Проект вноситься
народними депутатами України
Чернєвим Є.В., Тарасенком Т.П.,
Стефанчуком Р.О. та іншими

ПРОЕКТ ЗАКОНУ УКРАЇНИ
«ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ»

Цей Закон визначає правові відносини, пов'язані із захистом і обробкою персональних даних, з метою забезпечення прав людини на захист персональних даних та повагу до особистого і сімейного життя.

РОЗДІЛ І

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Сфера дії Закону

1. Цей Закон поширюється на відносини, пов'язані з обробкою персональних даних із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

2. Дія цього Закону поширюється на всіх суб'єктів, пов'язаних з обробкою та захистом персональних даних, крім випадків передбачених цим Законом.

3. Дія цього Закону не поширюється на обробку персональних даних фізичними особами для особистих чи побутових потреб, які не пов’язані зі здійсненням професійної чи будь-якої іншої діяльності, що має на меті отримання прибутку.

4. Обробка персональних даних для особистих чи побутових потреб охоплює, зокрема, ведення кореспонденції та збереження поштових (електронних) адрес, підтримання соціальних контактів, а також комунікація у мережі Інтернет, яка здійснюється в контексті такої діяльності.

Стаття 2. Визначення термінів

1. У цьому Законі терміни вживаються в такому значенні:

біометричні дані — персональні дані, які стосуються фізичних, фізіологічних чи поведінкових характеристик фізичної особи, які в результаті спеціальної технічної обробки надають можливість ідентифікувати або верифікувати фізичну особу;

витік персональних даних (витік) — випадкове чи неправомірне знищення, втрата, зміна, несанкціоноване розкриття персональних даних або доступ до персональних даних, що сталося внаслідок порушення вимог та умов безпеки обробки персональних даних;

генетичні дані — персональні дані щодо вроджених або набутих генетичних ознак фізичної особи, які надають унікальну інформацію про фізіологію чи здоров’я такої фізичної особи та такі, що отримані, зокрема, в результаті аналізу біологічного зразка, взятого у відповідної фізичної особи;

дані про стан здоров’я — персональні дані, про стан фізичного чи психічного здоров’я фізичної особи, включаючи дані про надання медичних послуг або допомоги, які містять інформацію про стан здоров’я фізичної особи;

загальний річний оборот - загальні надходження звітного періоду, отримані в результаті операційної, інвестиційної та фінансової діяльності контролера відповідно до звіту про рух грошових коштів;

згода на обробку персональних даних (згода) — будь-яке вільне, чітке, інформоване та однозначне волевиявлення суб'єкта персональних даних, виражене у формі заяви та/або чіткої стверджувальної дії, яким він дозволяє обробку своїх персональних даних;

знеособлення персональних даних — комплекс заходів щодо незворотного вилучення із сукупності даних про фізичну особу будь-якої інформації, яка дозволяє ідентифікувати фізичну особу та/або щодо незворотного розірвання будь-якого зв'язку між інформацією та фізичною особою;

контролер персональних даних (контролер) — будь-яка фізична або юридична особа, суб'єкт владних повноважень чи будь-який інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних, а також інші фізичні або юридичні особи, для яких цілі та засоби обробки визначені законом;

картотека персональних даних — будь-які структуровані за певними критеріями персональні дані, обробка яких здійснюється не автоматизовано;

контролюючий орган – уповноважений орган, який здійснює нагляд та контроль за дотриманням вимог цього Закону та повноваження якого передбачені цим Законом та окремим Законом про орган;

обробка персональних даних — будь-яка дія або сукупність дій з персональними даними з використанням або без використання автоматизованих засобів, зокрема збирання, фіксація, упорядкування, структурування, зберігання, адаптація, зміна, відновлення, ознайомлення, псевдонімізація,

профілювання, знеособлення, використання, розкриття шляхом передачі або поширення, або надання доступу у інший спосіб, групування або комбінування, обмеження, видалення або знищення;

обробка персональних даних в правоохоронних цілях - обробка персональних даних правоохоронними органами, спрямована на запобігання, виявлення, припинення, розкриття та розслідування кримінальних правопорушень, виконання кримінальних покарань; забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку; відкриття та проведення досудового розслідування і дізнання, процесуальне керівництво досудовим розслідуванням; здійснення розвідувальної діяльності; забезпечення національної безпеки;

оператор персональних даних (оператор) – будь-яка фізична або юридична особа, суб'єкт владних повноважень чи будь-який інший орган, який здійснює обробку персональних даних від імені контролера та уповноважена на це ним або законодавством;

одержувач – будь-яка фізична чи юридична особа, суб'єкт владних повноважень чи будь-який інший орган, якому надаються (розкриваються) персональні дані;

персональні дані — будь-яка інформація, що стосується фізичної особи, яку ідентифіковано або може бути ідентифіковано;

послуга інформаційного суспільства - оплатне чи безоплатне надання будь-яких товарів, робіт і послуг на вимогу їхнього отримувача на підставі правочину, укладеного за допомогою засобів дистанційного зв'язку або поза торговельними або офісними приміщеннями, в тому числі інформаційні електронні послуги;

правоохоронний орган - державний орган, на який покладаються завдання щодо: запобігання, виявлення, припинення, розкриття та розслідування

кримінальних правопорушень, віднесених до його компетенції; забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку; уповноважений виконувати кримінальні покарання; відкриття та проведення досудового розслідування і дізнання, процесуальне керівництво досудовим розслідуванням; державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України; розвідувальні та контррозвідувальні органи;

профілювання — форма автоматизованої обробки персональних даних, яка полягає у обробці персональних даних з метою оцінки певних індивідуальних характеристик, зокрема, аналізу та передбачення варіантів (моделей) поведінки суб'єкта персональних даних (в тому числі в професійній діяльності), його майнового стану, стану здоров'я, особистих уподобань, інтересів, надійності, місцезнаходження або пересування;

прямий маркетинг - інформування у будь-якій формі, метою якого є пряме чи опосередковане просування товарів, робіт чи послуг або ділової репутації особи, яка провадить господарську або незалежну професійну діяльність;

псевдонімізація — обробка персональних даних у спосіб, що не дозволяє ідентифікацію суб'єкта персональних даних без використання додаткової інформації, яка повинна зберігатися окремо із вжиттям усіх необхідних технічних та організаційних заходів, які не дають можливості відтворити зв'язок із суб'єктом персональних даних або ідентифікувати його;

суб'єкт персональних даних — фізична особа, персональні дані якої обробляються;

третя особа — фізична або юридична особа, за винятком суб'єкта персональних даних, контролера, оператора, а також інших осіб, які уповноважені обробляти

персональні дані під безпосереднім керівництвом такого контролера або оператора;

широкомасштабна обробка персональних даних – обробка значних обсягів персональних даних на регіональному, національному або міжнародному рівнях, яка може мати вплив на значну кількість суб'єктів персональних даних та яка може призвести до ризиків високого ступеню для їх прав та свобод.

2.Інші терміни в цьому Законі вживаються у значенні, наведеному в інших законах України, а також міжнародних актах.

Стаття 3. Законодавство про захист персональних даних

1.Законодавство у сфері захисту персональних даних становить Конституція України, цей та інші закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання Конституції та законів України інші нормативно-правові акти.

2. Якщо міжнародними актами, ратифікованими Верховною Радою України, встановлені інші правила обробки та захисту персональних даних, ніж у цьому Законі, застосовуються положення відповідних міжнародних актів.

Стаття 4. Принципи обробки персональних даних

1.Принципи обробки даних:

1) Законність, добросовісність та прозорість. Персональні дані повинні оброблятись на підставах, передбачених цим Законом. Персональні дані повинні оброблятися у спосіб, що передбачає належну поінформованість

суб’єкта персональних даних про обробку їхніх персональних даних (збір, використання та іншу обробку, її спосіб та обсяг), крім випадків, передбачених цим Законом, з метою забезпечення усунення непередбачуваного для суб’єкта персональних даних негативного впливу на нього від обробки персональних даних.

2) Обмеження мети. Персональні дані повинні збиратися для точно визначених, явних і легітимних цілей та не оброблятись у спосіб, що є несумісним з цими цілями. Контролер, зокрема, зобов’язаний визначити мету обробки персональних даних до початку їх збору та не може змінювати її після збору персональних даних без згоди суб’єкта персональних даних, крім випадків, передбачених статтею 13 цього Закону.

3) Мінімізація персональних даних. Склад та зміст персональних даних, що обробляються, повинен бути достатнім, адекватним, відповідним і ненадмірним відповідно до визначеної мети їх обробки.

Не допускається збір та обробка персональних даних, що:

є надмірними відповідно до визначеної мети;

призводять до надмірного втручання в приватне життя фізичної особи.

4) Точність персональних даних. Дані повинні бути точними та, в разі потреби, оновлюватись відповідно до цілі їх обробки. У разі виявлення, що персональні дані є не точними з огляду на мету їх обробки, такі персональні дані повинні бути без необґрунтованої затримки уточнені або знищені.

5) Обмеження зберігання. Дані повинні зберігатись у формі, що дозволяє ідентифікацію суб’єкта персональних даних не довше, ніж це необхідно для цілей, в яких вони обробляються, крім випадків, встановлених законом за умови дотримання сукупності наступних критеріїв: випадки мають бути встановлені

законом; становити необхідні та пропорційні заходи у демократичному суспільстві для забезпечення захисту конкретних цінностей , зокрема забезпечення громадської безпеки, важливих суспільних, економічних або фінансових інтересів); забезпечувати дотримання прав і свобод суб'єкта персональних даних. Персональні дані можуть зберігатись більший період часу для цілей архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей за умови вжиття технічних та організаційних заходів, які вимагаються для забезпечення дотримання прав і свобод суб'єкта персональних даних.

6) Цілісність і конфіденційність. Дані повинні оброблятися із вжиттям належних технічних та організаційних заходів в такий спосіб, що ґарантує їх належну безпеку, включаючи захист від несанкціонованої або неправомірної обробки, випадкової втрати, знищення або пошкодження.

7) Підзвітність. Контролер несе відповідальність за дотримання принципів, передбачених частиною першою цієї статті, та зобов'язаний вживати для цього усі належні організаційні та технічні заходи.

Обов'язок доведення дотримання цих принципів покладається на контролера. Контролер зобов'язаний вжити заходи, які забезпечують можливість підтвердження дотримання принципів обробки персональних даних.

РОЗДІЛ ІІ

ПІДСТАВИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 5. Підстави для обробки персональних даних

1. Обробка персональних даних є законною у разі:

1) надання згоди суб’єктом персональних даних на обробку його персональних даних для однієї або кількох точно визначених цілей;

2) укладення та виконання правочину, стороною якого є суб’єкт персональних даних або для здійснення заходів, що необхідні для укладення правочину, на вимогу суб’єкта персональних даних;

3) необхідності виконання юридичного обов’язку контролера персональних даних;

4) захисту життєво важливих інтересів суб’єкта персональних даних або іншої фізичної особи;

5) необхідності виконання завдань в суспільних інтересах або повноважень, покладених на контролера законом;

6) необхідності для цілей легітимного інтересу контролера або третьої особи, крім випадків, коли такі інтереси не переважають інтереси або основоположні права та свободи суб’єкта персональних даних, які вимагають захисту персональних даних, особливо якщо суб’єктом персональних даних є дитина.

2. Пункт 6 частини першої цієї статті не застосовується до випадків обробки персональних даних суб’єктами владних повноважень під час виконання їхніх повноважень, передбачених законодавством.

3. Легітимний інтерес контролера може полягати, зокрема, у обробці персональних даних для запобігання шахрайству, забезпечення інформаційної безпеки.

4. Для здійснення обробки персональних даних для цілі, іншої, ніж та, для якої вони були зібрані, якщо така обробка здійснюється не на підставі згоди суб’єкта персональних даних або закону, контролер має довести, що така нова ціль є

сумісною із ціллю, для якої персональні дані були зібрані з урахуванням норм статті 13 цього Закону.

5. Обробка персональних даних на підставі згоди суб'єкта персональних даних може здійснюватися лише у випадку відсутності інших передбачених частиною першою цієї статті підстав.

Стаття 6. Згода на обробку персональних даних

1. Згода суб'єкта персональних даних на обробку його персональних даних може бути надана:

1) у письмовій формі (заяви, анкети, заповнення бланку тощо), в тому числі поданої електронними засобами;

2) в електронній формі під час відвідування веб-сайту або користування електронною інформаційною системою, шляхом заповнення передбаченої інтерфейсом форми, проставлення у відповідному полі відмітки (позначки);

3) шляхом обрання відповідних технічних налаштувань в інтерфейсі веб-сайта, операційній системі, програмному забезпеченні, чи мобільному додатку, які передбачають обробку персональних даних;

4) через іншу ствердну дію чи поведінку, яка однозначно вказує на те, що суб'єкт персональних даних в конкретному випадку згоден на подальшу обробку його персональних даних.

2. Не є згодою суб'єкта персональних даних на обробку його персональних даних:

1) дії суб'єкта персональних даних, які не передбачають волевиявлення;

2) встановлені за замовчуванням налаштування веб-сайту, операційної системи, програмного забезпечення, мобільного додатку, в тому числі автоматичне заповнення передбаченої інтерфейсом форми або попереднє проставлення у відповідному полі відмітки (позначки) без безпосередньої участі конкретного суб’єкта персональних даних;

3) бездіяльність такого суб’єкта.

3. Згода не вважається вільною якщо:

1) суб'єкт персональних даних знаходиться у залежному чи підпорядкованому становищі відносно контролера, якому надається згода;

2) у суб’єкта персональних даних немає вільного вибору або немає можливості відмовити в наданні згоди або немає можливості відкликати раніше надану згоду, без настання негативних наслідків для себе;

3) у суб’єкта персональних даних відсутні альтернативні шляхи доступу до певних товарів, послуг, соціальних благ тощо, без надання ним згоди на обробку своїх персональних даних;

4) вона не передбачає окремого дозволу суб’єкта персональних даних на окремі види обробки персональних даних, незважаючи на те, що такий дозвіл є необхідним за індивідуальних обставин.

4. Не допускається відмова від надання суб’єкту персональних даних товарів, робіт чи послуг на підставі відмови суб’єкта від надання згоди.

5. Згода суб’єкта персональних даних на обробку його персональних даних вважається інформованою, якщо до її надання або на момент її надання суб'єкт персональних даних був проінформований про:

1) підставу, мету, вид обробки його персональних даних;

2) персональні дані, які підлягають обробці;

3) контактні дані контролера : постійне місце розташування та засоби зв'язку з ними у обсязі, який дозволяє суб'єкту персональних даних ідентифікувати такого контролера та оператора та безперешкодно зв'язатися з ними;

4) права, передбачені законодавством у сфері захисту персональних даних, та способи їх реалізації;

5) будь-яку іншу інформацію, необхідну для забезпечення чесної та прозорої обробки персональних даних.

Інформація, вказана в цій статті, надається суб’єктам персональних даних у доступний спосіб та зрозумілою мовою, які забезпечують її ясність та зрозумілість для відповідних суб’єктів персональних даних.

6. Згода на обробку персональних надається контролеру незалежно від форм та способів її надання.

7. Згода на обробку персональних даних не може бути підставою для обробки персональних даних суб’єктами владних повноважень, суб’єктами природних монополій, а також підприємствами, установами або організаціями, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором.

8. Якщо обробка персональних даних здійснюється на підставі згоди суб'єкта персональних даних, відповідний суб’єкт має право відкликати згоду в будь-який час.

9. Згоду на обробку персональних даних малолітньої особи надає її законний представник.

10. Контролер зобов’язаний вжити всіх розумних заходів для перевірки того, що згода надана суб’єктом персональних даних, який досяг 14 років, а у разі якщо суб’єкт є малолітньою особою, що згода надана від її імені законним представником.

11. Надана згода вважається недійсною з моменту її надання у разі недотримання вимог цієї статті.

12. Обов’язок доведення факту надання суб’єктом персональних даних згоди на обробку його даних з дотриманням вимог, передбачених цією статтею, покладається на контролера.

РОЗДІЛ ІІІ

СПЕЦІАЛЬНІ ВИМОГИ ДО ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 7. Особливі вимоги до обробки персональних даних (чутливі персональні дані)

1.Забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в професійних спілках, а також генетичних та біометричних даних, даних, що стосуються здоров'я, статевого життя або сексуальної орієнтації, психометричних даних.

2. Положення частини першої цієї статті не застосовується, якщо обробка персональних даних:

1) здійснюється за умови надання суб'єктом персональних даних явної згоди на обробку таких даних відповідно до статті 6 цього Закону, крім випадків, коли обробка персональних даних на підставі згоди заборонена;

2) необхідна для здійснення прав та виконання обов'язків контролера або суб’єкта персональних даних у сфері трудових правовідносин або соціального захисту у випадках, передбачених законом. Такий закон має передбачати належні гарантії захисту прав та інтересів суб’єкта персональних даних;

3) необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої фізичної особи у разі, якщо суб'єкт персональних даних фізично неспроможний надати згоду або є недієздатним;

4) здійснюється із забезпеченням відповідного захисту організацією, об’єднанням або будь-якою неприбутковою організацією в політичних, світоглядних, релігійних або профспілкових цілях за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв’язку з цілями діяльності організації та що персональні дані не розкриваються за межами цієї організації без згоди суб’єкта персональних даних;

5) стосується даних, які суб'єкт персональних даних явно оприлюднив. Для цілей цього Закону під формулюванням «явно оприлюднено» необхідно розуміти оприлюднення персональних даних в такій формі або у такий спосіб, які уможливлюють ознайомлення з ними необмеженого кола осіб;

6)необхідна для подання, обґрунтування або захисту юридичної вимоги або необхідна для здійснення судом його повноважень;

7) необхідна в цілях значного суспільного інтересу у випадках, передбачених законом, за умови, що такий закон є пропорційним відносно цілі, яка переслідується, враховує принцип поваги до суті права на захист персональних даних та передбачає належні та відповідні засоби захисту основоположних прав та інтересів суб’єкта персональних даних;

8) необхідна в цілях профілактики та лікування професійних захворювань, оцінки працездатності працівника, встановлення медичного діагнозу, надання соціальних послуг або послуг в сфері охорони здоров'я (включаючи електронну систему охорони здоров'я), лікування або управління системою охорони здоров'я та соціальних послуг на підставі закону або договору із працівниками закладів охорони здоров'я за умови дотримання умов та гарантій, передбачених частиною другою цієї статті;

9) необхідна в цілях суспільного інтересу в сфері громадського здоров'я, такого як захист від серйозних транскордонних загроз для здоров'я або забезпечення високих стандартів якості та безпеки послуг з охорони здоров'я та медичних продуктів або медичного устаткування у випадках, передбачених законом, який передбачає належні і відповідні засоби захисту основоположних прав та свобод суб'єкта персональних даних, зокрема, професійної таємниці;

10) необхідна в цілях архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей, що здійснюється на підставі закону, який є пропорційним відносно мети, яка переслідується, та враховує принцип поваги до суті права на захист персональних даних та передбачає належні та відповідні засоби захисту основоположних прав та інтересів суб'єкта персональних даних;

11) необхідна в цілях попередження, розслідування, виявлення правопорушень або виконання кримінальних покарань або покарань за адміністративні правопорушення, у випадках визначених законом, який має передбачати належні гарантії захисту прав та інтересів суб'єкта персональних даних.

