповідно до законодавства та/або внутрішніх нормативних документів Товариства. Якщо визначення у внутрішніх документах Товариства відрізняються від наведених у цьому документі, для цілей тлумачення Політики, превалюють значення, наведені у тексті цієї Політики.

ІІІ.ПРЕДМЕТ ТА ЗАВДАННЯ ПОЛІТИКИ

9. Основним завданням даної Політики є формування вимог для забезпечення проведення безперервної оцінки та зниження рівня ризиків витоку ПД, що оброблюються та зберігаються Товариством та його повіреними. Для вирішення цього завдання в Товаристві впроваджена система управління інформаційною безпекою (далі – СУІБ) та кібербезпекою, які містять в собі комплекс організаційно-технічних процесів і нормативно-розпорядчих документів.

10. Дана Політика визначає фундаментальні вимоги до процесів збору, обробки і зберігання ПД, захисту від існуючих та потенційних загроз.

11. Основні цілі захисту ПД – це забезпечення цілісності, доступності, конфіденційності та спостережності ПД під час обробки та зберігання.

12. Керівництво Товариства сприяє створенню, впровадженню, контролю, підтримці та вдосконаленню Політики.

13. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладений на Департамент інформаційних технологій.

14. Кожен працівник Товариства у межах своїх повноважень забезпечує підтримку та виконання вимог Політики та несе відповідальність за їх порушення згідно із законодавством України та внутрішніми нормативними документами Товариства.

ІV.ЗАХИСТ ТА ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ

15. Дана Політика обов'язкова для застосування відповідальним виконавцем та всіма працівниками, які безпосередньо здійснюють обробку та/або мають доступ до персональних даних у зв'язку з виконанням своїх службових обов'язків.

1. Суб'єкти відносин та обробка ПД у Товаристві

16. Суб'єктами відносин, пов'язаних із ПД, є: суб'єкт ПД; володілець ПД; розпорядник ПД; третя особа; Уповноважений.

17. ПД, що обробляються Товариством, відносяться до КІ.

18. Товариство згідно з чинним законодавством України, та/або на підставі укладених договорів, є розпорядником ПД.

19. Порядок обробки ПД в Товаристві визначається цією Політикою на підставі чинного законодавства України.

20. Первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи, підписані нею документи, відомості, які особа надає про себе.

21. Процеси (підпроцеси, процедури) обробки ПД є частиною бізнес-процесів Товариства. Процеси обробки ПД можуть бути автоматизованими або неавтоматизованими.

22. Товариство обробляє ПД, які можуть бути об'єднані в бази ПД.

23. Товариство може доручити обробку ПД розпоряднику ПД відповідно до договору, укладеного в письмовій формі. Розпорядник ПД може обробляти ПД лише з метою і в обсязі, визначених у договорі.

24. Товариство не обробляє ПД про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються статевого життя, біометричних або генетичних даних.

25. В усіх випадках, не врегульованих цим Положенням, необхідно керуватися чинним законодавством України.

2. Вимоги до обробки ПД

26. В основу визначення мети обробки ПД закладено принцип законності їх обробки.

27. Обробка ПД здійснюється Товариством відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.

28. ПД, що обробляються Товариством мають бути точними, достовірними та оновлюватися за потребою, визначеною метою їх обробки.

29. Склад та зміст ПД, що обробляються Товариством, мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки.

30. Обробка ПД здійснюється Товариством для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.

31. Строк зберігання ПД встановлюється Товариством залежно від категорії суб'єктів ПД, мети обробки ПД та визначається чинним законодавством України.

3. Категорії суб'єктів ПД

32. Товариство здійснює обробку ПД таких категорій суб'єктів персональних даних:

1) страхувальники, застраховані особи, вигодонабувачі за договорами страхування, потерпілі треті особи за договорами страхування відповідальності (фізичні особи та представники таких осіб);

2) контрагенти (суб'єкти, які перебувають у цивільно-правових та господарсько-правових відносинах з Товариством - представники юридичної особи, фізичні особи-підприємці, фізичні особи без статусу господарюючого суб'єкта);

3) працівники.

4. Використання та підстава для обробки ПД

33. Використання ПД передбачає будь-які дії Товариства щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки ПД іншим суб'єктам відносин, пов'язаних із ПД, що здійснюються на підставі укладеного з суб'єктом ПД договору та/або за згодою суб'єкта ПД, або відповідно до вимог Закону.

