АНАЛІЗ ЄВРОПЕЙСЬКИХ МОДЕЛЕЙ НЕЗАЛЕЖНИХ НАГЛЯДОВИХ ОРГАНІВ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ТА ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ

Звіт підготували:
Діана Шинкунєне, Лілія Олексюк, Олександр Шевчук

Ця публікація виготовлена за фінансової підтримки Європейського Союзу та Ради Європи. Погляди, викладені в цьому документі, не відображають офіційну позицію Європейського Союзу та Ради Європи.

Верстка, дизайн обкладинки та друк: «К.І.С.»

Фото: © Shutterstock

Council of Europe Publishing
F-67075 Strasbourg Cedex
(http://book.coe.int)

ЗМІСТ

1

ВСТУП

Особливого значення тема захисту персональних даних набуває для України. Угода про асоціацію між Україною та Європейським Союзом вимагає увідповіднення законодавства України європейським стандартам, що стосується також сфери захисту персональних даних.

Розділом III Угоди про асоціацію передбачається співробітництво у сфері юстиції, свободи та безпеки. Згідно зі статтею 15 Угоди про асоціацію, «Україна та Європейський Союз погодились співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів, зокрема відповідних документів Ради Європи».

Одне з головних завдань України — гармонізація національного законодавства з європейськими стандартами у сфері захисту персональних даних шляхом імплементації Регламенту (ЄС) 2016/679 відповідно до пункту 11 Плану заходів № 1106 із виконання Угоди про асоціацію, затвердженого Кабінетом Міністрів України від 25 жовтня 2017 року.

Головна проблема у сфері захисту персональних даних в Україні полягає у відсутності ефективної загальнодержавної системи захисту персональних даних, належного організаційно-правового механізму регулювання відносин та відповідальності за скоєння правопорушень у цій сфері.

З цього погляду важливо створити ефективний інституційний механізм захисту персональних даних в Україні — незалежний наглядовий орган, що відповідатиме за розроблення методичних рекомендацій, моніторинг і контроль за додержанням законодавства у сфері захисту персональних даних.

Мета цього «Аналізу європейських моделей незалежних наглядових органів у сфері захисту персональних даних та доступу до публічної інформації» — презентувати результати аналізу, проведеного групою експертів Ради Європи, і надати рекомендації щодо оптимальної моделі або певних її складників, які мають бути враховані при створенні незалежного наглядового механізму у сфері захисту персональних даних в Україні. Стаття 15 Конвенції 108+ зобов'язує сторони створити один чи кілька органів, відповідальних за забезпечення дотримання положень цієї Конвенції, що мають виконувати свої обов'язки і здійснювати повноваження повністю незалежним та нейтральним способом, при цьому не звертатися по вказівки і не виконувати чужих вказівок. Стаття 52 Регламенту (ЄС) 2016/679 містить роз'яснення, що члени наглядового органу під час виконання своїх завдань та здійснення своїх повноважень згідно з Регламентом мають бути захищеними від прямого чи опосередкованого зовнішнього впливу та не звертатися по вказівки і не виконувати вказівок будь-яких інших осіб.

Проведений експертами аналіз охоплює такі сфери:

- місце інституції в системі органів державної влади;
- сферу нагляду (контролю);
- гарантії незалежності (інституційної, функціональної, фінансової);
- повноваження на розслідування, виправні повноваження та санкції;
- дозвільні та консультативні повноваження;

- повноваження брати участь у судовому процесі;
- діяльність щодо підвищення рівня обізнаності громадськості.

Основою для аналізу послужили стандарти Ради Європи та Європейського Союзу, зокрема оновлена Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ухвалена Комітетом Міністрів на 128-й сесії Комітету міністрів (Ельсінор, 18 травня 2018 р.), та Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загального регламенту про захист даних), а також відповідні рішення Суду Європейського Союзу.

Група експертів провела опитування на тему функціонування наглядових органів у сфері захисту персональних даних у державах — членах Європейського Союзу та Європейської економічної зони. Запропоновані питання анкети наведено в додатку 1 до цього аналізу. Загалом отримано відповіді на 20 питань, які використано для ілюстрації практичного виконання вимог щодо незалежного функціонування наглядового органу.

Експерти також проаналізували наявну в публічному доступі інформацію про статус, завдання і повноваження наглядових органів у сфері захисту персональних даних і матеріали попередніх досліджень, підготовлені органами ЄС, науковцями та експертами.

Рекомендації, наведені в цьому документі, мають на меті сприяти пошукові найпослідовнішого способу впровадження міжнародних принципів у сфері захисту персональних даних в Україні, тому вони враховують вищезгадані стандарти Ради Європи та Європейського Союзу, практику, що існує в державах — членах ЄС, а також положення Конституції України і правові принципи створення державних органів в Україні.

Автори цього документу — експерти Ради Європи: Діана Шинкунєне, Лілія Олексюк та Олександр Шевчук.

2

СПИСОК СКОРОЧЕНЬ

Конвенція 108+	Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS No.108), ухвалена 28 січня 1981 року у Страсбурзі, зі змінами, внесеними відповідно до Протоколу № 223
FRA	Агентство Європейського Союзу з основоположних прав людини
ЗРЗД	Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загального регламенту про захист даних)
СЄС	Суд Європейського Союзу
ОЗПД	Орган(и) у сфері захисту персональних даних
Пояснювальна записка	Пояснювальна записка до Конвенції 108+, ухвалена Комітетом міністрів на 128-й сесії (Ельсінор, 18 травня 2018 року)
Звіт	«Аналіз європейських моделей незалежних наглядових органів у сфері захисту персональних даних і доступу до публічної інформації»

3

МІСЦЕ ІНСТИТУЦІЇ В СИСТЕМІ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ, СФЕРА НАГЛЯДУ, ГАРАНТІЇ НЕЗАЛЕЖНОСТІ

3.1. Статус і місце інституції в системі органів державної влади

Незалежні наглядові органи у сфері захисту персональних даних — невіднятний складник системи захисту персональних даних у демократичному суспільстві, мета якої — забезпечення права на захист персональних даних. Суд Європейського Союзу у своєму рішенні від 9 березня 2010 у справі «Європейська комісія проти Федеральної Республіки Німеччини» C-518/07 постановив: «Наглядові органи, передбачені статтею 28 Директиви 95/46, стоять на варті основних прав і свобод, і їхнє існування в державах — членах ЄС, як зазначено в пункті 62 преамбули до Директиви 95/46, вважається невіднятним складником системи захисту фізичних осіб у зв'язку з обробкою персональних даних»[1].

Стаття 15 Конвенції 108+ зобов'язує сторони передбачити створення органів, відповідальних за забезпечення дотримання положень цієї Конвенції. Конвенція 108+ та Загальний регламент про захист даних не містять вимог щодо складу такого органу (тобто чи це має бути одна уповноважена особа, чи колегіальний орган), і можна відзначити, що серед європейських країн існують різні підходи. У деяких країнах можна побачити єдиного уповноваженого (Хорватія, Кіпр, Естонія, Ірландія, Латвія, Ліхтенштейн, Литва, Норвегія, Румунія, Словаччина тощо), тоді як в інших за ведення нагляду за реалізацією законодавства у сфері захисту персональних даних відповідає колегіальний орган (Франція, Греція, Італія, Люксембург, Португалія тощо). Наглядовий орган Ісландії зазначив, що повсякденною роботою керує уповноважений, проте до складу органу також входить правління, що ухвалює рішення у значних справах, зокрема про штрафи.