3. Обробка персональних даних, вказаних в частині першій цієї статті, здійснюється на підставі закону посадовою (службовою) особою за умови, якщо ця особа несе відповідальність за розголошення професійної таємниці

відповідно до закону. Доступ до такої інформації можуть мати посадові (службові) особи, які несуть відповідальність за розголошення професійної таємниці відповідно до закону.

Стаття 8. Обробка персональних даних, пов’язаних з притягненням до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості, а також пов'язаних із цим заходів безпеки

1. Обробка персональних даних, пов’язаних з притягненням осіб до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості, а також пов'язаних із цим заходів безпеки, може здійснюватись у випадках, передбачених законом, який містить належні гарантії для захисту прав і свобод суб’єкта персональних даних згідно з Конституцією та міжнародними договорами, згода на обов’язковість яких надана Верховною Радою України.

2. Контроль за обробкою персональних даних, пов’язаних з притягненням осіб до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості, а також пов'язаних із цим заходів безпеки, здійснюється контролюючим органом у затвердженому ним порядку.

Стаття 9. Обробка біометричних даних суб’єктами владних повноважень

1. Обробка біометричних даних є правомірною у разі дотримання сукупності вимог:

1) якщо вона передбачена законом, який передбачає належні гарантії захисту прав суб'єкта даних відповідно до Конституції України та міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України;

2) здійснюється з метою національної безпеки, економічного добробуту, прав людини;

3) є необхідною в демократичному суспільстві у випадках передбачених частиною другою статті 7 цього Закону.

2. Обробка біометричних даних суб’єктами владних повноважень є правомірною, якщо вона здійснюється з метою:

1) забезпечення національної безпеки, оперативно-розшукової та контррозвідувальної діяльності, протидії злочинності, підтримання громадської безпеки і порядку, економічного добробуту та прав людини;

2) авторизації користувачів в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, задля уникнення розголошення інформації з обмеженим доступом в процесі виконання покладених на них функцій та повноважень, якщо досягнення зазначених цілей іншими засобами неможливе або пов’язане з непропорційними зусиллями;

3) оформлення в порядку, встановленому законодавством, документів, що посвідчують особу, підтверджують її громадянство або спеціальний статус.

Стаття 10. Здійснення відеоспостереження

1. Здійснення суб’єктами владних повноважень, правоохоронними органами відеоспостереження в громадських та публічних місцях, інших місцях загального користування, включаючи громадський транспорт, допускається

лише у випадках, передбачених законодавством, з метою попередження правопорушень та забезпечення громадської безпеки.

2. Здійснення відеоспостереження юридичними або фізичними особами, допускається в цілях попередження правопорушень та захисту майна в будівлях та на територіях, які перебувають у їхній власності або законному володінні чи користуванні, на підставі законодавства.

3. Відеоспостереження допускається лише у разі, якщо за конкретних обставин не можна досягнути легітимної мети іншими заходами, ступінь втручання у приватне життя осіб яких є меншим та якщо інші заходи не призведуть до непропорційних витрат.

4. Контролюючий орган затверджує типовий порядок здійснення відеоспостереження.

5. Контролер зобов'язаний розмістити попередження про те, що здійснюється відеоспостереження, на доступному для кожного місці офіційною державною мовою та однією із мов, яка є найбільш розповсюдженою у відповідному населеному пункті. Попередження повинно містити назву та контактні дані контролера та особи, яка здійснює відеоспостереження, якщо вона є відмінною від контролера.

6. Забороняється обробляти персональні дані, зібрані засобами відеоспостереження, у спосіб, несумісний з цілями, задля яких вони були зібрані.

7. Відеоспостереження за житлом фізичних осіб або в приміщеннях, де особа проживає, особами, які там не проживають, не допускається, крім випадків, встановлених законом. Відеоспостереження житлових будівель, крім того, що здійснюється в цілях розслідування злочину відповідно до кримінального

процесуального законодавства, допускається виключно з метою забезпечення безпеки фізичних осіб та захисту майна на підставі згоди більше половини власників такої будівлі та за таких умов:

1) відеоспостереження може здійснюватися лише за входом та загальними приміщеннями будівлі;

2) перегляд збережених відеозаписів допускається лише у випадку протиправних дій або обґрунтованої підозри протиправних дій з метою встановлення обставин та/або осіб, винних у вчиненні таких дій.

8. Персональні дані, зібрані в результаті відеоспостереження на підставі цієї статті, можуть зберігатись не більше 6 місяців.

9. Забороняється здійснення відеоспостереження в приміщеннях, в яких розумно очікується, що особа може здійснити повне або часткове оголення частин тіла, які зазвичай не підлягають оголенню в публічних місцях, а також в місцях, призначених для задоволення гігієнічних чи фізіологічних потреб.

10. У разі якщо в результаті відеоспостереження відеозаписи зберігаються, особа яка здійснює відеоспостереження, зобов'язана створити базу даних, призначену для зберігання відеозаписів. Разом з відеозаписами в системі повинна зберігатись інформація про дату, місце і час здійснення запису, а також відомості про осіб які переглядали збережені відеозаписи, дату, місце, час та підстави здійснення перегляду відеозапису.

11. Вимоги до здійснення відеоспостереження, передбачені цією статтею, застосовуються до фото- та відеозйомки, яка здійснюється в аналогічний спосіб з такими ж цілями.

Стаття 11. Обробка персональних даних в результаті аудіо, відео або фото фіксації публічних заходів

1. У разі здійснення аудіозапису, відеозйомки, кінозйомки, фотозйомки або будь-якої іншої фіксації зображення або голосу суб'єкта персональних даних, незалежно від технології що використовувалася, відкрито на вулиці або на заходах публічного характеру (публічних зборах, конференціях тощо), контролер зобов’язаний завчасно вжити достатніх заходів для повідомлення суб’єктів персональних даних про здійснення аудіозапису, відеозйомки, кінозйомки, фотозйомки або будь-якої іншої фіксації зображення або голосу суб'єкта персональних даних у спосіб, який надає можливість суб’єкту персональних даних заперечити проти обробки його персональних даних.

2. Оприлюднення, у тому числі публічний показ матеріалів відеозйомки, кінозйомки або фотозйомки, на яких можна ідентифікувати суб'єктів персональних даних, допускається за умови, що оприлюднення є пропорційним відносно легітимної цілі, яка переслідується, враховує принцип поваги до суті права на захист персональних даних та передбачає належні та відповідні засоби захисту основоположних прав та інтересів суб’єкта персональних даних.

Стаття 12. Обробка персональних даних з метою прямого маркетингу, передвиборчої агітації та політичної реклами

1. Обробка персональних даних з метою прямого маркетингу, передвиборчої агітації, політичної реклами та профілювання з цими цілями, зокрема з використанням соціальних мереж, автоматизованих систем аудіо та відео дзвінків, надсилання електронних повідомлень, електронних листів, здійснюється виключно на підставі явної згоди суб’єкта персональних даних на таку обробку, окрім випадків передбачених частиною другою цієї статті.

2. Обробка персональних даних з метою прямого маркетингу, без згоди суб’єкта персональних даних, на підставі легітимного інтересу контролера, можлива виключно у разі дотримання усіх зазначених нижче вимог:

контактні дані суб’єкта персональних даних отримані внаслідок укладення та виконання правочину, стороною якого є суб’єкт персональних даних або для здійснення заходів, що необхідні для укладення правочину, на вимогу суб’єкта персональних даних;

прямий маркетинг здійснюється з метою пропонування аналогічних або супутніх товарів чи послуг відносно тих що були предметом первинного правочину;

під час отримання контактних даних, суб'єкта персональних даних було повідомлено про намір подальшої їх обробки з метою прямого маркетингу та надано можливість відмовитися від такої обробки;

можливість відмовитися від обробки персональних даних з метою прямого маркетингу повинна надаватися суб’єкту персональних даних кожного разу, коли здійснюються заходи прямого маркетингу;

можливість відмовитися від обробки персональних даних з метою прямого маркетингу не повинна мати негативних наслідків для суб'єкта персональних даних та не повинна вимагати від нього докладання більших зусиль, витрат та часу, ніж первинне надання його контактних даних;

ступінь втручання в приватне життя суб'єкта персональних даних не більша ніж була необхідна з метою виконання первинного правочину.

3. Якщо персональні дані обробляються з метою, передбаченою частиною першою цієї статті, суб’єкт персональних даних має право відкликати свою згоду на таку обробку та право на заперечення проти обробки, включаючи здійснення профілювання для прямого маркетингу, в будь-який час. У разі якщо суб’єкт персональних даних відкликає свою згоду або заперечує проти обробки персональних даних з метою, передбаченою частиною першою цієї статті,

контролер зобов’язаний припинити таку обробку негайно з моменту отримання відповідної вимоги суб’єкта персональних даних.

4. У разі, якщо суб’єкт персональних даних заперечує проти обробки персональних даних з метою, передбаченою цією статтею, ці персональні дані підлягають видаленню контролером.

5. Не допускається обробка персональних даних осіб, які не досягли 14 років, з метою прямого маркетингу та профілювання з цією метою.

Стаття 13. Обробка персональних даних з іншою метою, ніж та, з якою вони збирались

1. Обробка персональних даних з іншою метою (нова мета), ніж та, з якою вони збирались (первинна мета), забороняється, крім випадків, якщо нова мета є сумісною з первинною. Для визначення того, чи є нова мета сумісною з первинною, враховується:

1) наявність зв’язку між первинною метою та новою метою;

2) обставини, за яких персональні дані було зібрано;

3) особливості обробки персональних даних, передбачені статтями 7 та 8 цього Закону;

4) можливі наслідки обробки персональних даних з новою метою для суб’єкта персональних даних;

5) наявність відповідних та достатніх гарантій для захисту прав і свобод суб’єкта персональних даних у первинній обробці персональних даних та обробці, яка планується, що можуть включати шифрування або псевдонімізацію.

2. Обробка для цілей архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей вважається обробкою, сумісною з початковою метою.

3. Якщо нова мета є несумісною з первинною метою, обробка персональних даних з новою метою є правомірною у випадках:

1) надання суб'єктом персональних даних згоди на обробку даних з новою метою;

2) якщо така обробка необхідна для виконання юридичного обов'язку, передбаченого законом, який містить належні гарантії для захисту прав і свобод суб'єкта персональних даних згідно з Конституцією та міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України.

Стаття 14. Обробка персональних даних з метою архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей

1. Обробка персональних даних для цілей архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей здійснюється виключно, якщо це необхідно для досягнення цих цілей з урахуванням принципу мінімізації даних. Контролер зобов'язаний знеособити дані у разі, якщо це не перешкодить досягненню визначених цілей. У разі, якщо цілей обробки неможливо досягти шляхом обробки даних через знеособлення персональних даних, контролер зобов'язаний застосувати псевдонімізацію, якщо це не перешкодить досягненню визначених цілей.

2. Контролер, який здійснює обробку персональних даних з метою наукового або історичного дослідження, може обмежити права суб'єкта персональних даних, передбачених статтями 19, 21, 22, 24 цього Закону, в тій мірі, в якій їх

реалізація призведе до неможливості досягнення цих цілей та таке обмеження є необхідним для їх досягнення.

Обмеження прав суб'єкта персональних даних, передбачених частиною другою статті 14 цього Закону, є правомірними у разі вжиття технічних та організаційних заходів з метою дотримання принципу мінімізації персональних даних.

3. Якщо обробка персональних даних здійснюється з метою формування, обліку, зберігання і використання Національного архівного фонду права суб'єкта персональних даних, передбачені статтями 19 та 21 цього Закону, реалізовуються в порядку визначеному Законом України «Про Національний архівний фонд та архівні установи» або іншими законами.

Стаття 15. Обробка персональних даних для цілей журналістської чи творчої діяльності

1. До обробки персональних даних для цілей журналістської та творчої діяльності не застосовуються положення п. 1 частини першої статті 4 щодо принципів добросовісності та прозорості, пунктів 4 і 6 частини першої статті 4, статей 18-27, статті 34, статей 36-40 цього Закону.

2.Частина перша цієї статті застосовується лише за умови, якщо контролер, що здійснює обробку персональних даних винятково для цілей журналістської та творчої діяльності, обґрунтовано вважає, що оприлюднення інформації здійснюється в суспільних інтересах, а шкода від оприлюднення такої інформації не переважає суспільний інтерес в її отриманні.

3. Для цілей цієї статті поняття журналістська діяльність підлягає тлумаченню з урахуванням практики Європейського суду з прав людини.

Стаття 16. Обробка персональних даних після смерті суб'єкта персональних даних

1. Згода суб'єкта персональних даних є чинною протягом 10 років після його смерті, якщо суб'єкт персональних даних не прийняв іншого рішення до його смерті. Якщо смерть суб'єкта персональних даних настала у віці до 18 років, його згода є чинною протягом 20 років після його смерті, якщо суб'єкт персональних даних не прийняв іншого рішення до його смерті.

2. Після смерті суб'єкта персональних даних обробка його персональних даних дозволяється на підставі згоди його нащадків. Згода нащадків не вимагається, якщо:

1) з дня смерті суб'єкта персональних даних пройшло 10 років;

2) з дня смерті суб'єкта персональних даних, який на день смерті не досяг 18 років, пройшло 20 років;

3) обробка персональних даних здійснюється на підставах, передбачених цим Законом.

3. Якщо померлий суб'єкт персональних даних має декількох нащадків, обробка його персональних даних після смерті здійснюється на підставі згоди одного із нащадків. У такому випадку контролер зобов'язаний вжити всіх заходів для повідомлення інших нащадків про обробку персональних даних померлого суб'єкта персональних даних та роз'яснення права на заперечення проти обробки тих персональних даних померлого суб'єкта персональних даних, які одночасно є персональними даними таких нащадків.

4. Згода, передбачена частиною другою цієї статті, не вимагається у разі, якщо персональні дані померлого суб'єкта персональних даних, що обробляються,

містять виключно часткове або повне ім’я, стать, дату народження та дату смерті, факт смерті, а також дату та місце поховання.

Стаття 17. Використання технологій відстеження дій суб’єктів персональних даних у електронних комунікаціях та сервісах

1. Відстеження дій суб'єктів персональних даних за допомогою програмного забезпечення, мобільних чи інших застосунків, веб-сайтів, інших технологій електронних комунікацій та сервісів, а також за допомогою пристроїв, які належать чи використовуються суб'єктом персональних даних, забороняється крім випадків, визначених цим Законом.

2. Обробка персональних даних, передбачених частиною першою цієї статті, є правомірною, за умови дотримання принципів обробки персональних даних, встановлених цим Законом, у випадку:

1) надання суб’єктом персональних даних явної згоди на таку обробку;

2) обробка є необхідною для забезпечення функціонування програмного забезпечення, мобільного чи іншого застосунку, веб-сайту чи іншої телекомунікаційної технології;

3) обробка є виключно необхідною для надання послуги суб’єкту персональних даних за його замовленням.

3. Контролери та оператори, які здійснюють обробку персональних даних, передбачених частиною першою цієї статті, повинні забезпечити, щоб кожний суб'єкт, чиї дані будуть оброблятися, ознайомився з повідомленням про таку обробку до її початку. Повідомлення має містити:

1) опис технології відстеження та інформацію передбачену статтею 18 цього Закону;

2) роз’яснення про те, що суб’єкт персональних даних має право обрати, на яку технологію він надає згоду, у разі якщо обробка відбувається на підставі згоди.

4. Контролери та оператори, які здійснюють обробку персональних даних, передбачених частиною першою цієї статті, повинні забезпечити:

1) автоматизований доступ суб'єктів персональних даних до всієї інформації про них, яка зібрана або створена у процесі такої обробки, включаючи доступ до профілів користувача та інших даних створених у результаті обробки відомостей про суб'єкта персональних даних;

2) безумовну автоматизовану можливість внесення суб'єктом персональних даних будь-яких змін до його персональних даних, що обробляються, включаючи їх видалення.

5. Забороняється відмовляти суб’єкту персональних даних у наданні доступу до веб-сайту (його окремих частин) або обмежувати використання програмного забезпечення, мобільного чи іншого застосунку, чи іншої телекомунікаційної технології або сервісу на підставі його відмови у наданні згоди на обробку персональних даних, передбачених частиною першою цієї статті.