34. Для належного використання ПД в Товаристві створені умови для їх захисту.

35. Використання ПД працівниками суб'єктів відносин, пов'язаних з ПД, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб ПД, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законодавством. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з ПД, крім випадків, установлених законодавством.

36. Згода суб'єкта персональних даних на обробку його ПД.

37. Дозвіл на обробку ПД, наданий Товариству відповідно до Закону виключно для здійснення його повноважень.

38. Укладення та виконання правочину, стороною якого є суб'єкт ПД або який укладено на користь суб'єкта ПД чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта ПД.

39. Захист життєво важливих інтересів суб'єкта ПД.

40. Необхідність виконання обов'язку Товариством, який передбачений законодавством.

41. Необхідність захисту законних інтересів Товариства або третьої особи, якій передаються ПД, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта ПД у зв'язку з обробкою його даних переважають такі інтереси.

4. Збирання ПД

42. Збирання ПД є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу.

43. Суб'єкт ПД повідомляється Товариством про склад та зміст зібраних ПД, свої права, визначені Законом, мету збору ПД та осіб, яким передаються його ПД:

1) в момент збору ПД, якщо ПД збираються у суб'єкта ПД;

2) в інших випадках протягом 30 (тридцяти) робочих днів з дня збору ПД.

44. Отримання згоди суб'єкта ПД та повідомлення його про обробку ПД не виконуються, якщо ПД були зібрані із загальнодоступних джерел.

5.Накопичення та зберігання ПД, доступ до ПД

45. Накопичення ПД передбачає дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення цих даних до бази ПД.

46. Зберігання ПД передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них.

47. Порядок доступу до ПД третіх осіб визначається статтею 16 Закону.

48. Порядок доступу до ПД третіх осіб визначається умовами укладеного з суб'єктом персональних даних договором та/або згоди суб'єкта персональних даних, наданої Товариству на обробку цих даних.

49. Доступ до ПД третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог Закону або неспроможна їх забезпечити.

50. Суб'єкт відносин, пов'язаних з персональними даними, подає Товариству запит щодо доступу до персональних даних (далі – запит), в якому зазначається:

1) прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи – заявника);

2) найменування, місцезнаходження юридичної особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи – заявника);

3) прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;

4) відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника цієї бази;

5) перелік персональних даних, що запитуються;

6) мета запиту.

51. Строк вивчення запиту на предмет його задоволення не може перевищувати тридцяти календарних днів з дня його надходження.

52. Відстрочення доступу до персональних даних третіх осіб допускається у разі, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження

запиту. При цьому загальний термін вирішення питань, порушених у запиті, не може перевищувати сорока п'яти календарних днів.

53. Відмова у доступі до персональних даних допускається, якщо доступ до них заборонено згідно із законом.

54. Товариство безоплатно надає суб'єкту ПД інформацію про обробку його ПД, крім випадків, установлених законодавством.

55. Суб'єкт ПД має право на отримання своїх ПД, які він надав Товариству, в структурованому, загальноприйнятому форматі, що легко зчитується машиною, та має право на передавання таких даних іншому володільцю/розпоряднику.

6. Видалення або знищення ПД, поширення ПД

56. ПД видаляються або знищуються в порядку, встановленому відповідно до вимог чинного законодавства.

57. ПД підлягають видаленню або знищенню у разі:

1) закінчення строку зберігання даних, визначеного угодою, укладеною з суб'єктом ПД або згодою суб'єкта ПД на обробку цих даних, якщо інше не передбачено законом;

2) припинення правовідносин між суб'єктом ПД та Товариством, якщо інше не передбачено законодавством;

3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого;

4) набрання законної сили рішенням суду щодо видалення або знищення ПД.

58. Відомості про особу, які не відповідають дійсності, мають бути негайно змінені або знищені.

59. Персональні дані, зібрані з порушенням вимог Закону, підлягають видаленню або знищенню у встановленому законодавством порядку.

60. Видалення та знищення ПД здійснюється у спосіб, що виключає можливість їх поновлення.

61. Поширення ПД передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта ПД.

62. Поширення ПД без згоди суб'єкта ПД або уповноваженої ним особи дозволяється у випадках, визначених законодавством, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.