На відміну від складу наглядових органів у сфері захисту персональних даних, різні аспекти їхньої незалежності відображено в Конвенції 108+ та ЗРЗД. Пункт 5 статті 15 Конвенції 108+ передбачає, що наглядові органи виконують свої обов'язки та здійснюють свої повноваження повністю незалежним та нейтральним способом. Аналогічні положення містяться в пункті 1 статті 52 ЗРЗД, де також конкретизуються інші аспекти, важливі з погляду незалежного функціонування (функціональна незалежність (члени наглядового органу мають бути захищеними від прямого чи опосередкованого зовнішнього впливу та не звертатися по вказівки і не виконувати вказівок будь-яких інших осіб), а також фінансова та організаційна незалежність).

Місце наглядового органу у сфері захисту персональних даних у системі інших органів державної влади грає важливу роль, бо тісно пов'язане з функціональною незалежністю. Питання зовнішнього впливу особливо гостре та актуальне, якщо члена або членів наглядового органу призначає уряд і, як наслідок, цей орган входить до структури виконавчої влади держави. Втім слід

зазначити, що участь уряду у процесі призначення не виключена. Пункт 1 статті 53 ЗРЗД передбачає, що кожного члена наглядового органу має призначати в порядку прозорої процедури уряд, парламент, голова держави чи незалежний орган, якому доручено здійснити призначення згідно з законодавством держави-члена. Відповідно до пункту 121 преамбули ЗРЗД, «загальні умови призначення членів наглядового органу мають бути визначені в законодавчому порядку в кожній державі-члені; зокрема, вони мають передбачати призначення таких членів на основі прозорої процедури парламентом, урядом або головою держави на підставі пропозиції, внесеної урядом, членом уряду, парламентом або палатою парламенту, або незалежним органом, уповноваженим на це відповідно до законодавства держави-члена». Опитування, проведене групою експертів, виявило існування в європейських країнах процедур призначення в різних поєднаннях. Хоча взаємодія між наглядовим органом у сфері захисту персональних даних та урядом може здаватися проблематичною з погляду незалежності такого органу, опитування показало, що уряд самостійно або спільно з парламентом чи головою держави бере участь у процедурі призначення в багатьох європейських країнах (див. таблицю 1).

Таблиця 1. Призначення складу наглядового органу у сфері захисту персональних даних

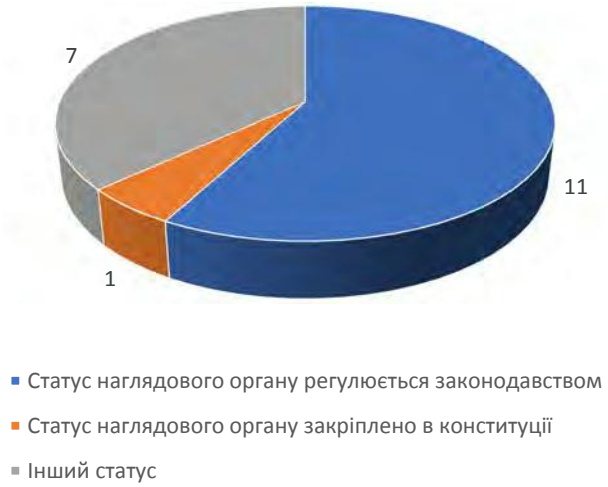
Склад призначає: / Країна	Уряд	Парламент / уряд	Президент / уряд	Парламент або президент / парламент
Австрія			+	
Чеська Республіка				+
Хорватія		+		
Кіпр	+			
Греція				+
Ісландія	+			
Італія				+
Естонія	+			
Латвія	+			
Ліхтенштейн		+		
Литва	+			
Люксембург			+	
Норвегія	+			
Польща				+
Португалія		+		
Румунія				+
Словенія				+
Словаччина		+		

Як показано в таблиці 1, уряд бере участь у процедурі призначення у 12 країнах.

Учасників опитування просили вказати статус наглядового органу: чи він орган виконавчої влади, підпорядкований міністерству; орган виконавчої влади з особливим статусом, закріпленим у законодавстві; орган виконавчої влади, закріплений у конституції; має інший статус. Відповіді засвідчили, що здебільшого статус наглядового органу регулюється законодавством і в одному випадку його статус закріплено в конституції (див. рисунок 1).

Жоден з учасників опитування не зазначив, що наглядовий орган — орган виконавчої влади, підпорядкований міністерству. Це не дивно, бо підпорядкування будь-якому іншому державному

Рисунок 1. Статус наглядового органу з питань захисту персональних даних



органові (необов'язково міністерству) було б порушенням вимоги щодо незалежності. Серед відповідей, що вказували на інший статус, респонденти надали такі варіанти: орган державної влади з власною правосуб'єктністю, автономний і незалежний від інших органів державної влади, а також до будь-яких фізичних чи юридичних осіб приватного сектору; незалежний державний орган (відокремлений від уряду аналогічно до омбудсмана); створений відповідно до конституції незалежний орган державної влади тощо. Можна відзначити, що проголошення незалежного статусу наглядового органу в законодавстві важливе, але недостатнє для забезпечення справжньої незалежності, якщо не створити гарантії щодо виділення ресурсів, можливості самостійно ухвалювати рішення щодо організації власної роботи, захисту від будь-якого зовнішнього впливу тощо.

Учасників опитування просили вказати, чи має наглядовий орган правосуб'єктність; входить до структури іншого органу; підпорядкований міністерству чи іншому державному органові. Значна більшість (18 респондентів) відповіли, що такий орган має правосуб'єктність, а це обов'язкова передумова незалежності, і лише один респондент зазначив, що цей орган підпорядковується міністерству чи іншому державному органові.

За результатами опитування, жоден європейський наглядовий орган у сфері захисту персональних даних не входить до структури іншого органу. Це, знову ж таки, не дивно, бо перебування у структурі іншого органу несумісне з вимогами щодо незалежності. Також варто згадати, що слід уникати не лише перебування у структурі, але й підпорядкування міністерству чи іншому державному органові, бо це може призвести до обмеження інших гарантій, спрямованих на забезпечення незалежного статусу наглядового органу (наприклад, бюджетні процедури, визначення внутрішнього розпорядку та організаційної структури тощо).

Підсумовуючи, члени наглядового органу у сфері захисту персональних даних можуть бути призначені урядом, парламентом, головою держави або за участю кількох з них. Незалежно від того, хто призначає членів наглядового органу, цей орган повинен мати правосуб'єктність і не входити до структури чи бути підпорядкованим міністерству або іншому державному органові.