РОЗДІЛ IV

ПРАВА СУБ’ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 18. Право на інформацію

1. Якщо персональні дані збираються безпосередньо від суб’єкта персональних даних, контролер, який збирає персональні дані, при отриманні персональних даних або раніше зобов’язаний повідомити такому суб'єкту інформацію про:

1) контролера персональних даних - ідентифікаційні, та контактні дані контролера, та у разі наявності - його представника;

2)дані про оператора(ів) у разі його(їх) наявності;

3) контактні дані особи, відповідальної за захист персональних даних контролером;

4) мета, цілі та способи обробки;

5) дії або сукупність дій, які будуть здійснюватися з персональними даними;

6) персональні дані, які оброблятимуться;

7) підстави для обробки персональних даних відповідно до цього Закону;

8) одержувачів або категорії одержувачів, яким передаються або можуть передаватися персональні дані;

9) передачу персональних даних до іноземних держав або міжнародних організацій, а також інформацію про наявність або відсутність належного рівня захисту в цій державі або міжнародній організації;

10) строк, протягом якого зберігатимуться персональні дані або критерії для його визначення, якщо конкретний строк в момент збору персональних даних визначити неможливо;

11) право подати скаргу до контролюючого органу та контактні дані такого органу;

12) форму, зміст та порядок надання або відкликання згоди на обробку персональних даних, якщо обробка таких даних здійснюється на підставі згоди;

13) права суб’єкта персональних даних згідно з цим Законом;

14) наслідки, пов'язані з наданням або ненаданням, персональних даних;

15) наявність механізму автоматизованого прийняття рішень, у тому числі профілювання та необхідну інформацію про алгоритми (логіку), що використовуються у таких механізмах, а також значимість та передбачувані наслідки такої обробки для суб'єкта персональних даних;

16) здійснення обробки персональних даних для цілей прямого маркетингу, а також про право відмовитися від обробки персональних даних для таких цілей.

2. Положення частини першої цієї статті не застосовується, якщо суб'єкт персональних даних вже має цю інформацію.

3. Якщо персональні дані збираються не безпосередньо від суб'єкта персональних даних, інформація, передбачена частиною першою цієї статті, а також відомості про джерела отримання персональних даних, повідомляються суб'єкту персональних даних контролером:

1) не пізніше тридцяти днів з моменту збору персональних даних;

2) якщо персональні дані будуть використовуватися для здійснення комунікації з суб'єктом персональних даних — одночасно з першим контактом;

3) якщо передбачається поширення персональних даних — до першого факту такого поширення.

4. Положення частини третьої цієї статті не застосовується у випадках:

1) суб'єкт персональних даних вже має інформацію, передбачену частиною першою цієї статті;

2) надання такої інформації є неможливим у зв'язку з відсутністю контактних даних суб'єкта персональних даних або неможливістю встановити з ним зв'язок з використанням наявних контактних даних;

3) збір та оприлюднення персональних даних прямо передбачені законом;

4) якщо інформація про обробку персональних даних контролером становить передбачену законом таємницю;

5) якщо надання такої інформації становитиме надмірний тягар для контролера, зокрема якщо обробка здійснюється для цілей архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей за умови дотримання умов, передбачених статтею 14 цього Закону.

5. Інформація, вказана в цій статті, надається суб'єктам персональних даних у доступний спосіб та зрозумілою мовою, які забезпечують її ясність та зрозумілість для відповідних суб'єктів персональних даних.

Стаття 19. Право суб'єкта персональних даних на доступ до персональних даних

1. Суб'єкт персональних даних має право на отримання від контролера інформацію про обробку або відсутність обробки його персональних даних, а у разі здійснення обробки - право на доступ до персональних даних та право на отримання інформації про:

1) цілі обробки;

2) склад персональних даних, які обробляються;

3) одержувачів та/або категорії одержувачів;

4) строк, протягом якого зберігатимуться персональні дані або критерії для його визначення, якщо конкретний строк в момент збору персональних даних визначити неможливо;

5) право на виправлення або на забуття, обмеження обробки персональних даних або заперечення проти обробки персональних даних;

6) право на подання скарги до контролюючого органу;

7) джерело збору персональних даних у разі, якщо дані збирались не від суб'єкта персональних даних;

8) наявність механізму автоматизованого прийняття рішень, у тому числі профілювання та інформацію про алгоритми (логіку), що використовуються у таких механізмах, а також значимість та передбачувані наслідки такої обробки для суб'єкта персональних даних;

9) відповідні гарантії захисту прав суб'єкта персональних даних у разі передачі персональних даних до іншої держави або міжнародної організації.

2. Суб'єкт персональних даних має право отримати копію своїх персональних даних, які обробляються контролером безоплатно.

3. Контролер зобов'язаний зберігати інформацію про джерело зібраних персональних даних, необхідних для доведення правомірності їх обробки.

4. Право на доступ суб'єкта персональних даних може бути обмежено на підставах, визначених цим Законом та іншими законами, якщо таке обмеження переслідує легітимну мету та є пропорційним.

5.Інформація, вказана в цій статті, надається суб'єктам персональних даних у доступний спосіб та зрозумілою мовою, які забезпечують її ясність та зрозумілість для відповідних суб'єктів персональних даних.

Стаття 20. Право суб'єкта персональних даних на виправлення персональних даних

1. Суб’єкт персональних даних має право на виправлення контролером неточних персональних даних без надмірної затримки в строк не більше тридцяти днів. Суб’єкт даних має право на доповнення персональних даних в залежності від мети обробки шляхом надання додаткових персональних даних контролеру.

2. Контролер має право отримати від суб’єкта персональних даних додаткові дані для виправлення. На вимогу суб’єкта персональних даних контролер зобов’язаний позначити персональні дані як такі, точність яких оскаржується, з моменту звернення суб’єкта персональних даних до контролера з заявою про виправлення своїх персональних даних і до прийняття рішення в результаті розгляду заяви, а у разі оскарження рішення контролера до суду, до постановлення остаточного рішення суду.

3. Контролер зобов’язаний повідомити всіх одержувачів, яким було відкрито персональні дані, про задоволення вимоги про виправлення даних, крім випадків, коли таке повідомлення становить для контролера надмірний тягар.

Стаття 21. Право суб’єкта персональних даних на забуття

1. Суб’єкт персональних даних має право на забуття, тобто на повне знищення контролером його персональних даних без надмірної затримки.

2. Контролер зобов’язаний знищити персональні дані без надмірної затримки в строк не більше тридцяти днів у разі, якщо:

1) відсутня необхідність подальшої обробки персональних даних, для цілей, для яких вони збирались або оброблялись;

2) суб'єкт персональних даних відкликав згоду, на підставі якої здійснювалась обробка персональних даних, та відсутні інші юридичні підстави для обробки;

3) суб'єкт персональних даних заперечує проти обробки відповідно до частини першої статті 22 цього Закону та відсутні переважаючі юридичні підстави для обробки або якщо суб'єкт персональних даних заперечує проти обробки відповідно до частини другої статті 22 цього Закону;

4) обробка персональних даних здійснювалась неправомірно;

5) персональні дані були зібрані для пропозиції суб'єкту персональних даних послуг інформаційного суспільства.

3. Якщо контролер, який зобов’язаний знищити персональні дані, поширив їх раніше, він має вжити всіх достатніх заходів, враховуючи наявні технологічні можливості, для повідомлення інших контролерів, які здійснюють обробку персональних даних, про вимогу суб’єкта персональних даних щодо знищення будь-яких посилань або копій персональних даних, крім випадків, коли таке повідомлення становить для контролера надмірний тягар.

4. Частини перша та друга цієї статті не застосовуються у разі, якщо обробка персональних даних необхідна для:

1) реалізації права на свободу вираження поглядів та інформації;

2) виконання юридичного обов'язку, який передбачає обробку на підставах, визначених законом;

3) цілей суспільного інтересу в сферах охорони здоров'я відповідно до пунктів 7 і 8 частини першої та другої статті 7 цього Закону;

4) цілей архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей, якщо реалізація права, передбаченого цією статтею, призведе до неможливості або становитиме серйозні перешкоди для досягнення цілей обробки;

5) необхідна для подання, обґрунтування або захисту юридичної вимоги.

Стаття 22. Право на заперечення проти обробки персональних даних

1. Суб’єкт персональних даних має право на заперечення в будь-який час проти обробки його персональних даних, яка здійснюється на підставі пунктів 5 та 6 частини першої статті 5 цього Закону, включаючи здійснення на підставі вказаних положень прямого маркетингу, профілювання. Контролер зобов’язаний припинити подальшу обробку, крім випадків, якщо обробка персональних даних здійснюється на законних підставах, які переважають інтереси, права та свободи суб’єкта персональних даних, або обробка необхідна для подання, обґрунтування або захисту юридичної вимоги. Доведення переважання законних підстав для обробки персональних даних є обов’язком контролера.

2. У сфері надання послуг інформаційного суспільства суб’єкт персональних даних може реалізувати своє право на заперечення за допомогою автоматизованих засобів.

3. Контролер повинен повідомити суб’єкта персональних даних, не пізніше першої з ним комунікації, про право, передбачене частинами першою та другою цієї статті.

4. Якщо обробка персональних даних здійснюється в цілях архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей, суб’єкт має право на заперечення проти обробки, крім випадків, коли вона необхідна для виконання завдань в суспільних інтересах.

Стаття 23. Право на мобільність персональних даних

1. Суб’єкт персональних даних має право вимагати від контролера надання копії будь-яких персональних даних такого суб’єкта, зібраних контролером під час автоматизованої обробки у структурованому та машинозчитуваному форматі.

2. Суб’єкт персональних даних має право на отримання особисто та/або передачу зазначених персональних даних від одного контролера іншому без перешкод з боку першого контролера на підставі відповідного запиту суб'єкта персональних даних у разі наявності відповідної технічної можливості.

3. У тому випадку, якщо вимога суб’єкта персональних даних, передбачена частиною першою цієї статті покладає на контролера надмірний тягар, контролер має право вимагати компенсації таких витрат за рахунок відповідного суб’єкта персональних даних за умов їх належного обґрунтування. Положення щодо компенсації витрат не застосовується, якщо:

1) внаслідок обробки персональних даних контролер отримав прибуток, розмір якого перевищує витрати на виконання вимог частини першою цієї статті;

2) внаслідок обробки персональних даних було завдано шкоди законним інтересам суб'єкта персональних даних;

3) обробка персональних даних здійснювалася з порушенням вимог цього Закону.

4. Право суб’єкта персональних даних, передбачене цією статтею, може бути обмежено на підставі закону, якщо обмеження переслідує легітимну мету та є необхідним в демократичному суспільстві.

5. Реалізація права, передбаченого цією статтею, не обмежує право суб’єкта персональних даних, передбачене статтею 21 цього Закону.

Стаття 24. Право на обмеження обробки персональних даних

1. Суб’єкт персональних даних має право на обмеження обробки персональних даних контролером у разі якщо:

1) суб’єкт персональних даних оскаржив точність персональних даних – протягом періоду перевірки точності персональних даних контролером;

2) обробка персональних даних є неправомірною і суб’єкт персональних даних заперечує проти видалення персональних даних та натомість вимагає обмежити їх використання;

3) у контролера більше немає необхідності в обробці персональних даних для цілей обробки, але вони необхідні суб’єкту персональних даних для подання, обґрунтування або захисту юридичної вимоги;

4) суб’єкт персональних даних заперечив проти обробки персональних даних відповідно до статті 22 цього Закону – до прийняття контролером рішення щодо переважання правомірних підстав для обробки над інтересами та правами суб’єкта персональних даних.

2. Якщо контролер обмежив обробку персональних даних відповідно до частини першої цієї статті, такі персональні дані, крім їх зберігання, можуть оброблятись виключно у одному з таких випадків:

1) суб’єкт персональних даних надав згоду на таку обробку персональних даних;

2) обробка персональних даних необхідна для подання, обґрунтування, захисту юридичної вимоги;

3) обробка персональних даних необхідна для захисту прав іншої фізичної чи юридичної особи;

4) наявності суспільного інтересу, який переважає над правами та інтересами суб'єкта персональних даних.

3. Контролер повинен завчасно повідомити суб’єкта персональних даних про зняття обмеження, накладеного за його вимогою.

4. Контролер зобов’язаний повідомити всіх одержувачів, яким було розкрито персональні дані, про обмеження обробки, виправлення чи видалення персональних даних, крім випадків, коли таке повідомлення становить для контролера надмірний тягар.

Стаття 25. Право на захист від автоматизованого прийняття рішення

1. Прийняття рішення, яке має юридичні наслідки для суб’єкта персональних даних або іншим чином має значний вплив на нього, виключно на підставі автоматизованої обробки його персональних даних забороняється.

2. Частина перша цієї статті не застосовується у випадках, якщо прийняття рішення:

1) необхідне для укладення або виконання договору між суб’єктом персональних даних та контролером;

2) передбачено законом, який передбачає належні і відповідні засоби захисту основоположних прав та свобод суб’єкта персональних даних;

3) здійснюється на підставі явної згоди суб’єкта персональних даних.

3. Якщо рішення приймається на підставі пункту 1 та пункту 3 частини другої цієї статті, контролер повинен вжити відповідних і достатніх заходів для захисту прав і свобод суб’єкта персональних даних та його легітимних інтересів. У таких випадках суб’єкт персональних даних має право на перегляд рішення контролером без застосування автоматизованої обробки даних, право

на врахування контролером позиції суб’єкта персональних даних та право на оскарження прийнятого рішення.

4. Приймати рішення у випадках, передбачених частиною другою цієї статті, на підставі даних, передбачених статтею 7 цього Закону, забороняється, крім випадків, коли обробка здійснюється на підставі пунктів 1 та 7 частини другої статті 7 цього Закону та за умови наявності відповідних і достатніх заходів захисту прав і свобод суб’єкта персональних даних та його легітимних інтересів.

Стаття 26. Право суб’єкта персональних даних на захист своїх прав та відшкодування шкоди

1. Суб’єкт персональних даних має право звернутись із скаргою на порушення його прав, передбачених цим Законом або порушення будь-яких положень цього Закону до контролюючого органу або до суду.

2. Суб’єкт персональних даних має право на відшкодування матеріальної та/або моральної шкоди, завданої в результаті порушення його прав, передбачених цим Законом. Відповідальність за порушення несе контролер. Оператор несе відповідальність за шкоду, заподіяну обробкою лише тоді, коли він не дотримується обов’язків відповідно до цього Закону, спрямованих безпосередньо на оператора, або якщо оператор діє всупереч законним вказівкам контролера.

3. Контролер звільняється від відповідальності за шкоду, завдану суб’єкту персональних даних, якщо доведе, що події, які спричинили завдання такої шкоди, мали місце не з його вини та він вжив всіх обґрунтованих заходів для попередження порушення прав та настання шкоди.

4. Для відшкодування шкоди, завданої суб’єкту персональних даних в результаті обробки персональних даних спільними контролерами, суб’єкт персональних даних може звернутись із скаргою або позовом до одного з таких контролерів. Відшкодування шкоди у такому випадку стягується з контролера персональних даних, до якого пред’явлено позов або подано скаргу. Контролер, який зобов’язаний за рішенням суду або контролюючого органу сплатити відшкодування шкоди, завданої спільно з іншими контролерами, має право звернутись з позовом до таких контролерів в порядку регресу пропорційно до їхньої участі в процесі обробки персональних даних, яким було завдано шкоду.

5. Контролер, який відшкодував суб’єкту персональних даних шкоду, завдану діями оператора персональних даних, має право вимагати від такого оператора відшкодування в порядку регресу.

Стаття 27. Порядок розгляду вимог суб’єкта персональних даних

1. З метою реалізації прав, передбачених цим Законом, суб’єкт персональних даних звертається до контролера з заявою, яка має містити :

1) персональні дані, достатні для ідентифікації суб’єкта персональних даних;

2) контактні дані;

3) вимогу про реалізацію права, передбаченого цим Законом.

2. Заява може бути подана у письмовій або електронній формі. Суб’єкт персональних даних має право звернутись до контролера в усній формі у разі, якщо контролер може здійснити його ідентифікацію.

3. Контролер приймає рішення за заявою суб’єкта персональних даних невідкладно, але у строк не більше одного місяця від дня її надходження. У разі якщо заява стосується обробки персональних даних, вказаних в статті 7 цього

Закону, контролер приймає рішення у строк до десяти днів з дня отримання заяви. У разі якщо для розгляду заяви з дотриманням вимог цього Закону контролеру необхідно отримати від суб'єкта персональних даних додаткову інформацію для його ідентифікації, він повідомляє про це суб'єкта персональних даних протягом десяти днів з дня отримання заяви. Строк прийняття рішення відраховується з дня, коли суб'єкт даних надав необхідну для ідентифікації інформацію. Доведення необхідності отримання додаткової інформації від суб'єкта персональних даних є обов'язком контролера.

4. Контролери, крім суб'єктів владних повноважень, можуть з урахуванням рекомендації контролюючого органу, встановлювати порядок ідентифікації суб'єкта персональних даних, необхідний для дотримання вимог цього Закону.

5. Відповідь про прийняте рішення за заявою контролер надає суб'єкту персональних даних письмово. У разі відмови у задоволенні заяви контролер повідомляє суб'єкта персональних даних про:

1) юридичну підставу для відмови у задоволенні заяви;

2) обґрунтування застосовності цієї підстави до обставин суб'єкта персональних даних;

3)порядок оскарження рішення до контролюючого органу або до суду.

6. Реалізація прав суб'єкта персональних даних, передбачених цим Законом, здійснюється безкоштовно. Контролер може обґрунтовано відмовити від задоволення заяви суб'єкта персональних даних у разі, якщо суб'єкт персональних даних зловживає своїми правами.

РОЗДІЛ V

ОБОВ'ЯЗКИ КОНТРОЛЕРА ТА ОПЕРАТОРА

Стаття 28. Загальні обов’язки контролера та оператора

1. Враховуючи характер, обсяг, контекст та цілі обробки персональних даних, а також ризики та серйозність наслідків для прав і свобод фізичної особи від обробки персональних даних, контролери та оператори вживати належні технічні та організаційні заходи для забезпечення обробки персональних даних у відповідності до вимог цього Закону та бути спроможними довести це. Заходи, які вживають контролером та оператором у разі необхідності мають оновлюватись з урахуванням технічного розвитку.