63. Виконання вимог встановленого режиму захисту ПД забезпечує сторона, що поширює ці дані.

64. Сторона, якій передаються ПД, повинна попередньо вжити заходів щодо забезпечення вимог чинного законодавства.

65. Передача ПД іноземним суб'єктам відносин, пов'язаних із ПД, здійснюється лише за умови забезпечення відповідною державою належного захисту ПД у випадках, встановлених законом або міжнародним договором України.

66. ПД не можуть поширюватися з іншою метою, ніж та, з якою вони були зібрані.

67. ПД можуть передаватися іноземним суб'єктам відносин, пов'язаних з ПД, також у разі:

1) надання суб'єктом ПД однозначної згоди на таку передачу;

2) необхідності укладення чи виконання правочину між володільцем ПД та третьою особою – суб'єктом ПД на користь суб'єкта ПД;

3) необхідності захисту життєво важливих інтересів суб'єктів ПД;

4) необхідності захисту суспільного інтересу, встановлення, виконання та забезпечення правової вимоги;

5) надання володільцем ПД відповідних гарантій щодо невтручання в особисте і сімейне життя суб'єкта ПД.

68. Товариство може передавати ПД суб'єктів ПД, що входять до Категорій «Клієнти», «Контрагенти» та «Працівники» таким третім особам (в тому числі, але не виключно):

1) розпорядникам (підприємствам, установам і організаціям усіх форм власності, органам державної влади чи органам місцевого самоврядування, фізичним особам - підприємцям, яким Товариством або чинним законодавством надано або буде надано право обробляти персональні дані);

2) третім особам, що залучені Товариством та/або приймають участь під час надання Товариством фінансових послуг;

3) архівним установам та іншим особам, що надають Товариству послуги зберігання інформації та документів (пов'язані з цим послуги);

4) учасникам, афілійованим особам Товариства, особам, що мають істотну участь в Товаристві та/або здійснюють контроль над Товариством;

5) організаціям, які надають послуги Товариству (у т.ч., фінансові);

6) суб'єктам господарювання, що працюють під торговою маркою (брендом) СК "Еталон" , зокрема, для пропонування повного кола послуг суб'єктам ПД іншими суб'єктами господарювання, які працюють під торговою маркою (брендом) СК "Еталон" ;

7) іншим приватним особам та організаціям для забезпечення виконання останніми своїх функцій або надання послуг Товариству відповідно до укладених між такими особами (організаціями) та Товариством правочинів.

6. Повідомлення про дії з ПД, захист ПД

69. Про передачу ПД третій особі Товариство протягом десяти робочих днів повідомляє суб'єкта ПД, окрім наступних випадків:

1) передачі ПД за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;

2) виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом;

3) здійснення обробки ПД в історичних, статистичних чи наукових цілях;

4) можливість передачі ПД третім особам передбачена умовами укладеного Товариством та суб'єктом ПД правочину.

70. Забезпечення безпеки персональних даних в Товаристві ґрунтується на наступних фундаментальних принципах:

1) принцип мінімальних повноважень: доступ до персональних даних повинен бути організований таким чином, щоб надавати тільки ті повноваження, яких достатньо для виконання службових завдань та обов'язків;

2) принцип явного санкціонування дій: дії працівників Товариства, пов'язані з персональними даними, які прямо не передбачені внутрішніми організаційно-розпорядчими або нормативними документами Товариства, є забороненими;

3) принцип законності: Товариство керується вимогами чинного законодавства України пов'язаного з безпекою персональних даних;

4) принцип відповідальності: керівництво Товариства, а також працівники, бізнес-партнери і будь-які треті сторони, які мають або мали доступ до персональних даних, повинні дотримуватися вимог регламентуючих документів та законодавства України.

5) принцип комплексності та системності: захист персональних даних в Товаристві забезпечується на правовому, адміністративному, організаційному і програмно-технічному рівнях, а також шляхом комплексного застосування засобів захисту інформації та взаємодії всіх підрозділів Товариства між собою.

71. Товариство вживає заходів щодо забезпечення захисту ПД на всіх етапах їх обробки за допомогою організаційних та технічних заходів.