3.2. Сфера нагляду

Пункт 1 статті 15 Конвенції 108+ передбачає, що для забезпечення дотримання положень Конвенції може бути створено більш ніж один орган. Може існувати потреба в кількох органах з

урахуванням особливостей різних правових систем, наприклад у випадку федеральної держави. Пояснювальна записка містить відповідне роз'яснення: «Також допускається створення спеціальних наглядових органів, чия діяльність обмежуватиметься конкретним сектором (електронними комунікаціями, охороною здоров'я, державним сектором тощо)». Пункт 1 статті 85 ЗРЗД також вимагає від держав-членів зобов'язати один або кілька незалежних органів державної влади вести моніторинг застосування ЗРЗД. З метою забезпечення незалежності судової гілки влади при виконанні своїх судових функцій (зокрема, ухваленні рішень), наглядові органи не мають повноважень вести нагляд за операціями опрацювання даних судами при виконанні своїх обов'язків (див. пункт 10 статті 15 Конвенції 108+, пункт 3 статті 55 ЗРЗД)[2]. Таке обмеження повноважень з нагляду має стосуватися лише діяльності суддів у межах національного законодавства[3]. Отже, слід зазначити, що опрацювання судами інших даних, не пов'язане із здійсненням функцій правосуддя (наприклад, опрацювання персональних даних співробітників, відеоспостереження для цілей безпеки тощо), входить до компетенції наглядового органу у сфері захисту персональних даних.

Особливу увагу слід приділяти наглядові за опрацюванням даних для цілей національної безпеки. Через те що питання національної безпеки виходять за межі дії законодавства Європейського Союзу, дія ЗРЗД не поширюється на опрацювання відповідних даних, і, як наслідок, наглядовий орган не має повноважень вести такий нагляд (див. підпункт a пункту 2 статті 2 ЗРЗД). Втім опрацювання даних, пов'язане з національною безпекою та обороною, повністю не виключено зі сфери дії Конвенції 108+. Що стосується нагляду за опрацюванням даних для цілей національної безпеки та оборони, пункт 3 статті 11 Конвенції 108+ передбачає, що кожна сторона має право, лише в межах необхідності для досягнення цієї мети і пропорційно цій меті в демократичному суспільстві, законодавчо встановити винятки зі сфери дії статті 15, пункту 2, підпунктів a, b, c і d. Пояснювальна записка містить додаткове роз'яснення щодо можливості запровадження інших необхідних механізмів незалежного й ефективного контролю та нагляду за опрацюванням даних для цілей національної безпеки та оборони з дотриманням відповідних вимог щодо незалежності та ефективності механізмів контролю і нагляду (див. пункти 117, 118).

У преамбулі Конвенції 108+ згадується, що право на захист персональних даних має розглядатися у зв'язку з його роллю в суспільстві і що воно має узгоджуватися з іншими правами людини та основними свободами, зокрема свободою вираження поглядів, а також враховувати принцип права на доступ до офіційних документів у ході виконання правил, пов'язаних із захистом персональних даних. Пункт 11 Пояснювальної записки містить зауваження, що право на захист персональних даних не абсолютне і, зокрема, не може бути використане як спосіб завадити доступові громадськості до офіційних документів. Стаття 85 ЗРЗД регулює узгодження права на захист персональних даних з правом на свободу вираження поглядів та свободу інформації, зокрема опрацювання для цілей журналістики та цілей наукової, художньої чи літературної діяльності. У статті 86 ЗРЗД також наголошується на узгодженні публічного доступу до офіційних документів з правом на захист персональних даних.

Слід зазначити, що конкретні повноваження незалежних органів у сфері захисту персональних даних не можуть бути надані іншим наглядовим органам, що не мають такого незалежного статусу і не визнаються в законодавстві Європейського Союзу як органи одного рівня. Дублювання повноважень цих органів також може поставити під загрозу узгодженість наглядової діяльності[4].

2 У пункті 20 преамбули ЗРЗД міститься роз'яснення, що нагляд за операціями опрацювання таких даних може бути доручене спеціальним органам у структурі судової системи держави-члена.

3 Пояснювальна записка, п. 134.

4 Див. Висновок європейського інспектора із захисту даних стосовно пропозиції Комісії (ЄС) щодо Регламенту Європейського парламенту і ради про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку (Регламенту про електронні довірчі послуги), пункт 41. URL: https://edps.europa.eu/sites/default/files/publication/12-09-27_electronic_trust_services_en_0.pdf, станом на 19 квітня 2021 р.

У пункті 2 статті 51 ЗРЗД підкреслюється роль наглядових органів у сприянні послідовному застосуванню цього Регламенту в межах усього Європейського Союзу. Послідовне та комплексне застосування норм про захист даних важливе в контексті співпраці не лише між різними державами, але й між різними галузями в межах однієї держави.

Стаття 41 Директиви (ЄС) 2016/680 про захист фізичних осіб у зв'язку з опрацюванням персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування за скоєння кримінальних злочинів або виконання кримінальних покарань і про вільний рух таких даних, а також скасування Рамкового рішення Ради 2008/977/JHA, допускає, що наглядові органи, створені державами-членами відповідно до ЗРЗД, виступатимуть як наглядові органи, передбачені цією Директивою, і відповідатимуть за виконання завдань такого наглядового органу та контроль за застосуванням цієї Директиви з метою забезпечити захист основних прав і свобод фізичних осіб у зв'язку з опрацюванням даних і сприяти вільному рухові персональних даних у межах Європейського Союзу (див. пункти 1 і 3)[5].

Що стосується ЗРЗД, пункт 1 статті 1 передбачає, що цей Регламент встановлює норми щодо захисту фізичних осіб у зв'язку з опрацюванням персональних даних і норми про вільний рух персональних даних. Отже, також важливо відзначити, що до завдання наглядових органів у сфері захисту персональних даних належить не лише нагляд за дотриманням норм щодо опрацювання персональних даних, але й забезпечення балансу між дотриманням основних прав та інтересами, що вимагають вільний рух персональних даних. Цю подвійну роль підкреслив СЄС у вищезгаданому рішенні від 9 березня 2010 року у справі C-518/07: «Щоб гарантувати такий захист, наглядові органи мають забезпечити баланс між дотриманням основних прав, з одного боку, та інтересами, що вимагають вільний рух персональних даних, — з іншого»[6].

Діяльність наглядових органів у сфері захисту персональних даних має охоплювати всі питання, пов'язані з опрацюванням персональних даних, що регулюються Конвенцією 108+ та ЗРЗД, тому важливо належним чином визначити сферу нагляду за опрацюванням персональних даних у різних секторах та для різних цілей. Що стосується сфери нагляду, результати опитування показали, що в багатьох випадках діяльність наглядових органів у сфері захисту персональних даних охоплює опрацювання персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування за скоєння кримінальних злочинів або виконання кримінальних покарань, а також опрацювання даних для цілей журналістики та наукової, художньої чи літературної діяльності. У п'яти випадках наглядові органи також виконують функції, пов'язані з доступом громадськості до офіційних документів.

Результати опитування виявили, що жоден з наглядових органів у сфері захисту персональних даних не має повноважень вести нагляд за операціями опрацювання даних судами при виконанні їхніх обов'язків.

Підсумовуючи, один і той самий наглядовий орган у сфері захисту персональних даних може відповідати за ведення нагляду за правомірністю опрацювання даних у різних сферах та для різних цілей. Нагляд за операціями опрацювання даних судами при виконанні своїх обов'язків має залишитися за межами його компетенції.

5 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680&from=EN#d1e2779–89–1.

6 Рішення СЄС від 9 березня 2010 року у справі «Європейська комісія проти Федеративної Республіки Німеччини», C-518/07, [2010] ECR I-1885, para. 24.