2. У разі необхідності з урахуванням характеру обробки персональних даних, заходи, які вживаються з метою виконання обов’язків, передбачених частиною першою цієї статті, можуть включати затвердження контролером кодексу поведінки з питань захисту персональних даних.

3. Технічні та організаційні заходи, які вжиті контролером або оператором для виконання обов’язків, передбачених частиною першою цієї статті, повинні переглядатись та оновлюватись у разі необхідності.

Кожен контролер та оператор, а також їхні представники у разі призначення, зобов’язані співпрацювати з контролюючим органом на його вимогу щодо питань виконання їхніх обов’язків, передбачених цим Законом.

Стаття 29. Захист персональних даних за проектуванням та за замовчуванням

1. Кожен контролер зобов'язаний вжити відповідних і достатніх технічних та організаційних заходів, які забезпечують:

1) належне та ефективне виконання принципів обробки персональних даних, передбачених цим Законом з урахуванням практики Європейського суду з прав людини;

2) дотримання підстав обробки персональних даних, передбачених цим Законом;

3) інтеграцію захисних гарантій в процес обробки персональних даних.

2. Обов'язки, передбачені частиною першою цієї статті, застосовуються як до визначення засобів обробки персональних даних, так й до процесу обробки персональних даних.

3. Кожен контролер зобов'язаний вжити відповідних і достатніх технічних та організаційних заходів для забезпечення того, що обробляються тільки ті персональні дані, які необхідні для точно визначеної легітимної мети обробки.

4. Обов'язки, передбачені частиною третьою цієї статті, застосовуються до :

1) обсягу персональних даних, які збираються;

2) обсягу обробки персональних даних;

3) строку зберігання персональних даних;

4) доступності персональних даних;

5. Заходи, які вживаються для виконання обов'язку, передбаченого частиною третьою цієї статті, повинні забезпечувати, щоб персональні дані за замовчуванням не були доступними невизначеному колу осіб без втручання людини.

6. Суб'єкти владних повноважень зобов'язані погоджувати проєкти нормативно-правових актів, які передбачають обробку персональних даних, з контролюючим органом, у порядку, визначеному законом.

Стаття 30. Спільні контролери

1. Якщо цілі та засоби обробки персональних даних визначаються двома або більше контролерами спільно, вони вважаються спільними контролерами.

2. Спільні контролери зобов'язані визначити їхні обов'язки стосовно дотримання вимог обробки персональних даних в договорі про розподіл обов'язків щодо дотримання вимог обробки персональних даних, крім випадків, коли такі обов'язки передбачені законодавством.

3. У договорі про розподіл обов'язків щодо дотримання вимог обробки персональних даних контролери повинні передбачити, який з контролерів є відповідальним за комунікацію з суб'єктом персональних даних.

Положення договору, що регулюють розподіл обов'язків щодо дотримання вимог обробки персональних даних та впливають на права суб'єктів персональних даних надаються у порядку, встановленому Законом України «Про доступ до публічної інформації».

Суб'єкт персональних даних може здійснювати свої права щодо кожного з контролерів незалежно від умов договору та ознайомитись із змістом цього договору у порядку, встановленому Законом України «Про доступ до публічної інформації».

Стаття 31. Оператор персональних даних

1. Контролер може дозволити обробляти персональні дані від свого імені виключно такому оператору, який забезпечить достатні гарантії вжиття відповідних і достатніх технічних та організаційних заходів для обробки персональних даних у відповідності до вимог цього Закону та захисту прав суб'єкта персональних даних.

2. Оператор не може залучати іншого оператора без попереднього письмового дозволу контролера. У випадку, якщо контролер надав загальний дозвіл на

залучення іншого оператора, оператор до залучення іншого оператора зобов’язаний проінформувати контролера про намір залучити додаткового оператора або заміну оператора з метою надання можливості контролеру заперечити проти цього.

3. Обробка персональних даних оператором повинна здійснюватися на підставі договору або нормативно-правового акта, які повинні передбачати вид та категорії персональних даних, які підлягають обробці, строк, характер та мету обробки, вид та категорії суб’єктів персональних даних, чиї дані підлягають обробці, та права і обов’язки контролера.

Договором або нормативно-правовим актом повинно бути передбачено, що оператор повинен:

1) обробляти персональні дані виключно за наявності письмового доручення контролера, яке включає, зокрема, визначення питання передачі персональних даних іншим державам або міжнародним організаціям, якщо це не передбачено законом. Якщо передача персональних даних іншим державам або міжнародним організаціям передбачена законом, оператор повинен повідомити про це контролера перед здійсненням обробки, крім випадків, коли надання такої інформації заборонено законом;

2) допускати до обробки персональних даних лише тих осіб, на яких поширюється передбачене законодавством зобов'язання щодо збереження конфіденційності інформації, або осіб які дали відповідне письмове зобов'язання;

3) вживати заходів для забезпечення вимог щодо захисту персональних даних, передбачених статтею 35 цього Закону;

4) визначити порядок реалізації вимог, передбачених частиною другою та четвертою цієї статті;

5) надавати допомогу та сприяння у дотриманні контролером обов'язку відповідати на запити суб'єктів персональних даних щодо реалізації їх прав, передбачених Розділом II цього Закону;

6) надавати допомогу та сприяти контролеру у дотриманні ним обов'язків, передбачених статтями 35 та 40 цього Закону, з урахуванням характеру обробки та інформації, доступної для оператора;

7) на вимогу контролера видалити або повернути всі персональні дані контролеру після закінчення строку надання послуг з обробки персональних даних, а також видалити наявні копії персональних даних, крім випадків, якщо обов'язок збереження персональних даних передбачено законом;

8) надавати контролеру всю інформацію, необхідну для підтвердження дотримання вимог, передбачених цією статтею, дозволяти та сприяти проведенню перевірок, які здійснюються контролером або іншою уповноваженою ним особою. Якщо оператор вважає, що виконання вимоги контролера за цим положенням призведе до порушення вимог цього Закону, оператор повинен негайно повідомити про це контролера.

Положення договору між контролером та оператором, на підставі якого здійснюється обробка та впливають на права суб'єктів персональних даних надаються у порядку, встановленому Законом України «Про доступ до публічної інформації».

4. Якщо оператор залучив іншого оператора для здійснення певних процесів з обробки персональних даних від імені контролера, залучений оператор має ті самі обов'язки, які передбачені договором або нормативно-правовим актом, на

підставі якого здійснюється обробка від імені контролера. Такі обов'язки покладаються на залученого оператора договором або нормативно-правовим актом. Якщо залучений оператор не виконує покладених на нього обов'язків з захисту персональних даних, відповідальність за порушення ним зобов'язань перед контролером несе оператор, який здійснив залучення.

5. Примірний договір затверджується контролюючим органом.

6. Оператор, який самостійно визначає цілі та засоби обробки персональних даних, вважається контролером відповідно до цього Закону.

Стаття 32. Обробка персональних даних за дорученням контролера або оператора

1. Оператор або будь-яка особа, яка має доступ до персональних даних та діє за дорученням контролера або оператора, може здійснювати обробку персональних даних виключно відповідно до завдання контролера, крім випадків передбачених законом.

Стаття 33. Представник контролера або оператора

1. Контролер або оператор, який створений та/або діє у інших державах, зобов'язаний призначити свого представника на території України за однієї з таких умов:

1) обробка персональних даних пов'язана з пропонування товарів, робіт або послуг на платній чи безоплатній основі суб'єктам персональних даних, які знаходяться на території України;

2) обробка персональних даних пов'язана з моніторингом поведінки суб'єктів персональних даних під час їхнього перебування на території України;

3) контролер здійснює обробку персональних даних громадян України.

2. Контролер або оператор зобов’язані оприлюднити контактні дані представника з питань захисту персональних даних до початку обробки персональних даних. Інформація про представника повинна бути розміщена на офіційному веб-сайті контролера, оператора державною мовою та повідомлена контролюючому органу.

3. Положення частини першої цієї статті не застосовуються, якщо обробка персональних даних не є систематичною.

4. Представник контролера або оператора повинен бути уповноважений контролером або оператором для комунікації з контролюючим органом та суб’єктами персональних даних, щодо всіх питань, пов’язаних з обробкою персональних даних, а також представляти інтереси в суді та інших установах, а також:

- діє в межах представницьких повноважень, наданих контролером або оператором;

- повідомляє контролера та оператора про всі скарги на обробки персональних даних, які до нього надійшли;

- повідомляє контролера та оператора про запити та/або іншу інформацію, отриману від контролюючого органу;

- представляє контролера або оператора у провадженні, відкритому в зв'язку з порушенням контролером або оператором положень цього Закону.

Стаття 34. Реєстрація операцій з обробки персональних даних

1. Кожен контролер або у разі наявності представник контролера зобов’язаний здійснювати реєстрацію операцій з обробки персональних даних, за яку контролер несе відповідальність. Реєстрація операцій здійснюється шляхом

ведення протоколу. Протокол обробки персональних даних повинен містити інформацію про:

1) назву (ім’я) та контактні дані контролера, у разі наявності, спільного контролера, представника контролера та відповідальної особи з питань захисту персональних даних;

2) мету обробки;

3) опис категорій суб’єктів персональних даних та категорій персональних даних;

4) категорії одержувачів, яким персональні дані були або можуть розкриватись, включаючи одержувачів в інших державах або міжнародні організації;

5) передачу персональних даних іншим державам або міжнародним організаціям, включаючи назву цієї держави або міжнародної організації, а також у разі передачі персональних даних до іншої держави відповідно до частини четвертої статті 48 цього Закону - інформацію про документи, які підтверджують наявність належних захисних гарантій;

6) строк для видалення різних категорій персональних даних у разі, якщо це можливо;

7) загальний опис технічних та організаційних заходів з безпеки, передбачених частиною першою статті 35 цього Закону.

2. Кожен оператор та у разі наявності представник оператора зобов’язаний здійснювати реєстрацію всіх видів операції з обробки, яка здійснюється від імені контролера, шляхом ведення протоколу. Протокол повинен містити інформацію про:

1) назву (ім’я) та контактні дані оператора (операторів), назву кожного контролера, від імені якого здійснюється обробка, у разі наявності представника контролера або оператора та відповідальної особи з питань захисту персональних даних;

2) категорії дій з обробки персональних даних, які здійснюються від імені кожного контролера;

3) передачу персональних даних іншим державам або міжнародним організаціям, включаючи назву цієї держави або міжнародної організації, а також у разі передачі персональних даних до іншої держави відповідно до частини четвертої статті 48 цього Закону - інформацію про документи, які підтверджують наявність належних захисних гарантій;

4) загальний опис технічних та організаційних заходів з безпеки, передбачених статтею 35 цього Закону.

3. Контролер або оператор, а також представник контролера або оператора у разі призначення, зобов’язані надавати протоколи обробки персональних даних контролюючому органу у відповідь на запит.

4. Положення частини першої та другої цієї статті не застосовуються до суб'єктів мікропідприємництва, підприємств, організацій і установ незалежно від форми власності та організаційно-правової форми з чисельністю працівників менше ніж 10 осіб, крім випадків, коли:

1) обробка персональних даних може становити ризик порушення прав і свобод суб’єкта персональних даних;

2) обробка персональних даних є систематичною;

3) здійснюється обробка персональних даних, передбачена частиною першою статті 7 та статтею 8 цього Закону.

Стаття 35. Безпека обробки персональних даних

1. Контролер та оператор зобов’язані вживати належні заходи технічного та організаційного характеру для забезпечення належної безпеки обробки персональних даних такого рівня, який є співмірний ризику обробки персональних даних для прав і свобод суб’єктів персональних даних із дотриманням принципу пропорційності. Заходи з забезпечення безпеки можуть включати:

1) псевдонімізацію та шифрування персональних даних;

2) безперервне забезпечення конфіденційності, цілісності, доступності персональних даних і стійкості систем і сервісів обробки;

3) забезпечення своєчасного відновлення доступу до персональних даних у разі виникнення аварійної ситуації або інциденту;

4) регулярне тестування, оцінка та вимірювання ефективності технічних та організаційних заходів щодо забезпечення безпеки обробки;

5) забезпечення дотримання кодексу обробки персональних даних працівниками контролера та оператора.

2. При оцінці належності рівня безпеки обробки персональних даних враховуються ризики обробки персональних даних щодо випадкового або неправомірного знищення, втрати, зміни, несанкціонованого розкриття або доступу до персональних даних, переданих, збережених або іншим чином підданих обробці.

3. Контролер зобов’язаний здійснити оцінку ризиків обробки персональних даних та належність заходів, які повинні бути вжиті для безпеки обробки персональних даних, до початку обробки, а також здійснювати нову оцінку під час обробки в розумні строки.

4. Контролер та оператор зобов’язані вживати заходи для забезпечення обробки персональних даних будь-якою фізичною особою, яка діє за дорученням контролера або оператора та має доступ до персональних даних, виключно у межах наданого контролером доручення, якщо інше не вимагається законом.

Стаття 36. Співпраця контролера та оператора з контролюючим органом

1. Контролер та оператор, а також їхній представник у разі призначення, до яких звернувся контролюючий орган, зобов’язані:

1) забезпечувати доступ до приміщень, засобів, інформаційно телекомунікаційних систем, матеріалів і документів, у тому числі на засадах, визначених законодавчими актами щодо захисту інформації з обмеженим доступом;

2) надавати інформацію і давати пояснення стосовно фактичної і правової підстави своїх дій та рішень, пов’язаних з обробкою персональних даних;

3) виконувати інші законні вимоги контролюючого органу.

Стаття 37. Повідомлення контролюючого органу про витік персональних даних

1. Контролер не пізніше семидесяти двох годин з моменту, коли йому стало відомо про витік, зобов’язаний повідомити про нього контролюючий орган крім випадків, якщо витік малоймовірно може призвести до ризику для прав та свобод фізичної особи.

2. У разі неможливості здійснити повідомлення про витік у строк, передбачений частиною першою цієї статті, контролер зобов'язаний повідомити про нього контролюючий орган без невиправданої затримки з моменту, коли йому стало відомо про витік, з обґрунтуванням причин недотримання строку, передбаченого частиною першою цієї статті.

3. Оператор зобов'язаний повідомити контролера про витік без невиправданої затримки з моменту, коли йому стало про нього відомо.

4. Повідомлення про витік повинно, зокрема, включати:

1) опис характеру витоку, включаючи категорії та кількість суб'єктів персональних даних, яких стосується витік, а також категорії та кількість реєстраційний записів персональних даних, яких стосується витік;

2) контактні дані відповідальної особи з питань захисту персональних даних або іншої особи, яка може надати додаткову інформацію;

3) опис ймовірних наслідків витоку;

4) опис заходів, які було вжито або які плануються контролером для зменшення наслідків витоку.

5. Підготовка повідомлення не є обставиною, що виправдовує недотримання строку, передбаченого частиною першою цієї статті.

6. Інформація, передбачена в частині четвертій цієї статті, має бути надана одночасно. У разі неможливості надання інформації, передбаченої частиною четвертою цією статті, одночасно, контролер зобов'язаний її надати частинами без невиправданої затримки.

7. Контролер зобов'язаний документувати будь-які випадки витоків, включаючи факти, пов'язані з ними, їх наслідками та заходами, вжитими для їх усунення.

Стаття 38. Повідомлення суб’єкта персональних даних про витік

1. Контролер зобов’язаний повідомити про витік суб’єкта персональних даних без невиправданої затримки у випадку, якщо існує ймовірність високого ступеню ризику для прав та свобод фізичної особи.

2. Повідомлення суб’єкта персональних даних про витік повинно містити опис характеру витоку та інформацію, передбачену частиною четвертою статті 37 цього Закону.

3. Контролер не зобов’язаний повідомити про витік суб’єкта персональних даних у разі дотримання однієї із наступних умов:

1) контролер вжив відповідних і достатніх технічних та організаційних заходів захисту і такі заходи були застосовані до персональних даних, яких стосувався витік, зокрема, щодо усунення можливості порушення прав суб'єктів персональних даних.

2) контролер вжив заходи для запобігання настання ризиків високого ступеню для прав та свобод суб’єкта персональних даних;

3) повідомлення становить надмірний тягар для контролера.

4. У разі якщо повідомлення суб’єкта персональних даних становить надмірний тягар для контролера, він зобов’язаний вжити інші заходи для інформування суб’єкта персональних даних про витік, наприклад, здійснити повідомлення з використанням засобів масової інформації, соціальних мереж та офіційних веб-сайтів.

5. У разі якщо контролер не повідомив суб’єкта персональних даних про витік, контролюючий орган може:

1) зобов’язати контролера здійснити таке повідомлення у випадку, якщо він дійде висновку про ймовірність настання ризиків високого ступеня для прав і свобод суб’єкта персональних даних;

2) прийняти рішення про дотримання умов, передбачених частиною третьою цієї статті.

6. Інформація, вказана в цій статті, надається суб’єктам персональних даних у доступний спосіб та зрозумілою мовою, які забезпечують її ясність та зрозумілість для відповідних суб’єктів персональних даних.

Стаття 39. Оцінка впливу обробки персональних даних

1. Контролер зобов’язаний здійснити оцінку впливу обробки персональних даних на захист персональних даних до початку такої обробки, якщо використання нових технологій або характер, обсяг, контекст та цілі обробки ймовірно призведуть до настання ризику високого рівня для прав та свобод фізичної особи.

2. Контролер зобов’язаний залучити відповідальну особу з питань захисту персональних даних, у разі його призначення, до здійснення оцінки впливу, передбаченої частиною першою цієї статті.

3. Оцінка впливу, передбачена частиною першою цієї статті, проводиться у разі здійснення:

1) систематичного та широкомасштабного аналізу особистісних аспектів життя фізичних осіб, який здійснюється автоматизованими засобами обробки, включаючи профілювання, та на результатах якого ґрунтуються рішення, що мають юридичні наслідки для фізичної особи або у інший подібний спосіб впливають на неї;

2) широкомасштабної обробки персональних даних, передбачених статтями 7 та 8 цього Закону;

3) систематичного і широкомасштабного моніторингу загальнодоступних місць або джерел.

