ЗАТВЕРДЖЕНО
рішенням Ради адвокатів України
від «16» листопада 2017 року № 250

із зміною, внесеною
рішенням Ради адвокатів України
від «30» березня 2018 року № 38

ПОРЯДОК

обробки персональних даних у базах персональних даних

І. Загальні положення

1.1 Цей Порядок встановлює загальні вимоги до організаційних та технічних заходів захисту персональних даних під час їх обробки у базах персональних даних володільцем та розпорядником персональних даних – Національною асоціацією адвокатів України, Вищою кваліфікаційно-дисциплінарною комісією адвокатури, Вищою ревізійною комісією адвокатури, радами адвокатів регіонів, кваліфікаційно-дисциплінарними комісіями адвокатури.

Терміни у цьому Порядку вживаються у значенні, наведеному в Законі України «Про захист персональних даних» (далі - Закон) і Типовому порядку обробки персональних даних, затвердженому наказом Уповноваженого Верховної Ради України від 08.01.2014 року № 1/02-14.

(пункт 1.1. із зміною, внесеною рішенням РАУ від 30.03.2018 № 38)

1.2 У цьому Порядку терміни вживаються у такому значенні:

автентифікація – процедура встановлення належності працівникові чи посадовій особі НААУ, ВКДКА, ВРКА, КДКА, РАР пред’явленого нею ідентифікатора;

авторизація – процедура отримання дозволу на проведення дій з обробки персональних даних у складі інформаційної (автоматизованої) системи;

відповідальна особа – особа, на яку НААУ, ВКДКА, ВРКА, КДКА, РАР, відповідно до її службових, трудових, професійних обов’язків покладено організацію роботи, пов’язаної із захистом персональних даних при їх обробці;

володілець персональних даних – НААУ, ВКДКА, ВРКА, КДКА, РАР, інші органи адвокатського самоврядування;

знеособлення персональних даних – вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу;

ідентифікація — процедура розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої інформації про нього, яка сприймається інформаційною (автоматизованою) системою;

структурний підрозділ – структурна одиниця, що діє у складі володільця або розпорядника персональних даних та відповідно до його прав та обов'язків на підставі положення про нього здійснює організацію роботи, пов'язаної із захистом персональних даних при їх обробці.

Інші терміни у цьому Порядку вживаються у значеннях, наведених у Законі України «Про захист персональних даних».

1.3 Захист персональних даних покладається на володільця персональних даних – НААУ, ВКДКА, ВРКА, КДКА, РАР, інші органи адвокатського самоврядування.

НААУ здійснює обробку персональних даних відповідно до закону.

На дії НААУ, ВКДКА, ВРКА, КДКА, РАР поширюються усі вимоги щодо захисту персональних даних від незаконної обробки, а також від незаконного доступу до них.

НААУ, ВКДКА, ВРКА, КДКА, РАР при опублікуванні (висвітлені на офіційних веб-ресурсах) будь-яких рішень щодо фізичних осіб, адвокатів, клієнтів тощо зобов'язані знеособлювати персональні дані з метою уникнення ідентифікації особи (осіб).

1.4 НААУ надає суб'єкту персональних даних інформацію про мету обробки персональних даних до моменту отримання згоди від суб'єкта персональних даних.

1.5 НААУ зберігає персональні дані у строк не більше, ніж це необхідно відповідно до мети їх обробки, якщо інше не передбачено законодавством.

1.6 НААУ визначає:

- мету обробки та підстави, склад персональних даних у базі персональних даних та її місцезнаходження;
- які відомості про особу є інформацією з обмеженим доступом (персональними даними), і які є відкритими та загальнодоступними;
- порядок доступу до персональних даних осіб, які здійснюють обробку, а також суб'єктів персональних даних;
- порядок внесення, зміни, поновлення, використання, поширення, знеособлення, знищення персональних даних у базі персональних даних;
- відповідальну особу;
- порядок захисту персональних даних від незаконної обробки, у тому числі від втрати, незаконного або випадкового знищення, а також від незаконного доступу до них.

1.7 Відповідальна особа відповідно до покладених завдань:

- забезпечує ознайомлення працівників НААУ, ВКДКА, ВРКА, КДКА, РАР з вимогами законодавства про захист персональних даних, зокрема щодо їхнього обов'язку не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних, службових чи трудових обов'язків;

- забезпечує організацію обробки персональних даних працівниками НААУ, ВКДКА, ВРКА, КДКА, РАР відповідно до їх професійних, службових чи трудових обов'язків в обсязі, необхідному для виконання таких обов'язків;
- організовує роботу з обробки запитів щодо доступу до персональних даних суб'єктів відносин, пов'язаних з обробкою персональних даних;
- забезпечує доступ суб'єктів персональних даних до власних персональних даних;
- інформує керівника володільця та розпорядника персональних даних про заходи, яких необхідно вжити для приведення складу персональних даних та процедур їх обробки у відповідність до закону;
- інформує Голову НААУ про порушення встановлених процедур з обробки персональних даних.