3.3. Гарантії незалежності

Пункт 5 статті 15 Конвенції 108+ передбачає, що наглядові органи виконують свої обов'язки та здійснюють свої повноваження повністю незалежним і нейтральним способом, при цьому не повинні звертатися по вказівки і не виконувати чужі вказівок. Згідно з Пояснювальною запискою (див. пункт 129), серед елементів, що сприяють забезпеченню незалежності, є такі: склад наглядового органу; спосіб призначення його членів; строк повноважень та умови їх припинення; можливість участі у відповідних нарадах без необґрунтованих обмежень; можливість консультуватися з технічними та іншими експертами або проводити зовнішні консультації; наявність у наглядового органу достатніх ресурсів; можливість наймати власних співробітників; ухвалення рішень без прямого чи опосередкованого зовнішнього втручання (див. пункт 129).

Пункт 1 статті 54 ЗРЗД визначає перелік правил заснування наглядових органів, що мають бути передбачені законодавством:

- заснування кожного наглядового органу;
- кваліфікації та умови прийнятності, необхідні для призначення члена кожного наглядового органу;
- правила і процедури для призначення члена чи членів кожного наглядового органу;
- тривалість строку повноважень члена чи членів кожного наглядового органу становить не менш ніж чотири роки;
- можливість повторного призначення членів кожного наглядового органу та максимальна кількість повторних строків перебування на посаді;
- умови, що регулюють обов'язки члена чи членів і персоналу кожного наглядового органу, заборони на дії, види діяльності та переваги, несумісні з ними протягом і після строку повноважень, і правила, що регулюють припинення зайнятості.

Виділення ресурсів — це ще один фактор, що має визначну роль у забезпеченні незалежності наглядового органу. Пункт 6 статті 15 Конвенції 108+ вимагає забезпечити наглядові органи ресурсами, необхідними для ефективного виконання ними своїх функцій та здійснення повноважень. У пункті 4 статті 52 ЗРЗД наведено детальніший перелік ресурсів із зауваженням, що держави-члени мають забезпечити наглядові органи людськими, технічними і фінансовими ресурсами, приміщеннями та інфраструктурою, необхідними для ефективного виконання ними своїх завдань і здійснення повноважень. Забезпечення належних фінансових, людських, технічних та інших ресурсів — суттєвий аспект незалежності наглядового органу. Невиконання цієї вимоги може серйозно вплинути на його здатність виконувати завдання і здійснювати повноваження.

3.3.1. Строк повноважень членів наглядових органів

Відповідно до пункту 1 статті 54 ЗРЗД, закон має передбачати строк повноважень членів кожного наглядового органу, і цей строк має бути не менше ніж чотири роки (за винятком першого призначення після 24 травня 2016 року, частина якого може становити коротший період, якщо це необхідно для захисту незалежності наглядового органу за допомогою поетапної процедури призначення), а також можливість повторного призначення на посаду і максимальну кількість повторних строків перебування на посаді. СЄС у своєму рішенні від 8 квітня 2014 року у справі «Європейська комісія проти Угорщини» C-288/12 постановив, що з метою забезпечення незалежності наглядового органу [відповідно до підпункту 2 статті 28(1) Директиви 95/46] держава зобов'язана дозволити цьому органові працювати до завершення повного строку його

повноважень[7]. У тому ж рішенні СЄС підкреслив: «Якби кожній державі-члену було дозволено примусити наглядовий орган піти у відставку до завершення повного строку його повноважень всупереч нормам і гарантіям, встановленим у цьому зв'язку відповідним законодавством, загроза такої дострокової відставки, що існувала б протягом усього строку повноважень наглядового органу, могла б підштовхнути його до конформізму з органом державної влади, що несумісно з вимогою щодо його незалежності»[8].

Опитування показало, що строк повноважень наглядових органів варіюється від чотирьох до семи років. Як показано на рисунку 2, здебільшого строк повноважень становить п'ять років.

Рисунок 2. Строк повноважень наглядових органів

Згідно з результатами опитування, у більшості європейських країн дозволяється призначення членів наглядових органів на два повторні строки. У деяких країнах повторне призначення не допускається, тоді як у деяких інших жодного обмеження щодо повторного призначення на посаду не визначено (див. рис. 3).

Рисунок 3. Можливість повторного призначення на посаду

Що стосується того, як поєднуються строк повноважень і повторне призначення на посаду, у європейських країнах не спостерігається чіткої тенденції. Наглядовий орган Італії повідомив, що згідно з законом про зміну строку повноважень інспекторів, яких призначають до певних

7 Рішення СЄС від 8 квітня 2014 року у справі «Європейська комісія проти Угорщини», C-288/12, ECLI:EU:C:2014:237, п. 60.

8 Див. п. 54.

незалежних органів, зокрема членів наглядового органу у сфері захисту персональних даних, був установлений семирічний строк повноважень без можливості поновлення. До цього строк повноважень становив чотири роки і міг бути подовжений один раз. Наглядовий орган Ісландії повідомив, що членів правління призначають на п'ятирічний строк, що може бути подовжений двічі (до п'ятнадцяти років загалом), тоді як інспектора призначають на п'ятирічний строк і його можуть призначити повторно без жодних обмежень.

Підсумовуючи, строк повноважень членів наглядових органів має становити не менше ніж чотири роки. Члени наглядових органів може бути призначені на повторний строк, але можливість повторного призначення не необхідна з погляду забезпечення незалежності.

3.3.2. Припинення повноважень членів наглядових органів

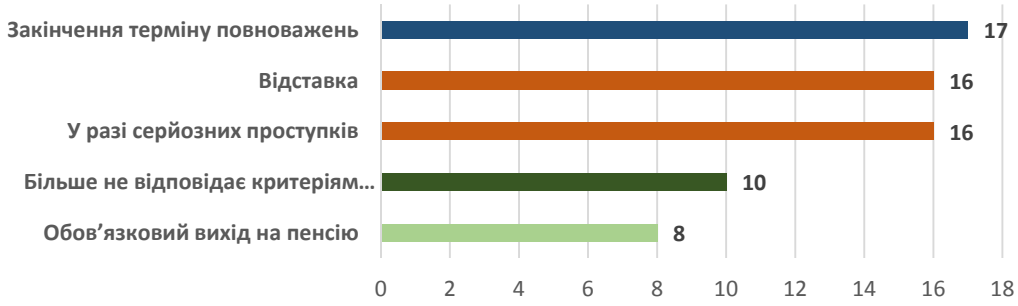
У пунктах 3 і 4 статті 53 ЗРЗД викладено основні норми щодо припинення повноважень членів наглядових органів:

1) Припинення повноважень членів наглядових органів можливе у разі завершення строку повноважень, складення повноважень чи обов'язкового виходу на пенсію згідно з законодавством.

2) Звільнення члена наглядового органу з посади можливе лише у разі серйозного проступку або невідповідності члена до необхідних умов виконання своїх обов'язків.

Підстави для припинення повноважень / звільнення з посади членів наглядових органів, вказані учасниками опитування, зображено на рис. 4.