4. Перелік видів обробки, при застосуванні яких контролер зобов'язаний здійснити оцінку впливу, передбачену частиною першою цієї статті, затверджується контролюючим органом.

5. За результатами оцінки впливу контролер складає висновок у письмовій формі, який повинен містити, зокрема:

1) детальний опис запланованої обробки персональних даних та її цілей;

2) інформацію про оцінку необхідності та пропорційності обробки персональних стосовно цілей;

3) інформацію про оцінку ризиків для прав та свобод суб'єктів персональних даних;

4) інформацію про заходи, які передбачені для реагування на ризики, включаючи гарантії, заходи безпеки та механізми для забезпечення захисту персональних даних та демонстрації дотримання вимог цього Закону.

6. Частина перша та п'ята цієї статті не застосовується у разі, якщо обробка персональних даних здійснюється на підставі пунктів 3 і 5 статті 5 цього Закону і випадки такої обробки передбачені законом, процес прийняття якого включав оцінку впливу обробки на захист персональних даних.

7. Контролер зобов'язаний з розумною періодичністю, але не рідше одного разу на три роки, здійснювати перегляд оцінки впливу, якщо обробка здійснюється

відповідно до попередньої оцінки впливу, та у разі зміни ризиків відповідної обробки.

8. Контролер зобов'язаний врахувати результат оцінки впливу обробки персональних даних при визначенні відповідних і достатніх заходів, які мають вживатись для дотримання цього Закону. Контролер зобов'язаний до обробки персональних даних провести консультації з контролюючим органом у разі, якщо результати оцінки впливу свідчать, що обробка персональних даних містить ризик високого ступеню, який не може бути усунено заходами контролера з огляду на наявні технології та витрати на їх впровадження. Контролер зобов'язаний до обробки персональних даних провести консультації з контролюючим органом відповідно до статті 40 цього Закону.

Стаття 40. Попередні консультації

1. У разі якщо оцінка впливу, здійснена відповідно до статті 39 цього Закону, свідчить, що обробка персональних даних ймовірно може призвести до настання високого ступеню ризиків за відсутності вжиття заходів для їх усунення, контролер зобов'язаний провести попередню консультацію з контролюючим органом до початку обробки персональних даних.

Суб'єкти владних повноважень та правоохоронні органи зобов'язані провести попередні консультації з контролюючим органом щодо заходів, які становлять широкомасштабну обробку персональних даних, до їх вжиття.

2. У разі якщо контролюючий орган у результаті попередньої консультації з контролером, передбаченої частиною першою цієї статті, дійде висновку про те, що обробка, щодо якої проводяться попередні консультації, становитиме порушення вимог цього Закону, контролюючий орган ухвалює рішення про

надання рекомендацій з метою усунення порушень цього Закону при обробці персональних даних контролером.

3. Контролюючий орган надає рекомендації контролеру в строк до 45 днів з моменту отримання запиту контролера. У разі якщо обробка персональних даних, щодо якої здійснюються консультації, є складною, контролюючий орган може продовжити строк надання рекомендацій або прийняття іншого рішення до 65 днів з моменту отримання запиту на консультацію. Рішення про продовження ухвалюється в письмовій формі та повинно містити належне обгрунтування. Рішення про продовження строку надання рекомендації або прийняття іншого рішення в результаті консультацій повідомляється контролеру у п’ятиденний строк з моменту прийняття.

4. При здійсненні консультацій контролер зобов’язаний надати інформацію про:

1) обов’язки контролера, спільних контролерів та операторів, залучених до обробки персональних даних (за наявності);

2) цілі та засоби обробки персональних даних, яка планується;

3) заходи та гарантії захисту, які передбачені для захисту прав і свобод суб’єктів персональних даних відповідно до цього Закону;

4) контактні дані відповідальної особи з захисту персональних даних (у разі її призначення);

5) оцінку впливу обробки персональних даних на захист персональних даних, передбачену статтею 39 цього Закону;

6) будь-яку іншу інформацію, яку запитує контролюючий орган.

5. Суб’єкти владних повноважень зобов’язані провести попередні консультації з контролюючим органом щодо заходів, які становлять широкомасштабну обробку персональних даних, до їх вжиття.

Стаття 41. Відповідальна особа з питань захисту персональних даних

1. З метою організації та здійснення заходів для виконання вимог цього Закону, контролер та оператор зобов’язані призначити відповідальну особу з питань захисту персональних даних у одному із таких випадків:

1) обробка персональних даних здійснюється суб’єктом владних повноважень;

2) основна діяльність контролера або оператора полягає у обробці персональних даних, яка за своїм характером, обсягом та/або її цілі, вимагає регулярного та систематичного та широкомасштабного моніторингу дій або бездіяльності суб’єктів персональних даних;

3) основна діяльність контролера або оператора полягає або пов’язана з широкомасштабною обробкою персональних даних;

4) основна діяльність контролера або оператора полягає або пов’язана з обробкою персональних даних, визначених статтями 7-10.

2. Спільні контролери або група операторів за взаємною згодою можуть визначити одну відповідальну особу з питань захисту персональних даних за умови наявності вільного доступу до неї кожного з них.

3. Суб’єкт владних повноважень може призначити одну відповідальну особу з питань захисту персональних даних для виконання повноважень в його територіальних органах.

4. Відповідальна особа з питань захисту персональних даних повинна:

1) надавати інформацію та рекомендації контролеру або оператору та працівникам, які безпосередньо залучені до обробки персональних даних, про їх обов'язки відповідно до цього Закону;

2) здійснювати моніторинг дотримання вимог цього Закону, включаючи розподіл обов'язків, підвищувати рівень обізнаності працівників контролера або оператора з питань захисту персональних даних, які безпосередньо залучені до обробки персональних даних;

3) надавати рекомендації щодо оцінки впливу на захист персональних даних та здійснювати моніторинг її виконання;

4) співпрацювати з контролюючим органом;

5) бути контактною особою для контролюючого органу з питань, пов'язаних з обробкою персональних даних, включаючи попередні консультації та інші питання щодо виконання вимог цього Закону.

5. Контролер та оператор повинні забезпечити залучення відповідальної особи з питань захисту персональних даних вчасно та у належний спосіб до вирішення всіх питань, пов'язаних з обробкою та захистом персональних даних.

6. Відповідальною особою з питань захисту персональних даних може бути призначена особа, яка має ступінь вищої освіти не нижче бакалаврського та досвід роботи у сфері захисту персональних даних.

7. Не може бути відповідальною особою з питань захисту персональних даних особа, яка:

1) має судимість за вчинення тяжкого або особливо тяжкого злочину;

2) обмежена у дієздатності або визнана недієздатною за рішенням суду;

3) не склала кваліфікаційний іспит - для суб’єктів владних повноважень та контролерів та операторів, які здійснюють широкомасштабну обробку персональних даних.

8. Керівник контролера або оператора забезпечує незалежність відповідальної особи з питань захисту персональних даних від впливу чи втручання у його роботу. Відповідальна особа з питань захисту персональних даних підзвітна і підконтрольна керівнику контролера та оператора.

9. Відповідальну особу з питань захисту персональних даних не може бути звільнено чи примушено до звільнення, притягнуто до дисциплінарної відповідальності чи піддано з боку контролера та оператора іншим негативним заходам впливу (переведення, атестація, зміна умов праці, зменшення заробітної плати тощо) або загрозі таких заходів впливу у зв’язку з належним виконанням ним завдань, передбачених цим Законом.

10. Контролер або оператор зобов’язані оприлюднити контактні дані відповідальної особи з питань захисту персональних даних та повідомити їх контролюючому органу.

11.Відповідальна особа з питань захисту персональних даних може виконувати інші завдання та обов’язки. Контролер чи оператор забезпечує, що будь-які інші завдання та обов’язки не становлять конфлікт інтересів.

Конфліктом інтересів для цілей цієї статті вважається суміщення завдань і обов’язків відповідальної особи з іншими посадовими та/або службовими обов’язками, які включають прийняття рішення про обробку персональних даних, представлення інтересів контролера чи оператора в судових або арбітражних провадженнях, що стосуються питань захисту персональних даних.

Стаття 42. Кваліфікаційний іспит на посаду відповідальної особи з питань захисту персональних даних

1. Суб'єкт владних повноважень може призначити особу на посаду відповідальної особи з питань захисту персональних даних, якщо така особа успішно пройшла кваліфікаційний іспит і отримала сертифікат.

2.Кваліфікаційний іспит полягає у виявленні належних теоретичних знань та рівня професійної підготовки особи для зайняття посади відповідальної особи з питань захисту персональних даних.

3. Кваліфікаційний іспит проводиться шляхом складення кандидатом на посаду відповідальної особи з питань захисту персональних даних письмового анонімного тестування та виконання анонімного письмового практичного завдання з метою виявлення рівня знань, практичних навичок та умінь у застосуванні законодавства з питань захисту персональних даних.

Результати кваліфікаційного іспиту дійсні протягом трьох років з дня складення іспиту.

4. Контролюючий орган затверджує рекомендації щодо порядку складення кваліфікаційного іспиту, змісту тестових питань та практичних завдань, методику оцінювання результатів для розробки програм навчання, підвищення кваліфікації та робочих і навчальних, сертифікатних програм для закладів освіти.

Стаття 43. Кодекс поведінки з питань захисту персональних даних

1. Кодекс поведінки з питань захисту персональних даних є комплексом правил, стандартів і процедур, які забезпечують дотримання вимог цього Закону для певної галузі, сектору, об'єднань підприємств, установ, саморегулівних організацій.

2. Об’єднання підприємств, асоціації, громадські об’єднання чи саморегулівні організації затверджують Кодекс поведінки з питань захисту персональних даних для певної галузі, сектору, об’єднань підприємств, установ, членів саморегулівних організацій, у випадках, якщо:

1) основна діяльність контролерів або операторів, які належать до певної галузі, сектору, об’єднань підприємств, установ, саморегулівних організацій, полягає у обробці персональних даних, яка за своїм характером, обсягом та/або її цілі, вимагає регулярного та систематичного широкомасштабного моніторингу суб’єктів персональних даних; або

2) основна діяльність контролерів або операторів, які належать до певної галузі, сектору, об’єднань підприємств, установ, саморегулівних організацій, полягає у широкомасштабній обробці персональних даних.

3. Кодекс поведінки з питань захисту персональних даних має містити, зокрема, інформацію про:

1) сферу застосування та коло осіб, на яких поширюються його дія;

2) добросовісну та прозору обробку персональних даних;

3) легітимні інтереси, які переслідуються контролером;

4) порядок та підстави збору персональних даних;

5) псевдонімізацію персональних даних;

6) відомості, які мають оприлюднюватись та надаватись суб’єктам персональних даних;

7) порядок реалізації прав суб’єкта персональних даних;

8) порядок захисту дітей як суб’єктів персональних даних та надання їм інформації, а також спосіб відібрання згоди на обробку персональних даних малолітніх дітей у їхніх представників;

9) заходи, які вживаються на виконання обов’язків контролера та/або оператора для забезпечення захисту персональних даних за проектуванням і за замовчуванням, а також заходів для забезпечення безпеки обробки персональних даних;

10) порядок повідомлення про витік персональних даних контролюючому органу та суб’єктам персональних даних;

11) передачу персональних даних до інших держав або міжнародних організацій;

12) позасудовий порядок вирішення спорів між контролером та суб’єктами персональних даних щодо обробки персональних даних;

13) порядок здійснення взаємодії з контролюючим органом, в тому числі щодо моніторингу дотримання контролером або оператором вимог цього Закону.

РОЗДІЛ VI

ПЕРЕДАЧА ПЕРСОНАЛЬНИХ ДАНИХ НА ТЕРИТОРІЮ ІНОЗЕМНИХ ДЕРЖАВ АБО МІЖНАРОДНИМ ОРГАНІЗАЦІЯМ

Стаття 44. Підстави для передачі персональних даних на територію іноземної держави або міжнародній організації

1. Передача персональних даних іноземним державам та/або міжнародним організаціям може бути здійснена контролером у випадках, якщо:

1) іноземна держава або міжнародна організація забезпечує належний рівень захисту персональних даних;

2) контролер та/або оператор надав належні гарантії захисту персональних даних;

3) затверджені обов’язкові корпоративні правила у відповідності до вимог цього Закону.

2. Персональні дані можуть бути передані іноземній державі або міжнародній організації також у випадках передбачених цим Законом.

Стаття 45. Передача персональних даних на територію іноземної держави та міжнародній організації, які забезпечують належний рівень захисту персональних даних

1. Держави та організації, на які поширюється дія Загального регламенту Європейського союзу про захист персональних даних та/або Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних із змінами, внесеними Комітетом Міністрів Ради Європи у 2018 році, вважаються такими, що забезпечують належний рівень захисту персональних даних, за винятком випадків передбачених частиною сьомою цієї статті.

2. Перелік держав та/або організацій і осіб, на які не поширюється дія Загального регламенту Європейського союзу про захист персональних даних та/або Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних із змінами, внесеними Комітетом Міністрів Ради Європи у 2018 році, та які забезпечують належний захист персональних даних, встановлюється контролюючим органом.

3. При встановленні відповідності рівня захисту іноземної держави та/або організації контролюючий орган, зокрема, враховує:

1) стан дотримання прав людини та основоположних свобод; відповідне законодавство, включаючи сфери громадського порядку, національної безпеки, кримінального права; правила доступу державних органів до персональних даних; стан дотримання відповідного законодавства; законодавство або правила щодо подальшої передачі персональних даних іноземною державою або міжнародною організацією іншим державам або організаціям; ефективність та дотримання прав суб'єкта персональних даних; наявність адміністративних або судових засобів захисту для суб'єкта персональних даних, чиї дані передаються;

2) наявність та ефективність діяльності контролюючого органу з питань захисту персональних даних в державі, до якої передаються персональні дані, або повноваження якого поширюються на міжнародну організацію, яка є одержувачем персональних даних, з повноваженнями забезпечення дотримання вимог захисту персональних даних та надання допомоги суб'єкту персональних даних при реалізації його прав, а також повноваженнями щодо співпраці з контролюючим органом України;

3) міжнародні зобов'язання іноземної держави або міжнародної організації або інші зобов'язання, які випливають з обов'язкових для них міжнародних актах або інших договорах, в сфері захисту персональних даних.

4. Передача персональних даних з чи до держав та/або міжнародних організацій, які забезпечують належний рівень захисту персональних даних, не потребує окремого дозволу контролюючого органу.

5. Перелік держав та/або організацій і осіб, передбачений частиною третьою цієї статті, оприлюднюється контролюючим органом на його вебсайті.

6. У разі якщо контролюючий орган визнає, що іноземна держава або міжнародна організація не забезпечує належний рівень захисту персональних даних, передача персональних даних до них забороняється, крім випадків, передбачених статтями 46-49 цього Закону.

7. Перелік держав та міжнародних організації, які не забезпечують належний рівень захисту персональних даних, ведеться та оприлюднюється на вебсайті контролюючим органом.

Стаття 46. Передача персональних даних на територію іноземної держави або міжнародній організації на підставі наданих гарантій захисту персональних даних

1. У разі якщо іноземна держава або міжнародна організація не визнана такою, що забезпечує належний рівень захисту персональних даних відповідно до статті 45 цього Закону, контролер або оператор може передати персональні дані іноземній державі або міжнародній організації, якщо контролер або оператор надали належні гарантії захисту та за умови наявності прав та ефективних юридичних засобів захисту суб'єкта персональних даних

2. Належні гарантії захисту, передбачені частиною першою, без дозволу контролюючого органу можуть надаватись на підставі:

1) юридичних актів обов'язкового характеру, які регулюють відносини між суб'єктами владних повноважень;

2) обов'язкових корпоративних правил;

3) стандартизованих умов захисту персональних даних, затверджених контролюючим органом;

4) затвердженого кодексу поведінки з питань захисту персональних даних у поєднанні із зобов'язаннями контролера або оператора іноземної держави застосувати належні гарантії захисту, включаючи гарантії щодо прав суб'єкта персональних даних;

5) затвердженого порядку сертифікації у поєднанні із зобов'язаннями контролера або оператора іноземної держави застосувати належні гарантії захисту, включаючи гарантії щодо прав суб'єкта персональних даних.

3. Належні гарантії захисту, передбачені частиною першою цієї статті, з дозволу контролюючого органу можуть надаватись на підставі:

1) договірних положень між контролером або оператором та контролером, оператором або одержувачем персональних даних іноземної держави або міжнародної організації; або

2) положень угод про співпрацю, укладених між суб'єктами публічного права, які включають права суб'єкта персональних даних.

Стаття 47. Передача персональних даних на територію іноземної держави на підставі обов'язкових корпоративних правил

1. Об'єднання підприємств або окреме підприємство з об'єднання, залучені до спільної економічної діяльності , можуть здійснювати передачу персональних даних на територію іншої держави в межах їх групи на підставі корпоративних правил, затверджених в порядку, передбаченому цим Законом.

Група підприємств або окреме підприємство з групи, що здійснює спільну господарську діяльність, можуть передавати персональні дані на територію іншої держави в межах їхньої групи на підставі корпоративних правил, затверджених в порядку, передбаченому цим Законом.

2. Контролюючий орган зобов’язаний затвердити обов’язкові корпоративні правила за умови, що вони:

1) є обов’язковими, застосовуються і виконуються кожним членом групи підприємств або підприємств, залучених до спільної господарської діяльності, включаючи їхніх працівників;

2) чітко надають суб’єктам персональних даних права стосовно обробки персональних даних; та

3) відповідають вимогам, передбаченим частиною третьою цієї статті.