У текстах органів адвокатського самоврядування, що відкриті для загального доступу через оприлюднення на офіційному веб-порталі органу адвокатського самоврядування або офіційне опублікування, не можуть бути розголошені відомості, що дають можливість ідентифікувати фізичну особу. Такі відомості замінюються літерними або цифровими позначеннями.

До відомостей, зазначених вище, належать:

1) імена (ім'я, по батькові, прізвище) фізичних осіб;
2) місце проживання або перебування фізичних осіб із зазначенням адреси, номери телефонів чи інших засобів зв'язку, адреси електронної пошти, ідентифікаційні номери (коди);
3) інша інформація, що дає можливість ідентифікувати фізичну особу.

З метою ведення Єдиного реєстру адвокатів України дозволяється обробка персональних даних фізичних осіб відповідно до законодавства з питань захисту персональних даних.

1.8 НААУ веде облік:

- фактів надання та позбавлення працівників права доступу до персональних даних та їх обробки;
- спроб та фактів несанкціонованих та/або незаконних дій з обробки персональних даних.

1.9 НААУ може розмежувати режими доступу працівників до обробки персональних даних у базі персональних даних відповідно до їх професійних, трудових чи службових обов'язків.

1.10 Видалення або знищення персональних даних здійснюється у спосіб, що виключає подальшу можливість поновлення таких персональних даних.

ІІ. Обробка персональних даних в складі інформаційної (автоматизованої) системи та/або у формі картотек із застосуванням неавтоматизованих засобів

2.1. Процедури обробки, строк обробки та склад персональних даних повинні бути пропорційними меті обробки.

2.2. Мета обробки персональних даних повинна бути чіткою і законною та визначеною до початку їх збору.

2.3. У разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних, окрім випадків, визначених законодавством, повинен отримати згоду суб'єкта персональних даних на обробку його даних відповідно до нової мети.

2.4. Обробка персональних даних здійснюється володільцем персональних даних лише за згодою суб'єкта персональних даних, за винятком тих випадків, коли така згода не вимагається Законом.

2.5. Згода суб'єкта на обробку його персональних даних повинна бути добровільною та інформованою. Згода може надаватися суб'єктом у письмовій або електронній формі, що дає змогу зробити висновок про її надання. Документи (інформація), що підтверджують надання суб'єктом згоди на обробку його персональних даних, зберігаються володільцем впродовж часу обробки таких даних.

2.6. Володілець персональних даних, крім випадків, передбачених законодавством України, повідомляє суб'єкта персональних даних про склад і зміст зібраних персональних даних, його права, визначені Законом, мету збору персональних даних та третіх осіб, яким передаються його персональні дані:

- в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних;
- в інших випадках протягом тридцяти робочих днів з дня збору персональних даних.

2.7. Володілець зберігає інформацію (документи), які підтверджують надання заявнику вищезазначеної інформації протягом усього періоду обробки персональних даних.

2.8. НААУ обробляє персональні дані в складі інформаційної (автоматизованої) системи та/або у формі картотек із застосуванням неавтоматизованих засобів, у якій забезпечується захист персональних даних відповідно до вимог закону. Володілець та/або розпорядник персональних даних забезпечує захист персональних даних, які обробляються в складі інформаційної (автоматизованої системи).

2.9. Обробка персональних даних може здійснюватися повністю або частково із застосуванням автоматизованих засобів у складі інформаційної (автоматизованої) системи та/або у формі картотек із застосуванням неавтоматизованих засобів.

2.10. Працівники НААУ допускаються до обробки персональних даних лише після їх авторизації.

2.11. Доступ осіб, які не пройшли процедуру ідентифікації та/або автентифікації, повинен блокуватись.

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

- результатів ідентифікації та/або автентифікації працівників НААУ;
- дій з обробки персональних даних;
- факту встановлення ознаки «Підтвердження надання згоди на обробку персональних даних у базі персональних даних» за допомогою управляючих елементів веб-ресурсів НААУ, інтерфейсів користувача програмного забезпечення;
- результатів перевірки цілісності засобів захисту персональних даних.

Відповідальна особа може проводити аналіз реєстраційних даних. 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.

2.13. НААУ забезпечує антивірусний захист в інформаційній (автоматизованій) системі.

2.14. НААУ забезпечує використання технічних засобів безперебійного живлення елементів інформаційної (автоматизованої) системи.