Рисунок 4. Підстави для припинення повноважень / звільнення з посади членів наглядових органів



Тоді як підстави для припинення повноважень здаються досить об'єктивними, рішення про звільнення з посади може мати суб'єктивніший характер, а тому ставить під загрозу незалежність наглядового органу. Щоб гарантувати захист від необґрунтованого припинення повноважень у разі звільнення з посади члена наглядового органу, необхідні умови виконання обов'язків мають бути чітко передбачені законом. Наприклад, пункт 2 статті 19 Закону Кіпру 125(I) про захист фізичних осіб у зв'язку з опрацюванням персональних даних і вільний рух таких даних 2018 року передбачає, що особа, призначена на посаду інспектора, має відповідати тим самим кваліфікаційним вимогам, що й особа, призначена на посаду судді Верховного суду[9]. Пункт 2 статті 9 Закону Литовської Республіки про правові засади захисту персональних даних передбачає, що директором Державної інспекції із захисту персональних даних може бути призначений громадянин Литовської Республіки, що має бездоганну репутацію, ступінь бакалавра чи магістра права

9 http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf (неофіційний переклад). Станом на 22 травня 2021 р.

або професійну кваліфікацію в галузі права (однорівнева вища освіта) чи щонайменше десять років досвіду роботи або викладання в галузі права та відповідає вимогам, визначеним у пункті 2 статті 53 ЗРЗД[10]. Пункт 4 тієї ж статті зобов'язує директора Державної інспекції із захисту персональних даних припинити членство в політичних партіях на час перебування на посаді.

Також законом має бути передбачений вичерпний перелік видів діяльності, несумісних зі статусом члена наглядового органу. Наприклад, відповідно до пункту 1 статті 12 Закону Грецької Республіки № 4624, не мають права бути призначеними головою, заступником голови або членом наглядового органу особи, що обіймають такі посади: (a) міністр, державний секретар, генеральний або спеціальний секретар міністерства або окремого генерального чи спеціального секретаріату, депутат парламенту; (b) керівник або член керівного органу підприємства, що надає послуги, пов'язані з опрацюванням персональних даних, або має контракт на реалізацію проєкту аналогічного змісту[11]. У п. 2 тієї ж статті зазначено: «Будь-яка професійна чи інша діяльність, що входить до компетенції наглядового органу, несумісна зі статусом члена наглядового органу, за винятком науково-дослідницької діяльності. Члени наглядового органу не мають права виступати в наглядовому органі протягом двох (2) років після завершення строку їхніх повноважень».

Те саме можна сказати про «серйозний проступок»: види таких порушень мають бути чітко визначені. Наприклад, пункт 3 статті 21 Закону Кіпру 125(I) про захист фізичних осіб у зв'язку з опрацюванням персональних даних і вільний рух таких даних 2018 року передбачає звільнення інспектора з посади, коли він, всупереч вимогам Регламенту і цього закону, будь-яким способом оприлюднює інформацію чи персональні дані, доступ до яких отримав при здійсненні посадових обов'язків, або дозволяє їх отримати іншій особі, скоює порушення і в разі визнання його провини карається позбавленням волі на строк до трьох (3) років та/або стягненням штрафу розміром до тридцяти тисяч євро (€30 000). Відповідно до пункту 4 статті 19 того ж закону, підставою для звільнення інспектора з посади служить його неспроможність виконувати свої обов'язки через стан психічного чи фізичного здоров'я або фізичні вади.

Процедура звільнення з посади також важлива, тому має бути передбачена законом, і проводитися вона має за участю тих самих органів, що брали участь у призначенні членів наглядового органу.

Слід зазначити, що дуже важливо мати обмежений і чітко визначений перелік підстав для припинення повноважень / звільнення з посади членів наглядового органу, бо будь-які випадки звільнення від виконання обов'язків до завершення строку повноважень члена наглядового органу може ставити під загрозу незалежність цього органу. СЄС у своєму рішенні від 8 квітня 2014 року у справі «Європейська комісія проти Угорщини» постановив: «<…> Вимога щодо незалежності, викладена в підпункті 2 статті 28(1) Директиви 95/46, обов'язково має тлумачитися як така, що зобов'язує забезпечити можливість для наглядових органів працювати до завершення повного строку повноважень і дозволяє припиняти їхні повноваження до завершення повного строку лише з дотриманням норм і гарантій, передбачених відповідним законодавством (див. пункт 55)»[12].

При виконанні своїх обов'язків члени та співробітники наглядових органів мають доступ до персональних даних, тому особливу увагу необхідно приділяти дотриманню конфіденційності. Пункт 8 статті 15 Конвенції 108+ передбачає, що члени та співробітники наглядових органів зобов'язані дотримуватися конфіденційності щодо конфіденційної інформації, до якої мають або в

10 https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/asr, литовською мовою. Станом на 22 травня 2021 р.
11 https://www.dpa.gr/sites/default/files/2020–08/LAW%204624_2019_EN_TRANSLATED%20BY%20THE%20HDPA.PDF. Станом на 22 травня 2021 року.
12 Рішення СЄС від 8 квітня 2014 року у справі «Європейська комісія проти Угорщини», C-288/12, ECLI:EU:C:2014:237, п. 55.

минулому мали доступ при виконанні своїх обов'язків та здійсненні повноважень. Пункт 2 статті 54 ЗРЗД містить роз'яснення, що обов'язок щодо дотримання професійної таємниці зберігається як протягом, так і після завершення строку повноважень членів і співробітників наглядового органу, а також окремо наголошується, що протягом строку повноважень обов'язок дотримання професійної таємниці особливо стосується повідомлень фізичними особами про порушення ЗРЗД. Порушення обов'язку щодо дотримання конфіденційності може бути підставою для звільнення з посади членів наглядового органу.

Підсумовуючи, вичерпний перелік підстав для припинення повноважень та звільнення з посади членів наглядового органу, а також процедура звільнення з посади мають бути визначені законом, що також має забезпечувати участь у процедурі тих самих органів, що брали участь у призначенні членів наглядового органу. Закон також має чітко визначати кваліфікаційні та інші вимоги для призначення на посаду, заборони ведення діяльності, зокрема професійної, та отримання привілеїв, що несумісні зі статусом члена чи співробітника наглядового органу протягом або після завершення строку повноважень, а також обов'язки членів і співробітників наглядового органу.

3.3.3. Фінансові ресурси

Наявність достатнього бюджету дуже важлива, бо безпосередньо впливає на інші аспекти, якот оплата праці співробітників, власне приміщення, облаштування комунікаційних систем тощо. Хоча Конвенція 108+ прямо не регулює бюджетні процедури[13], пункт 6 статті 52 ЗРЗД передбачає, що кожен наглядовий орган повинен мати окремий річний бюджет, що може бути частиною загального державного чи національного бюджету. Одне з питань, пов'язане з розподілом бюджетних коштів, — те, чи має бюджет наглядового органу бути визначений окремим рядком (статтею) бюджету. СЄС у своєму рішенні від 16 жовтня 2012 року у справі «Європейська комісія проти Республіки Австрії» C-614/10 постановив: «<…> Держави-члени не зобов'язані відтворювати в національному законодавстві норми, аналогічні до норм розділу V Регламенту № 45/2001[14], щоб забезпечити повну незалежність своїх відповідних наглядових органів, а тому можуть передбачити, що, з погляду бюджетного законодавства, наглядові органи підпорядковуватимуться певному департаментові міністерства. Втім виділення таким органам необхідного обладнання і кадрів не має завадити їм діяти «повністю незалежним способом» при здійсненні повноважень, наданих їм відповідно до підпункту 2 статті 28(1) Директиви 95/46»[15]. Хоча визначення бюджету наглядового органу окремим рядком (статтею) бюджету не обов'язкове, обов'язок щодо забезпечення наглядового органу окремим бюджетом залишається в силі. Слід також зазначити, що якщо процедура розподілу бюджетних коштів дозволяє органам виконавчої влади держави справляти вирішальний вплив (наприклад, на етапі обговорення бюджету), це може створити можливість зовнішнього впливу на діяльність наглядового органу.