3. Обов’язкові корпоративні правила, передбачені частиною першою цієї статті, повинні передбачати:

1) структуру та контактні дані груп підприємств, передбачених частиною першої цієї статті, та кожного їхнього члена;

2) передачу персональних даних або сукупність операцій з передачі персональних даних, включаючи категорії персональних даних, види обробки персональних даних та їх цілі, види суб’єктів персональних даних, яких стосується передача персональних даних, інформацію про державу або держави, до яких передаються персональні дані;

3) обов’язкову юридичну силу правил;

4) застосування загальних принципів захисту персональних даних, зокрема, принцип обмеження мети, мінімізації персональних даних, обмеження строку зберігання персональних даних, точності персональних даних, захисту даних за проектуванням та за замовчуванням, законності обробки персональних даних, особливих вимог обробки персональних даних;

5) заходи забезпечення безпеки персональних даних та вимоги щодо подальшої передачі особам, на яких не поширюється дія корпоративних правил;

6) права суб'єктів персональних даних щодо обробки та засобів їх реалізації, включаючи право не бути суб'єктом рішення, прийнятого виключно в результаті автоматизованої обробки персональних даних, включаючи профілювання, право на подання скарги до контролюючого органу та суду, а також право на отримання відшкодування та/або компенсації за порушення обов'язкових корпоративних правил;

7) прийняття контролером або оператором, який знаходиться на території України, відповідальності за будь-які порушення обов'язкових корпоративних правил будь-яким членом групи, який знаходиться за межами України та з вини якого мала місце подія, яка призвела до настання шкоди;

8) спосіб, у який обов'язкові корпоративні правила надаються суб'єктам персональних даних;

9) завдання відповідальної особи з питань захисту персональних даних, призначеної відповідно до статті 41 цього Закону, або будь-якої особи чи організації, відповідальної за моніторинг дотримання обов'язкових корпоративних правил групою підприємств, передбачених частиною першою цієї статті;

10) порядок оскарження дій або бездіяльності;

11) порядок перевірки дотримання обов'язкових корпоративних правил в межах груп підприємств, передбачених частиною першою цієї статті. Така перевірка повинна включати аудит захисту персональних даних та методологію вжиття заходів з виправлення недоліків для захисту прав суб'єкта персональних даних. Результати такої перевірки повинні надаватись особі, призначеної відповідно до

пунктів 9 частини третьої цієї статті, та наглядовій раді групи підприємств, а також контролюючому органу за його вимогою;

12) порядок повідомлення та реєстрації змін корпоративних правил, а також порядок повідомлення контролюючого органу про зміни;

13) порядок співпраці з контролюючим органом для забезпечення дотримання кожним членом групи підприємств, зокрема, шляхом повідомлення контролюючому органу результатів перевірки заходів, передбачених пунктом 11 частини третьої цієї статті;

14) порядок повідомлення контролюючого органу про будь-які юридичні зобов'язання в іноземній державі, дія яких поширюється на групу підприємств та які можуть мати суттєвий негативний вплив на гарантії обов'язкових корпоративних правил;

15) обов'язкові навчальні заходи з питань захисту персональних даних для працівників групи підприємств, які мають постійний або систематичний доступ до персональних даних.

Стаття 48. Окремі випадки передачі персональних даних на територію іноземної держави або міжнародній організації

1. У разі якщо іноземна держава або міжнародна організація не забезпечує належний рівень захисту персональних даних відповідно до статті 45 цього Закону або не надає належні гарантії захисту персональних даних відповідно до статті 46 цього Закону, а також відсутні обов'язкові корпоративні правила відповідно до статті 47 цього Закону, передача даних до іноземної держави або міжнародної організації можлива у одному із таких випадків:

1) суб’єкт персональних даних надав явну згоду на таку передачу персональних даних після отримання інформації про ризики, які виникають в зв’язку з відсутністю відповідних гарантій захисту;

2) передача персональних даних є необхідною для виконання правочину між суб’єктом персональних даних та контролером або для виконання заходів з метою укладення правочину на вимогу суб’єкта персональних даних;

3) передача персональних даних є необхідною для укладення та виконання правочину, укладеного контролером та фізичною або юридичною особою в інтересах суб’єкта персональних даних;

4) якщо передача персональних даних є необхідною в суспільних інтересах, які визнаються законодавством України та які переважають інтереси суб’єкта персональних даних;

5) передача є необхідною для подання, обґрунтування або захисту юридичної вимоги;

6) передача є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних або іншої фізичної особи у разі, якщо суб'єкт персональних даних фізично неспроможний надати згоду або є недієздатним;

7) передача здійснена з реєстру, метою ведення якого є надання суспільству інформації та який є доступним для ознайомлення для кожної особи або для зацікавленої особи, яка може довести легітимний інтерес в отриманні відповідної інформації, - у разі дотримання вимог законодавства щодо ознайомлення з інформацією з такого реєстру;

8) якщо передача є необхідною для реалізації права на свободу вираження поглядів і є пропорційним заходом за конкретних обставин.

2. Передача даних відповідно до пункту 7 частини першої цієї статті не може включати весь обсяг персональних даних, який міститься в реєстрі. Якщо реєстр надає можливість ознайомитись із інформацією особам, які мають легітимний інтерес, передача персональних даних може здійснюватися виключно на запит таких осіб або якщо вони є одержувачами.

3. Забороняється передача персональних даних іноземній державі або міжнародній організації суб'єктом владних повноважень на підставі пунктів 1, 2 та 3 частини першої цієї статті, а також на підставі частини четвертої цієї статті.

4. Якщо передача персональних даних не може бути здійснена на підставі статей 45, 46, 47 цього Закону, а також частини першої цієї статті, контролер або оператор може здійснити передачу персональних даних до іноземної держави або міжнародної організації виключно у разі, якщо така передача є одноразовою, стосується обмеженої кількості суб'єктів персональних даних, є необхідною в легітимних інтересах контролера, які переважають інтереси, права і свободи суб'єкта персональних даних, та якщо контролер здійснив оцінку всіх обставин передачі персональних даних та на підставі результатів такої оцінки забезпечив належні гарантії захисту персональних даних. Якщо передача персональних даних відбулась на підставі положень цієї частини, контролер зобов'язаний:

1) повідомити про неї контролюючий орган;

2) повідомити про неї суб'єкта персональних даних, а також про переважаючий легітимний інтерес, який переслідується такою передачею, на додаток до інформації, яка має надаватись контролером відповідно до статті 18 цього Закону.

5. Контролер або оператор повинні документувати оцінку та належні гарантії захисту, передбачені частиною четвертою цієї статті, в протоколі реєстрації операцій з обробки персональних даних відповідно до статті 34 цього Закону.

Стаття 49. Передача персональних даних на територію іншої держави в правоохоронних цілях

1. Персональні дані можуть передаватись правоохоронними органами України в правоохоронних цілях до правоохоронних органів іноземної держави у разі, якщо іноземна держава забезпечує належний рівень захисту персональних даних відповідно до статті 45 цього Закону.

2. У разі якщо іноземна держава, до якої передаються персональні дані, не забезпечує належний рівень захисту персональних даних, персональні дані можуть бути передані правоохоронним органом України до правоохоронного органу іноземної держави в правоохоронних цілях на підставі відповідного міжнародного договору (міжнародної угоди), який забезпечує належний рівень захисту персональних даних.

РОЗДІЛ VII

ПОРЯДОК ДОСТУПУ ДО ПЕРСОНАЛЬНИХ ДАНИХ ТРЕТІХ ОСІБ

Стаття 50. Порядок доступу третіх осіб до персональних даних

1. Порядок доступу третіх осіб до персональних даних, які перебувають у володінні розпорядника публічної інформації, регулюється Законом України «Про доступ до публічної інформації».

2. Для отримання персональних даних, крім випадків встановлених частиною першою цієї статті, третя особа звертається до контролера із запитом, який має містити:

1) відомості про запитувача, достатні для ідентифікації його особи, якщо запитувачем є фізична особа;

2) найменування, місцезнаходження юридичної особи, яка звертається із запитом, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит, якщо запитувачем є юридична особа;

3) відомості, що дають змогу ідентифікувати фізичну особу, персональні дані якої запитуються;

4) перелік персональних даних, які запитуються;

5) мета та юридичні підстави для отримання персональних даних та обґрунтування їх застосовності в конкретному індивідуальному випадку;

6) зобов’язання використовувати отримані персональні дані виключно з легітимною метою, з якою вони були зібрані;

7) власноручний або електронний підпис запитувача.

3. Запит подається в письмовій формі.

4. Контролер зобов’язаний розглянути запит, передбачений частиною другою цієї статті, протягом 30 днів з дня його отримання та надати персональні дані або надати обґрунтовану відмову з урахуванням вимог цього Закону.

5. Контролер відмовляє у наданні персональних даних у разі, якщо:

1) запит не містить інформації, передбаченої частиною другою цієї статті;

2) надання персональних даних є неправомірним відповідно до цього Закону.

6. У разі якщо задоволення запиту передбачає виготовлення копій документів обсягом більш як 10 (десять) сторінок, запитувач зобов'язаний відшкодувати фактичні витрати на копіювання та друк.

7. Розмір фактичних витрат на копіювання та друк визначається відповідним контролером в межах граничних норм, встановлених контролюючим органом. У разі якщо контролер не встановив розміру плати за копіювання або друк, інформація надається безкоштовно.

РОЗДІЛ VIII

ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ РОБОТОДАВЦЕМ

Стаття 51 Загальні питання обробки персональних даних роботодавцем

1. Обробка роботодавцем персональних даних здійснюється у відповідності до вимог цього Закону з урахуванням особливостей, передбачених цим розділом.

2. Положення цього Розділу застосовуються до відносин між роботодавцем та кандидатом на працевлаштування, працівником, державним службовцем та іншими особами, перелік яких передбачено частиною третьою статті 3 Закону України «Про державну службу».

3. Для цілей цього Закону під цілями трудових відносин розуміються відносини між роботодавцем та працівником та/або кандидатом на працевлаштування, які стосуються працевлаштування, виконання трудового договору, включаючи виконання обов’язків, передбачених законодавством, установчими документами, колективним договором, а також планування та ефективне управління органом державної влади та органом місцевого самоврядування, підприємством, установою або організацією та розірвання трудових відносин. До цілей трудових відносин також належать відносини, які мають місце після припинення трудових відносин.

4. Роботодавець зобов’язаний обробляти лише ті персональні дані суб’єктів персональних даних, передбачених частиною другою цієї статті, які необхідні для реалізації трудових правовідносин, що пов’язані з:

1) виконанням обов'язків та реалізацією прав сторін трудових правовідносин;

2) наданням роботодавцем додаткових благ, заохочень;

3) особливим характером виконуваної роботи.

5. Роботодавець може обробляти персональні дані в цілях, які не передбачені частиною четвертою цієї статті, на підставі згоди суб’єкта персональних даних, якщо така згода є добровільною та її ненадання або відкликання не призводить до негативних наслідків для суб’єкта персональних даних

6. Під час обробки персональних даних для цілей трудових правовідносин роботодавець повинен вжити відповідні і достатні заходи для забезпечення дотримання принципів захисту персональних даних та для належного виконання обов’язків в якості контролера, що передбачені цим Законом. Такі заходи повинні відповідати обсягу та характеру персональних даних, що обробляються, характеру здійснюваної роботи, а також мають враховувати можливий вплив на основоположні права та обов’язки суб’єктів, передбачених частиною другою цієї статті.

7. Роботодавець зобов’язаний на вимогу контролюючого органу довести дотримання ним принципів захисту персональних даних та його обов’язків в якості контролера, передбачених цим Законом.

Стаття 52. Обробка персональних даних роботодавцем

1. Роботодавець зобов’язаний збирати персональні дані осіб, передбачених частиною другою статті 51, безпосередньо від таких осіб, крім випадків, передбачених трудовим договором та/або законодавством.

2. Роботодавець може збирати персональні дані осіб, передбачених частиною другою статті 51, від інших осіб (джерел) на підставі згоди. Згода осіб, передбачених частиною другою статті 51, не вимагається, якщо персональні дані збираються роботодавцем від органу державної влади для виконання ним своїх обов’язків, передбачених законодавством, або якщо збір персональних даних передбачено законом.

3. Зберігання персональних даних в цілях трудових правовідносин дозволяється виключно з дотриманням принципів, передбачених цим Законом, та протягом строку, необхідного для досягнення легітимної мети, яка переслідується. Такі персональні дані повинні бути відповідними, належними та не надмірними відносно легітимної мети, що переслідується.

4. Дані про оцінку відповідності професійних компетентностей особи, можуть зберігатись роботодавцем виключно з метою оцінки її професійно-ділових якостей або відповідності компетентностей вимогам умов праці та технологічних процесів. Роботодавець не може обробляти чутливі персональні дані особи, які стали підставою для оцінки її професійних компетентностей, після отримання результатів такої оцінки від компетентної особи.

5. Персональні дані, надані роботодавцю кандидатом на працевлаштування, мають бути видалені невідкладно після прийняття рішення про відмову у працевлаштуванні, крім випадків передбачених законом. Роботодавець може зберігати такі дані з метою працевлаштування в майбутньому на підставі згоди кандидата на працевлаштування.

6. Персональні дані, які оброблялись роботодавцем з метою здійснення внутрішнього (службового) розслідування, результати якого не призвели до негативних рішень для особи, щодо якої проводилось таке розслідування, повинні бути видалені роботодавцем після ознайомлення з матеріалами розслідування всіх осіб, які мають право на таке ознайомлення, але не раніше спливу строку позовної давності.

7. Персональні дані, зібрані в цілях трудових правовідносин, повинні оброблятись роботодавцем виключно в цих цілях та з урахуванням положень статті 13 цього Закону. У разі обробки в цілях трудових правовідносин персональних даних, які були зібрані роботодавцем з іншою метою, роботодавець зобов'язаний вжити відповідних і достатніх заходів для запобігання неналежному використанню таких персональних даних та попередньо повідомити про це працівника.

8. Для забезпечення дотримання вимог цього закону роботодавець зобов'язаний затвердити порядок обробки персональних даних, який регулює питання обробки персональних даних працівників. Такий порядок обробки персональних даних має бути наданий для ознайомлення кожному працівнику роботодавця, до якого він застосовується.

9. Персональні дані, зібрані роботодавцем в цілях трудових правовідносин, можуть бути передані суб'єктам владних повноважень виключно з метою та в обсязі, необхідному для виконання встановленого законом обов'язку роботодавця

10. Персональні дані, зібрані роботодавцем в цілях трудових правовідносин, можуть бути передані суб'єктам владних повноважень з іншою метою, ніж виконання передбаченого законом обов'язку роботодавця, або іншим особам, включаючи асоційовані підприємства у таких випадках:

1) обробка персональних даних є необхідною для цілей трудових правовідносин та такі цілі є сумісними з цілями, для яких персональні дані були зібрані, та працівник завчасно повідомлений про передачу;

2) працівник надав згоду на передачу персональних даних в конкретному випадку відповідно до вимог цього Закону;

3) якщо передача передбачена законом для виконання юридичного обов'язку або колективним договором.

11. Передача персональних даних в цілях трудових правовідносин третім особам, які знаходяться на території іншої держави, або міжнародній організації регулюється Розділом VI цього Закону.

12. Персональні дані, що стосуються суб'єкта персональних даних, уповноваженого на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень, не є конфіденційною інформацією і можуть бути відкритті третім особам.

13. Роботодавці повинні вживати відповідних і достатніх заходів для того, щоб передані персональні дані працівників були відповідними меті передачі, точними та актуальними.

Стаття 53. Обробка персональних даних працівників їх представниками

1.Персональні дані працівників обробляються їхніми представниками виключно в обсязі, необхідному для забезпечення належного представництва інтересів працівників, або для нагляду за дотриманням обов'язків роботодавцем, передбачених законодавством про працю та/або колективним договором. Роботодавець зобов'язаний не перешкоджати такій обробці та надавати доступ до персональних даних у порядку, передбаченому законодавством, та з дотриманням правил, встановлених внутрішніми актами роботодавця.

Стаття 54. Особливі вимоги до обробки роботодавцем персональних даних працівників або кандидатів на працевлаштування

1. Персональні дані про стан здоров'я працівника та кандидата на працевлаштування можуть збиратись роботодавцем від працівника або кандидата на працевлаштування.

2. Роботодавець може відібрати у кандидата на працевлаштування або працівника дані про стан здоров'я виключно у таких випадках:

1) дані є необхідними для визначення здатності працівника або кандидата на працевлаштування виконувати відповідну роботу;

2) дані є необхідним для виконання вимог щодо обов'язкових медичних оглядів у випадках, передбачених законом;

3) для забезпечення медичного обслуговування і оздоровлення або виконання вимог щодо організації праці;

4) для захисту життєво важливих інтересів працівника або інших фізичних осіб;

5) для забезпечення надання соціальних послуг або інших додаткових благ;

6) для обґрунтування, задоволення або захисту юридичної вимоги.

3. Забороняється обробка генетичних даних для цілей трудових відносин, включаючи обробку на підставі згоди працівника, крім виключних випадків, передбачених законом, який передбачає належні гарантії захисту прав працівника відповідно до Конституції України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України.

4. Роботодавець може використовувати біометричні дані працівників з метою виконання трудових відносин у разі одночасного дотримання таких умов:

1) така обробка необхідна для захисту законних прав та інтересів роботодавця або інших осіб;

2) біометричні дані використовуються з метою авторизації користувачів в інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах в процесі виконання покладених на них функцій та повноважень, задля уникнення розголошення інформації з обмеженим доступом, або з метою забезпечення безпеки приміщень у яких зберігаються матеріальні цінності або обладнання яке забезпечує збереження конфіденційної інформації;

3) права та інтереси роботодавця або інших осіб переважають ризики порушення прав суб'єкта персональних даних (працівника) та ступінь втручання в його особисте і сімейне життя;

4) досягнути мети не можливо без обробки біометричних даних.

Біометричні дані працівників не можуть бути використаними з іншою метою, ніж передбачено у цій статті.

5. Доступ до даних про стан здоров’я працівника та кандидата на працевлаштування можуть мати виключно ті працівники роботодавця, які несуть відповідальність за розголошення конфіденційної інформації та якщо це необхідно для виконання їхніх посадових обов’язків.

6. Дані про стан здоров’я працівника повинні зберігатися роботодавцем окремо від інших персональних даних, які обробляються роботодавцем. Роботодавець зобов’язаний вживати організаційних та технічних заходів для недопущення доступу до даних про стан здоров’я працівників осіб, які не мають дозволу на ознайомлення з такими даними від роботодавця.