2.15. Двері у приміщеннях (шафах, сейфах) повинні бути обладнані замком або контролем доступу.

2.16. Збирання персональних даних є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу. У момент збору персональних даних або у випадках, передбачених законом, протягом десяти робочих днів з дня збору персональних даних суб'єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, права такого суб'єкта, визначені Законом України «Про захист персональних даних», мету збору персональних даних та осіб, яким передаються його персональні дані.

2.17. Суб'єкт персональних даних має право відкликати згоду на обробку персональних даних без зазначення мотивів, у разі якщо єдиною підставою для обробки є згода суб'єкта персональних даних. З моменту

відкликання згоди володілець зобов’язаний припинити обробку персональних даних.

2.18. Видалення та знищення персональних даних здійснюється у спосіб, що виключає подальшу можливість поновлення таких персональних даних.

2.19. Порядок доступу до персональних даних суб’єкта персональних даних та третіх осіб визначається статтями 16-17 Закону.

2.20. Володілець повідомляє суб’єкта персональних даних про дії з його персональними даними на умовах, визначених статтею 21 Закону.

III. Захист персональних даних

3.1. Володілець, розпорядник персональних даних вживають заходів щодо забезпечення захисту персональних даних на всіх етапах їх обробки, у тому числі за допомогою організаційних та технічних заходів.

3.2. Володілець, розпорядник персональних даних самостійно визначають перелік і склад заходів, спрямованих на безпеку обробки персональних даних, з урахуванням вимог законодавства у сферах захисту персональних даних, інформаційної безпеки.

3.3. Захист персональних даних передбачає заходи, спрямовані на запобігання їх випадкових втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

3.4. Організаційні заходи охоплюють:

- визначення порядку доступу до персональних даних працівників володільця/розпорядника;
- визначення порядку ведення обліку операцій, пов’язаних з обробкою персональних даних суб’єкта та доступом до них;
- розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- регулярне навчання співробітників, які працюють з персональними даними.

3.5. Володілець/розпорядник веде облік працівників, які мають доступ до персональних даних суб’єктів. Володілець/розпорядник визначає рівень доступу зазначених працівників до персональних даних суб’єктів. Кожен із цих працівників користується доступом лише до тих персональних даних (їх частини) суб’єктів, які необхідні йому у зв’язку з виконанням своїх професійних чи службових або трудових обов’язків.

3.6. Усі інші працівники володільця/розпорядника мають право на повну інформацію лише стосовно власних персональних даних.

3.7. Працівники, які мають доступ до персональних даних, дають письмове зобов’язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв’язку з виконанням професійних чи службових або трудових обов’язків.

3.8. Датою надання права доступу до персональних даних вважається дата надання зобов’язання відповідним працівником.

3.9. Датою позбавлення права доступу до персональних даних вважається дата звільнення працівника, дата переведення на посаду, виконання обов’язків на якій не пов’язане з обробкою персональних даних.

3.10. У разі звільнення працівника, який мав доступ до персональних даних, або переведення його на іншу посаду, що не передбачає роботу з персональними даними суб’єктів, вживаються заходи щодо унеможливлення доступу такої особи до персональних даних, а документи та інші носії, що містять персональні дані суб’єктів, передаються іншому працівнику.

3.11. Володілець/розпорядник веде облік операцій, пов’язаних з обробкою персональних даних суб’єкта та доступом до них. З цією метою володільцем/розпорядником зберігається інформація про:

- дату, час та джерело збирання персональних даних суб’єкта;
- зміну персональних даних;
- перегляд персональних даних;
- будь-яку передачу (копіювання) персональних даних суб’єкта;
- дату та час видалення або знищення персональних даних;
- працівника, який здійснив одну із указаних операцій;
- мету та підстави зміни, перегляду, передачі та видалення або знищення персональних даних.

Володілець/розпорядник персональних даних самостійно визначає процедуру збереження інформації про операції, пов’язані з обробкою персональних даних суб’єкта та доступом до них. У випадку обробки персональних даних суб’єктів за допомогою автоматизованої системи, така система автоматично фіксує вказану інформацію. Ця інформація зберігається володільцем/розпорядником упродовж одного року з моменту закінчення року, в якому було здійснено зазначені операції, якщо інше не передбачено законодавством України.

3.12. Вимоги щодо обліку та збереження інформації про перегляд персональних даних не поширюється на володільців/розпорядників, які здійснюють обробку персональних даних в реєстрі, який є відкритим для населення в цілому.

3.13. Персональні дані залежно від способу їх зберігання (паперові, електронні носії) мають оброблятися у такий спосіб, щоб унеможливити доступ до них сторонніх осіб.

3.14. З метою забезпечення безпеки обробки персональних даних вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних.

_____