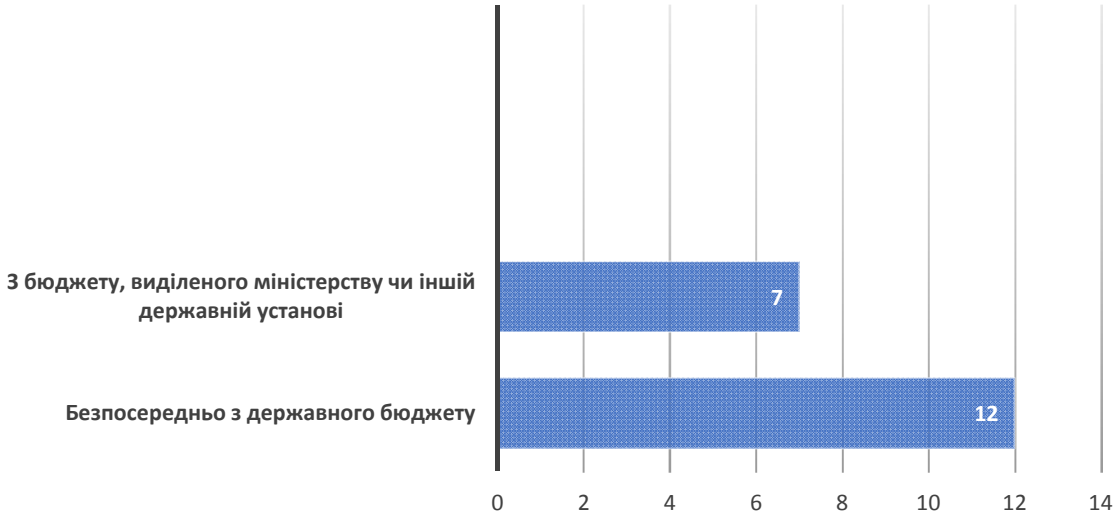
Опитування показало, що наглядові органи отримують фінансові ресурси або безпосередньо з державного бюджету, або з бюджетних коштів, виділених для міністерства чи іншого органу (див. рисунок 5).

13 Варто наголосити, що положення пункту 6 статті 15 Конвенції 108+, що зобов'язують сторони забезпечувати наглядові органи ресурсами, необхідними для ефективного виконання ними своїх функцій і здійснення повноважень, також мають на увазі фінансові ресурси.

14 Пункт 3 статті 43 Регламенту №45/2001 передбачає: «Бюджет [європейського інспектора із захисту даних] має бути визначений окремою статтею бюджету в частині VIII загального бюджету Європейського Союзу». Аналогічна норма міститься в пункті 3 статті 54 Регламенту (ЄС) 2018/1725 про скасування Регламенту № 45/2001: «Бюджет європейського інспектора із захисту даних має бути визначений окремою статтею бюджету в частині, присвяченій адміністративним витратами загального бюджету Європейського Союзу».

15 Див. пункт 58.

Рисунок 5. Виділення фінансових ресурсів наглядовим органам



Деякі респонденти уточнили, що навіть бюджет наглядового органу — частина бюджету іншого органу (наприклад, Міністерства юстиції), проте ресурси, виділені для наглядового органу, визначені окремим рядком бюджету.

Згідно з результатами опитування, окрім державного бюджету, у деяких європейських країнах існують інші джерела фінансування. Втім можна зробити висновок, що така практика не поширена, бо про існування інших джерел повідомили лише двоє респондентів: один із респондентів зазначив, що наглядовий орган у сфері захисту персональних даних отримує кошти від надання платних послуг (як плату за участь у семінарах, організованих наглядовим органом, та кваліфікаційних іспитів для інспекторів із захисту персональних даних), тоді як інший назвав надходження від адміністративних штрафів або інших грошових стягнень, накладених як покарання за порушення. Один із наглядових органів зазначив, що для його фінансування можуть використовуватися інші кошти, отримані законним шляхом.

Варто підкреслити, що поняття «необхідні фінансові ресурси» не однозначне, і що єдиної методології визначення обсягу необхідних фінансових ресурсів не існує. Агентство Європейського Союзу з основоположних прав людини (FRA) у своїй доповіді «Критерії незалежності наглядових органів з питань захисту персональних даних у ЄС» звертає увагу на той факт, що загальний рівень цін і, відповідно, рівень купівельної спроможності євро варіюється між державами — членами ЄС, а тому «в деяких країнах з урахуванням вищого рівня зарплати, вартості ресурсів тощо певна сума коштів дає більші можливості, ніж в інших, у зв'язку з чим будь-які порівняння між державами-членами виявляються викривленими. <...>» (див стор. 16)[16]. FRA зробило спробу порівняти витрати кожного наглядового органу у сфері захисту персональних даних у всіх 28 державах — членах ЄС з урахуванням населення кожної держави, а також з поправкою на коефіцієнт, що враховує купівельну спроможність в усіх державах-членах. Бюджет кожного наглядового органу поділено на цей коефіцієнт, а загальну суму витрат, своєю чергою, поділено на кількість населення держави-члена, що дозволило отримати відносну суму коштів у перерахунку на душу населення, яку виділяють наглядовим органам у сфері захисту персональних даних щороку[17].

16 https://www.asktheeu.org/en/request/2398/response/9765/attach/3/21.FRA%20Focus%20Data%20protection%20authorities%20independence%20funding%20and%20staffing%20ATTACHMENT%20FRA%202013%20Focus%20DPA.pdf . Станом на 24 травня 2021 року.

17 Там само.

Питання, яка сума коштів достатня і має бути виділена, завжди важливе, проте знайти на нього відповідь непросто. Відповідні показники можуть включати рівень зарплати співробітників наглядового органу. Результати опитування показали, що здебільшого вона відповідає середній зарплаті державних службовців / працівників у державному секторі (див. рисунок 6).

Рисунок 6. Рівень зарплати співробітників наглядового органу

Питання, тісно пов'язане з фінансовою незалежністю, — це процедура формування бюджету і можливість впливу з боку уряду чи його органів. У цьому разі важливу роль може грати сам наглядовий орган. Наглядовий орган буде значно більше фінансово незалежним, якщо братиме активнішу участь у формуванні бюджету, особливо в питанні визначення необхідної суми коштів і консультацій у рамках процесу ухвалення рішень. Участь наглядового органу сприятиме забезпеченню бюджетної стабільності та незалежності у процесі ухвалення рішень щодо виділення коштів і дозволить мінімізувати ризик впливу на нього з боку інших державних органів та уряду.