Стаття 55. Прозорість обробки персональних даних в цілях трудових правовідносин

1. Працівник має право отримати інформацію про обробку його персональних даних, у обсязі та у спосіб, передбачені статтями 18 та 19 цього Закону.

2. Роботодавець зобов'язаний ознайомити працівника з всією інформацією про обробку персональних даних, які можуть бути зібрані за допомогою інформаційно-комунікаційних технологій, включаючи відеоспостереження та можливого використання відеозаписів на робочому місці.

3. Працівник має право на отримання своїх персональних даних про його оцінку, включаючи дані оцінки його здібностей, навичок та професійної підготовки, після того як вони були створені. Працівник має право оскаржити достовірність та/або повноту обставин, які було взято до уваги під час формування оцінки його здібностей, навичок та професійної підготовки до керівника роботодавця або до суду.

4. Роботодавцю забороняється приймати рішення, яке має суттєвий вплив на права та обов'язки працівника, на підставі автоматичної обробки персональних даних без врахування позиції працівника.

5. Працівник має право на подання запиту роботодавцю про отримання інформації щодо обробки його персональних даних та отримати від роботодавця обґрунтування обробки його персональних даних.

6. Права працівника, передбачені цією статтею, можуть бути обмежені, якщо такі обмеження встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, економічного добробуту та прав людини з метою запобігання заворушенням чи злочинам.

7. У випадку провадження внутрішнього (службового) розслідування реалізація прав працівника, який є суб'єктом цього розслідування, передбачених цією статтею, може бути відстрочено до закінчення розслідування. Після закінчення розслідування інформація, яка запитувалась працівником відповідно до цього Закону, невідкладно надається працівнику роботодавцем.

РОЗДІЛ IX

ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Стаття 56. Обробка персональних даних постачальником електронних комунікаційних послуг

1. Обробка персональних даних постачальником електронних комунікаційних мереж та/або послуг здійснюється у відповідності до вимог цього Закону з урахуванням особливостей, передбачених цим розділом.

2. Для цілей цього розділу постачальник електронних комунікаційних мереж та/або послуг - це визначені Законом України «Про електронні комунікації» постачальник електронних комунікаційних мереж та постачальник електронних комунікаційних послуг.

Стаття 57. Безпека електронних комунікацій

1. Постачальник електронних комунікаційних мереж та/або послуг зобов'язаний вживати відповідних та достатніх технічних і організаційних заходів для забезпечення безпеки надання електронних комунікаційних послуг. У разі необхідності для забезпечення безпеки надання електронних комунікаційних послуг щодо безпеки електронних комунікаційних мереж, постачальник електронних комунікаційних послуг зобов'язаний вживати

відповідних і достатніх технічних та організаційних заходів у співпраці з постачальником електронних комунікаційних мереж.

2. Заходи, передбачені частиною першою цієї статті, враховуючи стан технологічного розвитку та вартість витрат для їх впровадження, повинні забезпечувати відповідний до ризиків рівень захисту. Для цілей цієї статті під ризиками розуміється будь-які дії, послуги або товари, які можуть зашкодити таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, конфіденційності та безпеці електронних комунікаційних мереж та/або електронних комунікаційних послуг, які призводять до зміни доступності, контенту або якості послуг та які постачальник електронних комунікаційних мереж та/або послуг може ефективно усунути самостійно або у співпраці з іншими постачальниками електронних комунікаційних мереж та/або послуг.

3. Заходи, передбачені частиною першою цієї статті, повинні, зокрема, забезпечувати:

1) щоб доступ до персональних даних мали лише особи, які мають на це дозвіл, в передбачених законом цілях; та

2) захист персональних даних, які зберігаються або передані, від знищення, втрати або зміни, неправомірного зберігання, обробки, доступу або оприлюднення; та

3) впровадження політики безпеки щодо обробки персональних даних.

4. Періодичні перевірки належності вжитих заходів проводяться контролюючим органом у відповідності до затвердженого ним порядку. Контролюючий орган надає практичні рекомендації щодо заходів, які необхідно вжити для

забезпечення належного рівня захисту обробки персональних даних в сфері електронних комунікацій.

Стаття 58. Повідомлення споживачів та кінцевих користувачів про ризик для безпеки електронних комунікаційних мереж та/або послуг

1. Постачальник електронних комунікаційних мереж та/або послуг зобов'язаний повідомляти споживачів та користувачів електронних комунікаційних послуг про виникнення ризику для безпеки електронних комунікаційних мереж негайно, не пізніше ніж 48 годин після того, як йому стане відомо про ризик через оголошення на його веб-сайті або у інший належний спосіб. Якщо постачальник електронних комунікаційних мереж та/або послуг не може вжити заходи для усунення ризику, він зобов'язаний повідомити споживачів та користувачів електронних комунікаційних послуг електронних комунікаційних послуг про всі можливі засоби для усунення ризику та надати їм можливість швидкого доступу до заходів захисту.

2. У разі якщо порушення безпеки електронних комунікацій мало місце не з вини споживачів та користувачів електронних комунікаційних послуг, постачальник електронних комунікаційних мереж та/або послуг несе всі витрати надання електронних комунікаційних послуг, які виникли в зв'язку з порушенням. Порушення не вважається таким, що мало місце з вини споживача електронних комунікаційних послуг, у разі якщо споживач вжив всіх розумно очікуваних заходів захисту та дотримувався правил, встановлених постачальником електронних комунікаційних мереж та/або послуг.

Стаття 59. Таємниця приватного спілкування

1. Охорона таємниці приватного спілкування, листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через інформаційні системи гарантуються Конституцією та законами України.

Спілкуванням є передання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв’язку будь-якого типу, у тому числі інформації системами електронних комунікацій. Спілкування є приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, при яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб.

Таємниця приватного спілкування охоплює, зокрема:

1) зміст спілкування;

2) дані трафіку;

3) дані про місцезнаходження споживача електронних комунікаційних послуг, до яких відносяться будь-які дані, що обробляються при наданні електронних комунікаційних послуг, в тому числі, щодо розташування термінального обладнання;

4) факти та обставини, за яких мало місце припинення або невстановлення з’єднання.

2. Постачальник електронних комунікаційних мереж та/або послуг та інші особи, залучені у процес діяльності засобів електронних комунікацій будь-якого типу, передачу інформації системами електронних комунікацій, повинні зберігати таємницю приватного спілкування після закінчення їх діяльності, на яку поширювалося зобов’язання збереження таємниці.

3. Постачальник електронних комунікаційних мереж та/або послуг та інші особи, залучені у процес діяльності засобів електронних комунікацій будь-якого типу, передачу інформації системами електронних комунікацій, можуть отримуваати, використовувати та передавати іншим інформацію про приватне спілкування, в обсязі, необхідному для надання електронних комунікаційних послуг.

4. Будь-яке втручання у приватне спілкування будь-якою особою, крім учасників спілкування, у формі прослуховування, записування, зберігання та передачі інформації, без згоди учасників спілкування заборонено, крім випадків, передбачених законом або якщо це необхідно для надання електронних комунікаційних послуг.

5. У разі якщо постачальник електронних комунікаційних мереж та/або послуг отримує інформацію про приватне спілкування або здійснюють запис приватного спілкування або зберігають інформацію про нього, він зобов'язаний повідомити про це споживача або користувача електронних комунікаційних послуг при укладенні договору про надання електронних комунікаційних послуг або до початку надання таких послуг та вилучити інформацію про приватне спілкування, як тільки це буде технічно можливо, та інформація не є необхідною для надання електронних комунікаційних послуг.

6. Здійснення запису приватного спілкування та пов'язаних з ним даних дозволяється під час здійснення підприємницької діяльності в цілях надання доказів здійсненої оплати або спілкування за умови, що учасники спілкування завчасно повідомлені про запис, його цілі та період зберігання даних. Записані і збережені дані повинні бути вилучені негайно після досягнення мети збереження або після закінчення строку оскарження відповідної дії.

7. Повідомлення про запис спілкування повинно бути надано у той же спосіб та в тій же формі, в які здійснюється спілкування.

Стаття 60. Збереження персональних даних про споживача та/або кінцевого користувача електронних комунікаційних послуг

1. Постачальник електронних комунікаційних мереж та/або послуг може збирати та зберігати лише ті персональні дані споживача або кінцевого користувача електронних комунікаційних послуг, які необхідні для:

1) виконання, укладення, зміни або розірвання договору про надання електронних комунікаційних послуг;

2) виставлення рахунків на оплату електронних комунікаційних послуг;

3) інших правомірних цілей за згодою споживача електронних комунікаційних послуг.

Стаття 61. Порядок надання інформації на запити про надання доступу до персональних даних споживача та/або кінцевого користувача електронних комунікаційних послуг та збереження інформації про такі запити

1. З метою забезпечення безпеки обробки персональних даних постачальники електронних комунікаційних мереж та/або послуг зобов’язані розробити, погодити з контролюючим органом та затвердити порядок надання інформації на запити суб’єктів владних повноважень щодо доступу до персональних даних споживача або кінцевого користувача електронних комунікаційних послуг. Постачальники електронних комунікаційних мереж та/або послуг зобов’язані зберігати інформацію про запити, включаючи кількість отриманих запитів, суб’єктів, які зробили запит, юридичне обґрунтування запиту та відповіді на запит, протягом трьох років.

2. Постачальник електронних комунікаційних мереж та/або послуг зобов’язаний надавати інформацію про запити на вимогу контролюючого органу.

Стаття 62. Каталоги номерів (телефонні довідники)

1. Споживачі та/або кінцеві користувачі повинні бути безкоштовно поінформовані до того, як їх дані будуть внесені до друкованого чи електронного довідника, публічно доступного чи через довідкові служби, про мету каталогу та про всі подальші можливості використання їхніх даних на основі пошукових функцій. Витрати на інформування абонентів несе емітент каталогів.

2.Споживачі та/або кінцеві користувачі мають право самостійно визначити які саме персональні дані можуть бути включені до каталогу та заперечувати проти включення до каталогів своїх персональних даних.

Якщо споживач або кінцевий користувач вирішив включити свої персональні дані до публічного каталогу, за замовчуванням, включаються дані про: ім’я, номер телефону та адресу листування споживача повинні бути включені до каталогу. Абоненти можуть перевірити включені дані та вимагати їх змін, підтримання в актуальному стані чи видалення.

3. Споживачам та кінцевим користувачам повинна бути надана можливість заборонити використання їх персональних даних для дзвінків з комерційною або дослідницькою метою. Споживач або кінцевий користувач може заборонити використовувати його персональні дані для обох або однієї з вищевказаних цілей при внесенні в каталог або в будь-який час згодом. Емітент каталогів повинен чітко позначити заборону на використання персональних даних абонента для певної мети в каталозі. Якщо абонент сигналізує про заборону

використання після включення в каталог або змінює зміст цієї заборони, емітент каталогів повинен внести зміни в наступному випуску каталогу.

4. Не включається до публічного каталогу інформація про перевірку, виправлення чи видалення персональних даних, зазначених у другому пункті цієї статті, внесення заборони на використання персональних даних абонента для цілей, зазначених у пункті третьому цієї статті або внесення змін до цієї заборони повинні бути безкоштовними для абонента.

Стаття 63. Дані трафіку

1. Дані трафіку, які пов’язані із споживачем та/або кінцевим користувачем електронних комунікаційних послуг та які зберігаються постачальником електронних комунікаційних мереж та/або послуг повинні бути вилучені або знеособленні як тільки вони перестали бути необхідними для цілей надання електронних комунікаційних послуг, крім випадків, коли збереження даних трафіку здійснюється:

1) на підставі закону;

2) для цілей виконання вимог статті 61 про внутрішній порядок надання інформації на запити цього Закону;

3) для захисту життєво важливих інтересів споживача електронних комунікаційних послуг;

4) для розрахунку оплати електронних комунікаційних послуг;

5) для надання маркетингових або інших додаткових електронних комунікаційних послуг;

2. Постачальник електронних комунікаційних мереж та/або послуг може обробляти дані трафіку, пов’язані із споживачем електронних комунікаційних

послуг, з метою надання маркетингових послуг або інших додаткових послуг протягом періоду, який є необхідним для надання таких послуг та лише якщо споживач таких послуг надав згоду на таку обробку персональних даних. Споживач електронних комунікаційних послуг до надання згоди повинен бути повідомлений про види даних трафіку, які будуть оброблятись, про цілі та тривалість обробки.

3. Постачальник електронних комунікаційних мереж та/або послуг може обробляти дані трафіку, пов'язані із споживачем електронних комунікаційних послуг, з метою розрахунку оплати електронних комунікаційних послуг до здійснення споживачем оплати. Постачальник електронних комунікаційних мереж та/або послуг зобов'язаний повідомити споживача про умови та тривалість обробки даних трафіку на підставі цього Закону.

4. Дані трафіку можуть оброблятись на підставі цієї статті виключно уповноваженими особами постачальника електронних комунікаційних мереж та/або послуг та які здійснюють оформлення рахунків або управління трафіком, відповідають на запити споживачів, встановлюють випадки шахрайства, надають маркетингові послуги або інші додаткові послуги, у обсязі та протягом періоду, необхідному для здійснення цієї діяльності.

5. Постачальник електронних комунікаційних мереж та/або послуг зобов'язаний надати дані трафіку, в тому числі пов'язані з ним документи, контролюючому органу на його вимогу з метою доведення дотримання вимог цього Закону.

Стаття 64. Дані про місцезнаходження споживача та/або кінцевого користувача

1. Дані про місцезнаходження споживача та/або кінцевого користувача електронних комунікаційних послуг, крім даних трафіку, можуть оброблятись в

обсязі та протягом періоду, необхідному для цілей надання додаткових послуг, на підставі закону або якщо вони знеособлені або споживач надав свою згоду.

2. До надання згоди на обробку персональних даних, передбачених частиною першою цієї статті, споживач та/або кінцевий користувач повинен бути повідомлений про:

1) можливість відкликати згоду;

2) вид даних, які підлягають обробці;

3) ціль та строк обробки персональних даних;

4) можливість передачі даних третім особам для надання додаткових послуг.

3. Споживач та/або кінцевий користувач, який надав згоду на обробку персональних даних, передбачених частиною першою цієї статті, має право безоплатно, з використанням простих засобів, наданих йому постачальником електронних комунікаційних мереж та/або послуг, відкликати згоду на обробку персональних даних щодо кожного з'єднання з мережею або щодо кожного випадку передавання даних.

4. Дані про місцезнаходження споживача та/або кінцевого користувача електронних комунікаційних послуг можуть оброблятись на підставі цієї статті, особами, уповноваженими постачальниками електронних комунікаційних мереж та/або послуг, які здійснюють оформлення рахунків або управління трафіком, відповідають на запити споживачів та/або кінцевих користувачів, встановлюють випадки шахрайства, надають маркетингові послуги або інші додаткові послуги, у обсязі та протягом періоду, необхідному для здійснення цієї діяльності.

5. Постачальник електронних комунікаційних мереж та/або послуг зобов’язаний надати дані про місцезнаходження споживача та/або кінцевого користувача контролюючому органу на його вимогу з метою доведення дотримання вимог цього Закону.

Стаття 65. Надання даних про місцезнаходження споживача та/або кінцевого користувача

1. Постачальник електронних комунікаційних мереж та/або послуг з метою захисту життєво важливих інтересів фізичної особи зобов’язаний надати уповноваженим органам або особам дані, необхідні для встановлення останнього місця знаходження мобільного кінцевого (термінального) обладнання, якщо :

1) надання цих даних є необхідним для попередження смерті, дорожньо-транспортної пригоди або спричинення серйозної шкоди особі, яка має або є підстави вважати, що має при собі мобільне кінцеве (термінальне) обладнання;

2) надання цих даних є необхідним для встановлення місця знаходження особи, яка визнана судом недієздатною, оголошена в розшук, хворіє на хворобу, яка може призвести до вчинення дій, що являють собою безпосередню небезпеку для неї чи оточуючих, та яка має або є підстави вважати, що має при собі мобільне кінцеве (термінальне) обладнання;

3) надання цих даних є необхідним для встановлення місця знаходження малолітньої або неповнолітньої особи, яку за заявою батьків або опікунів чи піклувальників оголошено в розшук та яка має або є підстави вважати, що має при собі мобільне кінцеве (термінальне) обладнання;

2. Дані, передбачені частиною першою цієї статті, надаються постачальником електронних комунікаційних мереж та/або послуг на письмовий обґрунтований

запит керівника уповноваженого органу, який здійснює розшук відповідної особи.

3. Інформація про місцезнаходження абонента (споживача), що здійснює виклик – це оброблені у електронній комунікаційній мережі дані, отримані від мережевої інфраструктури або мобільного кінцевого (термінального) обладнання, із зазначенням місцезнаходження мобільного кінцевого (термінального) обладнання (точки його підключення до мережі), а в мережі фіксованого зв'язку - даних про фізичну адресу кінцевого пункту мережі.

4. Уповноважений орган здійснює обробку персональних даних, отриманих на підставі цієї статті, з дотриманням принципів та вимог цього Закону.

5. Перевірка дотримання вимог та принципів цього Закону при обробці персональних даних, передбачених частиною першою цієї статті, здійснюється контролюючим органом у затвердженому ним порядку не рідше одного разу на рік.

6. Постачальник електронних комунікаційних мереж та/або послуг у відповідь на обґрунтований запит зобов'язаний надати дані настільки швидко, як тільки це технічно можливо. Відповідальність за дотримання законності при наданні даних несе постачальник електронних комунікаційних мереж та/або послуг.

7. Уповноважений орган зобов'язаний повідомити особу, щодо якої було отримано дані на підставі цієї статті, про отримання даних як тільки це стане можливим, крім випадків, коли повідомлення може нанести шкоду інтересам цієї особи або осіб, вказаних в частині першій цієї статті.