72. Під час обробки ПД Товариство забезпечує захист даних від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

73. Товариство використовує системні та програмно-технічні засоби, засоби зв'язку, які запобігають втратам, крадіжкам, несанкціонованому знищенню, викривленню, підробленню, копіюванню, відтворенню і поширенню інформації, зокрема, і в сфері захисту персональних даних та відповідають вимогам міжнародних та національних стандартів.

74. Товариство забезпечує архівацію персональних даних, які циркулюють в програмних комплексах та інформаційних ресурсах Товариства. Носії з архівними персональними даними зберігаються у сховищі.

75. Товариство обробляє персональні дані в складі інформаційної (автоматизованої) системи, у якій забезпечується захист персональних даних відповідно до вимог Закону. Норми технічного захисту інформації у Товаристві відповідають вимогам законодавства України щодо захисту інформації в інформаційно-телекомунікаційних системах та вимогам внутрішніх нормативних документів Товариства.

76. В інформаційних системах Товариства забезпечується антивірусний захист та використання технічних засобів безперебійного живлення елементів інформаційної системи.

77. Функціонування системних, програмно-технічних засобів та засобів зв'язку забезпечує дублювання роботи всіх систем та елементів для забезпечення збереження інформації та забезпечення неможливості її знищення з будь-яких обставин засобами, передбаченими Товариством.

78. Програмні продукти, що використовуються Товариством у процесі обробки персональних даних для досягнення мети їх обробки мають вбудовані механізми захисту інформації від несанкціонованого доступу для забезпечення ідентифікації та аутентифікації користувачів, цілісності електронних документів, реєстрації дій користувачів, управління доступом користувачів до інформації та окремих функцій, що надаються продуктом, та/або має змогу використовувати зазначені механізми захисту системного програмного забезпечення, а також можливість інтегруватися в комплексну систему захисту інформації автоматизованої системи, у якій цей продукт використовується.

79. Працівники допускаються до обробки персональних даних лише після їх авторизації. Доступ осіб, які не пройшли процедуру ідентифікації та/або автентифікації, блокується.

80. Працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення конфіденційної інформації та збереження таємниці надавача фінансових послуг, зокрема персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків.

81. В інформаційній (автоматизованій) системі, де обробляються персональні дані, може здійснюватися реєстрація, зокрема:

1) результатів ідентифікації та/або автентифікації працівників Товариства;
2) дій з обробки персональних даних;
3) факту встановлення ознаки "Підтвердження надання згоди на обробку персональних даних у базі персональних даних" за допомогою управляючих елементів веб-ресурсів володільця або розпорядника бази персональних даних, інтерфейсів користувача програмного забезпечення;
4) результатів перевірки цілісності засобів захисту персональних даних.

82. Відповідальна особа та/або структурний підрозділ може проводити аналіз реєстраційних даних.

83. Реєстраційні дані захищаються від модифікації та знищення. Реєстраційні дані повинні зберігатися та надаватися за вмотивованою вимогою для аналізу суб'єктам відносин, пов'язаним із персональними даними.

84. Відповідальною особою здійснюються заходи, спрямовані на підвищення обізнаності працівників Товариства із законодавством та внутрішніх нормативних документів Товариства у сфері захисту персональних даних, у тому числі проводить систематичне навчання персоналу.

V.ПРИКІНЦЕВІ ПОЛОЖЕННЯ

85. Політика вступає в силу з дати її затвердження.

86. Зміни та доповнення до цієї Політики затверджуються Рішеннями Наглядової ради Товариства та можуть оформлятися, в тому числі, шляхом викладення Політики в новій редакції.

87. У разі невідповідності будь-якої частини цієї Політики чинному законодавству України, в тому числі в зв'язку з прийняттям нових нормативно-правових актів, Політика діятиме тільки в тій частині, яка не суперечить чинному законодавству України.

88. Надання Політики зовнішнім органам, третім особам відбувається за обов'язковим погодженням з Департаментом інформаційних технологій та Департаментом внутрішньої безпеки відповідно до діючого законодавства України.

89. У разі необхідності ця Політика переглядається з метою поліпшення ефективності бізнес-процесів Товариства та удосконалення системи внутрішнього контролю, але не рідше ніж раз на рік.

90. У разі зміни назв структурних підрозділів, які задіяні в процедурах, що описані у цій Політиці, при незмінності функцій, ця Політика вважається дійсною щодо їх нової назви.