Підсумовуючи, наглядовий орган з питань захисту персональних даних повинен мати окремий державний річний бюджет, що може бути частиною загального державного чи національного бюджету. Наглядовий орган може отримувати фінансування з інших джерел, але обов'язок щодо забезпечення його достатніми ресурсами лежить на державі. Фінансові ресурси мають забезпечуватися належним обсягом, що має дати змогу наглядовому органові бути укомплектованим кваліфікованими кадрами, мати необхідні приміщення, технічне обладнання та інфраструктуру. Ризик зовнішнього впливу на діяльність наглядового органу у процесі розподілу бюджетних коштів може бути значно мінімізований за умови участі наглядового органу у процесі консультацій та ухвалення рішень щодо розподілу коштів.

3.3.4. Людські ресурси

Пункт 5 статті 52 ЗРЗД передбачає обов'язок забезпечити, щоб кожен наглядовий орган мав можливість самостійно набирати співробітників, що підпорядковуватимуться лише членам відповідного наглядового органу. Можливість для наглядового органу самостійно наймати своїх співробітників також підкреслюється в Пояснювальній записці (див. пункт 129). СЄС у своєму рішенні від 16 жовтня 2012 року у справі «Європейська комісія проти Республіки Австрії» C-614/10 постановив, що співробітники наглядового органу з питань захисту персональних даних не мають підпорядковуватися чи бути підконтрольними будь-якому іншому органові з погляду ієрархії та оплати праці, а також дисциплінарного контролю. СЄС підкреслив: «У цьому стосунку слід пам'ятати, що відповідно до пункту 45(1) Закону про державну службу 1979 року безпосередній керівник має широкі повноваження щодо контролю над посадовцями його департаменту. Ця норма дає змогу безпосередньому керівникові не лише забезпечувати виконання співробітниками своїх

завдань відповідно до закону і ефективним та економічним способом, але й скеровувати виконання ними своїх обов'язків, виправляти будь-які помилки та упущення і забезпечувати дотримання робочого графіка, заохочувати службове підвищення співробітників за результатами оцінки ефективності роботи і доручати їм завдання, що оптимально відповідають їхнім спроможностям»[18]. СЄС заперечив проти того, що «<…> ведення такого нагляду з боку держави несумісне з вимогою щодо незалежності наглядових органів у сфері захисту персональних даних, визначеною в підпункті 2 статті 28(1) Директиви 95/46»[19]. У тому ж рішенні СЄС звернув увагу на ризики для незалежності через організаційне дублювання з іншими державними органами у разі, коли члени наглядового органу одночасно беруть участь у їхній роботі: «З огляду на робоче навантаження на наглядовий орган, відповідальний за захист персональних даних, з одного боку, і той факт, що члени Комісії з питань захисту даних виконують свої обов'язки відповідно до пункту 36(3a) Закону про захист даних 2000 року і водночас виконують іншу роботу, — з другого, необхідно визнати, що члени такого органу значною мірою покладаються на співробітників, виділених їм для допомоги у виконанні доручених їм функцій. Той факт, що склад органу утворено з посадовців Федеральної канцелярії, що, своєю чергою, підлягають контролеві з боку Комісії з питань захисту даних, створює ризик впливу на рішення Комісії. У будь-якому разі, таке організаційне дублювання між Комісією з питань захисту даних та Федеральною канцелярією не дає змоги Комісії перебувати поза будь-якими підозрами в упередженості й тому несумісне з вимогою щодо «незалежності», передбаченої підпунктом 2 статті 28(1) Директиви 95/46»[20].

Учасників опитування попросили надати інформацію про статус співробітників, а також повноваження наглядового органу щодо внутрішнього управління (наприклад, рішень про внутрішню структуру органу, кількість та рівень кваліфікації співробітників). Згідно з результатами опитування, у європейських країнах існують різні практики стосовно статусу співробітників наглядового органу: вони можуть мати статус державних службовців, працювати за трудовим договором, можливе також поєднання обох підходів.

Попри статус співробітників наглядового органу, важливо мати гарантії захисту від будь-якого впливу. Наприклад, відповідно до пункту 3 статті 8 Закону про захист персональних даних Литовської Республіки, державні й муніципальні органи та установи, депутати парламенту, інші посадовці, політичні партії, державні організації, інші юридичні та фізичні особи не мають права чинити будь-який політичний, економічний, психологічний чи соціальний тиск або інший неправомірний вплив на Державну інспекцію із захисту персональних даних, її директора, державних службовців та співробітників, що працюють за трудовими договорами. Втручання в діяльність Державної інспекції із захисту персональних даних тягне за собою відповідальність, передбачену законом.

Що стосується внутрішньої структури, кількості та рівня кваліфікації співробітників, то здебільшого наглядові органи мають можливість самостійно ухвалювати рішення про внутрішню структуру органу. Втім, що стосується кількості співробітників, десятеро респондентів зазначили, що існує гранична кількість, встановлена законодавством (див. рисунок 7).

Незалежність наглядового органу посилюється, якщо він має повноваження самостійно призначати і керувати своїми співробітниками без зовнішнього впливу під час їх добору. Окрім наявності необхідних фінансових ресурсів, важливо мати можливість самостійно ухвалювати рішення, що визначають необхідну кількість співробітників, і наймати достатньо кваліфіковані кадри з різних галузей, здатні використати свій фаховий досвід з усіх аспектів роботи наглядового органу

18 Рішення СЄС від 16 жовтня 2012 року у справі «Європейська комісія проти Республіки Австрії», C-614/10, ECLI:EU:C:2012:631, п. 49.

19 Там само, п. 59.

20 Там само, п. 61.

Рисунок 7. Рішення щодо внутрішньої структури, кількості та кваліфікації персоналу

(наприклад, права, інформаційних та комунікаційних технологій тощо). Необхідно забезпечити справедливість і прозорість процесу набору кадрів як гарантію незалежності.

Хоча законодавче обмеження кількості співробітників наглядового органу не рідкість у європейських країнах, слід зазначити, що воно може негативно позначитися на спроможності належним чином виконувати свої завдання. Регламентування кількості персоналу може створити ситуацію, коли, навіть маючи достатні фінансові ресурси, наглядовий орган буде не в змозі наймати співробітників.

Також варто підкреслити, що важливий чинник спроможності співробітників належним чином виконувати свої завдання — підготовленість, тож наглядовому органові мають бути надані достатні ресурси для організації навчання у відповідних сферах. Належне навчання особливо важливе, враховуючи швидкий характер змін, що впливають на роботу співробітників.

Підсумовуючи, наглядовий орган повинен мати можливість самостійно добирати і наймати своїх співробітників, що підпорядковуватимуться тільки членам наглядового органу. Слід уникати встановлення іншими органами обмежень на кількість співробітників наглядового органу. Будь-яке організаційне дублювання між наглядовим органом у сфері захисту персональних даних та будь-яким іншим державним органом не дає змоги наглядовому органові бути поза підозрами в упередженості й тому несумісне з вимогою щодо незалежності.

3.4. Інші гарантії захисту від зовнішнього впливу

3.4.1. Гарантії захисту від контролю над внутрішньою діяльністю і використанням ресурсів

Вирішальне значення для забезпечення незалежності наглядового органу з питань захисту персональних даних має не лише виділення достатніх ресурсів, а й також можливість самостійного використання цих ресурсів і планування власної діяльності. Група експертів намагалася дізнатися, яким чином таку автономію реалізовано в європейських країнах, і попросила учасників опитування надати інформацію про використання виділеного бюджету (наприклад, чи вимагаються

попередні дозвіл / схвалення / консультації з боку інших державних органів), затвердження внутрішньої структури наглядового органу, рішення щодо кількості та кваліфікації співробітників, а також планування діяльності. Результати опитування представлено нижче (див. рисунок 8).