Стаття 66. Відстеження зловмисних або небажаних викликів абоненту

1. Абонент може подати письмовий запит постачальнику електронних комунікаційних мереж та/або послуг щодо відстеження зловмисних або

небажаних викликів. Оператор може тимчасово, але не більше трьох місяців, записувати походження всіх викликів до кінцевого термінального обладнання абонента чи кінцевих пунктів мережі, включаючи ті, для яких існує вимога не ідентифікації лінії виклику.

2. Постачальник електронних комунікаційних мереж та/або послуг повинен зберегти дані про відстеження та зробити доступними для абонента, який вимагав відстежити зловмисні або небажані виклики, у письмовій формі, дані про результати відстеження, тобто дані, що ідентифікують сторони, що здійснюють зв'язок, зокрема, номер абонента, дата.

3. Постачальник електронних комунікаційних мереж та/або послуг надсилає будь-які дані, що розкривають особу абонента, що викликає, лише у випадку, якщо абонент виявить юридичний інтерес до захисту своїх прав перед судом, внаслідок чого оператор повідомляє абонента, що викликає, та контролюючий орган.

4. Постачальники електронних комунікаційних мереж та/або послуг забезпечують збереження даних, зібраних відповідно до цієї статті, з належним урахуванням заходів, зазначених у частині третій статті 60 цього Закону, протягом трьох років після її надсилання абоненту.

5. Контролюючий орган здійснює нагляд за виконанням положень цієї статті.

Стаття 67. Небажані виклики та повідомлення абоненту

1. Здійснення небажаних викликів або направлення повідомлень забороняється.

2. Абонент має право звернутись до постачальника електронних комунікаційних мереж та/або послуг із запитом про встановлення контактних даних іншого абонента, який здійснює небажані виклики та повідомлення.

3. Абонент подає запит в письмовій формі, який має містити:

1) контактні дані абонента (номер, ім’я);

2) номер абонента, який здійснює небажані виклики;

3) відомості, які підтверджують, що до абонента здійснюються небажані виклики з номера, щодо якого здійснено запит;

4) зобов’язання абонента використовувати дані абонента, який здійснює небажані дзвінки, з метою захисту своїх інтересів та не використовувати дані з іншою метою.

4. Постачальник електронних комунікаційних мереж та/або послуг зобов’язаний протягом 10 днів надати відповідь абоненту про задоволення запиту або відмову у задоволенні. Постачальник електронних комунікаційних мереж та/або послуг має право відмовити у задоволенні запиту у випадку, якщо запит не містить відомостей, передбачених частиною третьою цієї статті.

5. У разі задоволення запиту постачальник електронних комунікаційних мереж та/або послуг повинен надати абоненту, який подав запит, інформацію про номер кінцевого (термінального) обладнання та ім’я (назву) абонента, який здійснює небажані виклики чи повідомлення, у разі наявності адресу реєстрації місця проживання та/або адресу реєстрації юридичної особи.

6. У разі задоволення запиту постачальник електронних комунікаційних мереж та/або послуг зобов’язаний зберігати інформацію про запит, який було задоволено, та відповідь на нього протягом трьох років з дня надання інформації абоненту у обсязі, необхідному для ідентифікації абонента та підтвердження здійснення ним небажаних викликів на номер абонента, який подав запит.

7. Постачальник електронних комунікаційних мереж та/або послуг зобов'язаний повідомити абонента, чиї дані були надані у відповідь на запит, передбачений цією статтею, про надання таких даних протягом трьох робочих днів з дня надання даних.

8. Повідомлення повинно містити номер та ім’я (назву) абонента, якому були надані його дані, інформацію про підстави та цілі надання такої інформації.

9. Постачальник електронних комунікаційних мереж та/або послуг зобов’язаний надати контролюючому органу необхідну інформацію про відмову або задоволення запитів, передбачених цією статтею, на його вимогу з метою доведення дотримання вимог цього Закону.

Стаття 68. Повідомлення про витік персональних даних

1. Постачальник електронних комунікаційних мереж та/або послуг зобов’язаний повідомити про будь-який витік персональних даних постійно діючий центральний орган виконавчої влади із спеціальним статусом у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв’язку України та контролюючий орган невідкладно, але не більше ніж протягом 48 годин з моменту, коли йому стало відомо про витік.

2. Постачальник електронних комунікаційних мереж та/або послуг зобов’язаний повідомити про витік персональних даних споживача та/або інших фізичних осіб у разі, якщо витік може призвести до ризику для їх прав та свобод, невідкладно, але не більше ніж протягом 48 (сорока восьми) годин з моменту, коли йому стало відомо про витік.

3. Повідомлення про витік має містити інформацію, передбачену частиною четвертою статті 37 повідомлення контролюючого органу про витік персональних даних.

4. Постачальник електронних комунікаційних мереж та/або послуг не зобов’язаний повідомляти про витік персональних даних самого споживача та/або кінцевого користувача або третіх осіб, чиїх прав і свобод стосується витік, у разі якщо постачальник електронних комунікаційних мереж та/або послуг вжив відповідних і достатніх технічних та організаційних заходів захисту і такі заходи були застосовані до персональних даних, яких стосувався витік, зокрема, щодо усунення можливості використання персональних даних особою, яка не має дозволу на доступ до них.

5. Контролюючий орган має право зобов’язати постачальника електронних комунікаційних мереж та/або послуг повідомити споживача та/або кінцевого користувача, третіх осіб про витік персональних даних у разі, якщо таке повідомлення не було здійснено та вжиті заходи, передбачені частиною четвертої цієї статті, не є відповідними та достатніми. Постачальник електронних комунікаційних мереж та/або послуг повинен повідомити контролюючий орган про виконання зобов’язання про повідомлення про витік невідкладно після виконання такого зобов’язання.

6. Постачальник електронних комунікаційних мереж та/або послуг зобов’язаний документувати будь-які випадки витоків персональних даних, включаючи факти, пов’язані з ними, їх наслідками та заходами, вжитими для їх усунення.

7. Порядок повідомлення постачальниками електронних комунікаційних мереж та/або послуг про витік персональних даних та форма такого повідомлення затверджуються контролюючим органом.

РОЗДІЛ X

ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ ПРАВООХОРОННИМИ ОРГАНАМИ

Стаття 69. Вимоги до обробки персональних даних правоохоронними та розвідувальними органами

1. Правоохоронні та розвідувальні органи при обробці персональних даних у правоохоронних цілях повинні дотримуватися цього Закону з урахуванням положень, визначених статтею 70 цього Закону.

2. Правоохоронні та розвідувальні органи мають право обробляти персональні дані у правоохоронних цілях лише у разі необхідності виконання завдань в суспільних інтересах або виконання повноважень, покладених на правоохоронний орган законом.

3. Персональні дані, отримані правоохоронним або розвідувальним органом в цілях правоохоронної чи розвідувальної діяльності не можуть оброблятися з іншою метою, якщо це прямо не дозволено законом.

4.Обробка персональних даних в правоохоронних цілях, яка здійснюється в порядку, передбаченому Кримінальним процесуальним кодексом України здійснюється з урахуванням принципів, визначених цим Законом.

5. Правоохоронні органи повинні чітко розмежовувати та обробляти окремо у різних базах даних інформацію про різні категорії суб'єктів персональних даних, таких як:

1) особи, щодо яких є обґрунтовані підстави вважати, що вони вчинили або збираються вчинити кримінальне правопорушення;

2) особи, засуджені за вчинення кримінального правопорушення;

3) особи, постраждалі внаслідок вчинення кримінального правопорушення або особи, щодо яких є обґрунтовані підстави вважати, що вони можуть стати постраждалими внаслідок вчинення кримінального правопорушення;

4) інші учасники кримінального провадження.

Стаття 70. Особливості реалізації прав суб'єктів персональних даних у зв'язку з обробкою персональних даних в цілях правоохоронної діяльності

1. У зв'язку з обробкою персональних даних в цілях правоохоронної діяльності, реалізація прав суб'єктів персональних даних передбачених статтями 18, 19 та 21 - 24 цього Закону може бути обмежена у випадках та порядку, передбачених законом і лише з метою недопущення :

1) розголошення інформації, що становить державну таємницю, таємницю слідства, розвідувальну таємницю;

2) перешкоджання проведенню слідчих, розшукових, розвідувальних дій;

3) загроз для громадської чи національної безпеки;

4) загроз для життя, здоров'я чи порушення прав і свобод інших осіб.

2. Рішення щодо обмеження реалізації прав суб'єктів персональних даних приймається у кожному окремому випадку, враховуючи обставини, характер права, щодо реалізації якого звернувся суб'єкт персональних даних та баланс між необхідністю досягнення мети правоохоронної діяльності та необхідністю забезпечення прав суб'єкта персональних даних.

3. Реалізація прав суб'єктів персональних даних повинна бути відновлена, як тільки закінчились обставини, у зв'язку з якими вона була обмежена.

4. Суб'єкт персональних даних має право оскаржити рішення щодо обмеження його прав до контролюючого органу або до суду.

РОЗДІЛ XI

ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Стаття 71. Відповідальність за порушення законодавства в сфері захисту персональних даних

1. Вчинення правопорушень у сфері захисту персональних даних тягне за собою відповідальність, передбачену цим Законом та іншими законами України.

2. Рішення про притягнення до відповідальності за правопорушення в сфері захисту персональних даних, а також про застосування інших заходів передбачених законом, приймається контролюючим органом в порядку, визначеному законодавством або судом.

3. До відповідальності передбаченої цим Законом можуть бути притягнені контролери або оператори персональних даних.

4. Притягнення винних осіб до відповідальності передбаченої цим Законом, а також адміністративної або кримінальної відповідальності не позбавляє суб'єктів персональних даних, права на відшкодування матеріальної та моральної шкоди завданої внаслідок порушення його прав в порядку передбаченому цивільним законодавством.

Стаття 72. Відповідальність контролерів та операторів за порушення законодавства у сфері захисту персональних даних

1. Порушення вимог передбачених статтями 4, 5, 6, 10, 11, 13, 14, 17, 20-24, 29, 30-32, 36, частинами першою — третьою статті 50, частиною четвертою статті 51, статтями 52, 55, частиною третьою статті 57, статтями 60, 62, 67 цього Закону, що не призвело до порушення прав суб’єктів персональних даних -

тягне за собою накладення штрафу на фізичних осіб в розмірі від 10 000 до 30 000 гривень, на юридичних осіб в розмірі від 0,05% до 0,1% загального річного обороту такої юридичної особи але не менше ніж 30 000 гривень за кожне окреме порушення вимог Закону.

2. Порушення вимог передбачених статтями 12, 18, 19, 25, 63-65, а також порушення вимог передбачених статтями 4, 5, 6, 10, 11, 13, 14, 17, 20-24, 29, 32,

34, частинами першою, четвертою та п'ятою статті 40, частинами першою — третьою статті 50, частиною четвертою статті 51 статтями 52, 55, частиною третьою статті 57, статтями 60, 61, 62 цього Закону, що призвело до порушення прав суб’єктів персональних даних -

тягне за собою накладення штрафу на фізичних осіб в розмірі від 30 000 до 100 000 гривень, на юридичних осіб в розмірі від 0,5% до 1% загального річного обороту такої юридичної особи але не менше ніж 100 000 гривень за кожне окреме порушення вимог Закону.

3. Порушення вимог передбачених статтями 7, 8, 9, 33, 37, 38, частинами першою — третьою та п'ятою — дев'ятою статті 41, статтею 44, частиною шостою статті 45, статтями 48, 49, частиною п'ятою статті 51, статтею 54, частиною першою статті 58, частинами другою — сьомою статті 59, статтями 63 — 65, статтею 68 цього Закону -

тягне за собою накладення штрафу на фізичних осіб в розмірі від 100 000 до 300 000 гривень, на юридичних осіб в розмірі від 3% до 5% загального річного обороту такої юридичної особи але не менше ніж 300 000 гривень за кожне окреме порушення вимог Закону.

4. Порушення інших положень цього Закону, не зазначених у частинах першій - третій цієї статті -

тягне за собою збільшення розміру штрафу передбаченого частинами першою - третьою цієї статті Закону на тридцять відсотків.

5. Кожне повторне порушення вимог Закону вчинене упродовж року тягне за собою накладення штрафу у розмірі двохсот відсотків від розміру раніше накладеного штрафу.

6. Якщо в межах однієї і тієї ж обробки персональних даних або кількох пов'язаних між собою операцій обробки персональних даних контролер або оператор персональних даних допустив порушення декількох вимог передбачених статтями цього Закону сукупний розмір штрафу не повинен

перевищувати розмір штрафу за найбільш серйозне порушення. Зазначене положення не поширюється на випадки передбачені частинами шостою та сьомою цієї статті Закону.

7. Загальні розміри штрафів, передбачених частинами першою - третьою цієї статті Закону не можуть перевищувати такі межі:

1) для штрафів передбачених частиною першою цієї статті Закону максимальний розмір штрафу становить: на фізичних осіб в розмірі до 10 мільйонів гривень, на юридичних осіб в розмірі до 50 мільйонів гривень або до 3% загального річного обороту такої юридичної особи за останній звітний рік, що передував року, в якому накладається штраф;

2) для штрафів передбачених частиною другою цієї статті Закону максимальний розмір штрафу становить: на фізичних осіб в розмірі до 20 мільйонів гривень, на юридичних осіб в розмірі до 90 мільйонів гривень або до 5% загального річного обороту такої юридичної особи за останній звітний рік, що передував року, в якому накладається штраф;

3) для штрафів передбачених частиною третьою цієї статті Закону максимальний розмір штрафу становить: на фізичних осіб в розмірі до 20 мільйонів гривень, на юридичних осіб в розмірі до 150 мільйонів гривень або до 8% загального річного обороту такої юридичної особи за останній звітний рік, що передував року, в якому накладається штраф.

Положення частини сьомої цієї статті не застосовується у випадках визначених частинами четвертою та п'ятою цієї статті Закону.

Стаття 73. Строки давності для застосування відповідальності передбаченої цим Законом

1. Особа не може бути притягнена до фінансової відповідальності за порушення законодавства про захист персональних даних, якщо минув строк давності притягнення до відповідальності.

Строк давності притягнення до передбаченої цим Законом відповідальності становить три роки з дня вчинення порушення, а в разі триваючого порушення - з дня виявлення порушення.

2. Перебіг строку давності зупиняється на час розгляду контролюючим органом справи про порушення законодавства в сфері захисту персональних даних, а також на час розгляду відповідної справи у суді.

Розділ XII

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності з дня опублікування та вступає в силу з 1 січня 2023 року.

2. Визнати таким, що втратив чинність Закон України «Про захист персональних даних» (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481 із наступними змінами) з дня набрання чинності цим Законом.

3. До приведення законодавства України у відповідність із цим Законом акти законодавства України застосовуються в частині, що не суперечить цьому Закону.

3. Кабінету Міністрів України:

1) протягом трьох місяців з дня набрання чинності цим Законом:

забезпечити прийняття нормативно-правових актів, необхідних для реалізації положень цього Закону;

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити приведення міністерствами, іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

4. Внести зміни до таких законодавчих актів України:

1) статтю 4 Кодексу законів про працю України (Відомості Верховної Ради УРСР, 1971 р., додаток до № 50, ст. 375) доповнити новою частиною такого змісту:

«Захист персональних даних працівників в трудових відносинах регулюється Законом України «Про захист персональних даних»;

2) друге речення частини першої статті 7 Закону України “Про поховання та похоронну справу” (Відомості Верховної Ради України (ВВР), 2004, № 7, ст.47) викласти в такій редакції:

«Надання такої інформації здійснюється відповідно до Закону України “Про захист персональних даних»

3) пункт 2 частини першої статті 3 Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» (Відомості Верховної Ради України, 2013 р., № 51, ст. 716) викласти в такій редакції:

« біометричні дані - персональні дані, які стосуються фізичних, фізіологічних чи поведінкових характеристик фізичної особи, які в результаті спеціальної технічної обробки надають можливість ідентифікувати або верифікувати фізичну особу (біометричні дані, параметри - відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук)»;

4) Статтю 11 Закону України «Про державні фінансові гарантії медичного обслуговування населення» (Відомості Верховної Ради України, 2018 р., № 5, ст. 31) викласти у наступній редакції:

«Стаття 11. Електронна система охорони здоров’я

1. Порядок функціонування електронної системи охорони здоров’я затверджується Кабінетом Міністрів України з урахуванням вимог Закону України «Про захист персональних даних».

2. Доступ до даних про пацієнта, що містяться в електронній системі охорони здоров’я має право лікар, з яким пацієнт (його законний представник) уклав декларацію, інші медичні працівники, на яких поширюється зобов’язання відповідно до статті 40 Закону України «Основи законодавства України про охорону здоров'я».

3. Уповноважений орган зобов’язаний опубліковувати на офіційному веб-сайті дані, накопичені в електронній системі охорони здоров’я, в обсязі та в порядку, встановленому Кабінетом Міністрів України, погодженому з контролюючим органом у сфері захисту персональних даних.

Дані можуть бути опубліковані за умови знеособлення персональних даних відповідно до вимог Закону України «Про захист персональних даних».»

5) Статтю 14 Закону України «Про електронну комерцію» (Відомості Верховної Ради України, 2015 р., № 45, ст. 410) викласти у наступній редакції:

«Стаття 14. Захист персональних даних у сфері електронної комерції

1. Використання персональних даних у сфері електронної комерції може здійснюватися у разі створення суб’єктом електронної комерції умов для захисту таких даних.

Учасники відносин у сфері електронної комерції зобов’язані забезпечити захист персональних даних у порядку, передбаченому Законом України «Про захист персональних даних».

2. Ідентифікація особи за допомогою електронного підпису, визначеного статтею 12 цього Закону, має здійснюватися під час кожного входу в інформаційну систему суб’єкта електронної комерції.

З метою недопущення несанкціонованого доступу до облікового запису особи в інформаційно-телекомунікаційній системі суб’єкта електронної комерції для ідентифікації такої особи може використовуватися додатковий унікальний набір електронних даних, що додаються (приєднуються) до спеціального набору електронних даних, який був введений (створений) такою особою під час реєстрації.»

Голова Верховної Ради України **Д. О. Разумков**