Рисунок 8. Автономія у використанні ресурсів та плануванні діяльності

Згідно з результатами опитування, слід також зазначити, що наглядові органи мають повну автономію у плануванні діяльності, бо жоден з респондентів не зазначив, що плани роботи підлягають оцінюванню, узгодженню та затвердженню іншими органами.

Автономія у використанні ресурсів не означає неможливості жодного виду контролю. Пункт 118 преамбули ЗРЗД містить роз'яснення, що незалежність наглядових органів не означає, що наглядові органи не можуть підлягати контролеві чи моніторингові фінансових витрат або судовому наглядові. Пункт 6 статті 52 ЗРЗД зобов'язує держави — члени ЄС забезпечити, щоб такий фінансовий контроль не впливав на незалежність наглядового органу.

Наглядовий орган у сфері захисту персональних даних має вести свою діяльність повністю незалежним способом, без жодного зовнішнього впливу з будь-чийого боку, зокрема з боку органів, над якими він веде нагляд, а також з боку держави. Це чітко зазначено СЄС у рішенні від 9 березня 2010 року у справі «Європейська комісія проти Федеративної Республіки Німеччини» C-518/07, у якому СЄС зауважив, що державний контроль у будь-якій формі загалом дозволяє урядові відповідної федеральної землі або адміністративному органові, підпорядкованому цьому урядові, прямим чи непрямим чином впливати на рішення наглядових органів або навіть скасовувати і заміняти ці рішення[21]. СЄС не підтримав позицію Федеративної Республіки Німеччини на тій підставі, що вимога «повної незалежності» передбачає функціональну незалежність наглядових органів у тому розумінні, що ці органи мають бути незалежними від органів поза державним сектором, над якими вони ведуть нагляд, і не зазнавати зовнішнього впливу, а також що державний контроль у федеральних землях Німеччини не такий зовнішній вплив, а урядовий механізм внутрішнього моніторингу, що застосовують державні органи, які входять до складу того ж адміністративного апарату, що й наглядові органи, і, як і наглядові органи, відповідають за виконання завдань Директиви 95/46[22]. Попри аргументи Федеральної Республіки Німеччини, що держава лише прагне гарантувати, щоб акти наглядового органу відповідали нормам національного законодавства та законодавства ЄС, і що вона, отже, не має на меті потенційно зобов'язати такі органи виконувати політичні завдання, що несумісні із захистом фізичних осіб у зв'язку з опрацю-

21 Рішення СЄС від 9 березня 2010 року у справі «Європейська комісія проти Федеративної Республіки Німеччини» C-518/07, ECLI:EU:C:2010:125, п. 32.

22 Там само, п. 16.

ванням персональних даних та їхніх основних прав, СЄС постановив, що державний контроль над наглядовими органами Німеччини, відповідальними за ведення нагляду за опрацюванням персональних даних за межами державного сектору, несумісний з вимогою щодо незалежності, визначеною в пункті 30 цього судового рішення[23].

Втім незалежність наглядового органу не означає, що його рішення не підлягають оскарженню. У разі, коли адміністративне рішення має правові наслідки, кожна особа, на яку поширюється дія цього рішення, має право на ефективний судовий захист згідно з відповідним національним законодавством. Серед таких осіб можуть бути суб'єкти даних, контролери даних, оператори даних, а також треті сторони. Пункт 9 статті 15 Конвенції 108+ передбачає, що рішення наглядового органу може бути оскаржене в суді. Відповідно до статті 78 ЗРЗД, окрім будь-яких інших засобів адміністративного чи несудового захисту, кожна фізична чи юридична особа у разі ухвалення щодо них наглядовим органом рішення зобов'язального характеру має право на ефективний судовий захист. Суб'єкт даних має право на ефективний судовий захист у разі, якщо наглядовий орган залишає без розгляду його скаргу або протягом трьох місяців не інформує суб'єкта даних про хід чи результат розгляду скарги.

Згідно з результатами опитування, більшість учасників зазначила, що рішення наглядових органів у сфері захисту персональних даних можуть бути оскаржені в суді відповідно до законодавства держави-члена (див. рисунок 9).

Рисунок 9. Оскарження рішень наглядового органу

Наглядовий орган Хорватії уточнив, що рішення наглядового органу жодним чином не підлягають апеляції, але за скаргою до компетентного адміністративного суду проти них може бути порушена адміністративна справа. Наглядовий орган Греції зазначив, що рішення можна оскаржити до Державної ради[24].

Троє респондентів зазначили, що рішення може бути оскаржене до вищого адміністративного органу чи установи.

23 Там само, пункти 33, 37.

24 За загальнодоступною інформацією, Державна рада виконує функції Верховного адміністративного суду Греції. http://www.adjustice.gr/webcenter/portal/SteEn/Home?_afrLoop=4467481217124692#!%40%40%3F_afrLoop%3D4467481217124692%26centerWidth%3D100%2525%26showHeader%3Dtrue%26_adf.ctrl-state%3Dtc3p6uucc_4, станом на 5 липня 2021 року.

Підсумовуючи, наглядовий орган повинен мати автономію в питаннях використання ресурсів і планування своєї діяльності й не підлягати зовнішньому контролеві — прямому чи опосередкованому. Втім фінансовий контроль, що ведеться відповідно до закону і не впливає на незалежність наглядового органу, допустимий. Оскарження рішень наглядового органу має відповідати принципові верховенства права. Кожна особа, на яку поширюється рішення наглядового органу, повинна мати можливість оскаржувати такі рішення до суду.

3.4.2. Законодавчі акти парламенту як гарантія захисту від зовнішнього впливу

Визначення структури і статусу наглядового органу, а також врегулювання аспектів, пов'язаних з його незалежністю, у законі чи іншому законодавчому акті, ухваленому парламентом, особливо важливе для забезпечення його стабільного функціонування. Група експертів спробувала дослідити, яка практика існує в європейських країнах, і які з зазначених нижче аспектів врегульовані законодавчими актами, ухваленими парламентом:

- призначення керівника / членів наглядового органу;
- кваліфікаційні та інші вимоги для призначення на посаду керівника / члена наглядового органу;
- строк повноважень керівника / членів наглядового органу;
- підстави для звільнення з посади керівника / членів наглядового органу;
- порядок звільнення з посади керівника / членів наглядового органу;
- бюджетні (фінансові) процедури;
- кадрова політика (наприклад, право самостійно наймати співробітників тощо);
- заробітна платна керівника / членів наглядового органу.

Шестеро учасників опитування вказали, що все вищезазначене регулюється законодавчими актами, ухваленими парламентом. Майже всі учасники відповіли, що законодавчі акти, ухвалені парламентом, визначають порядок призначення керівника / членів наглядових органів, кваліфікаційні та інші вимоги для призначення на посаду керівника / членів наглядових органів, а також строк повноважень керівника / членів наглядових органів. Співвідношення варіантів відповідей представлено на рисунку 10.

Рисунок 10. Аспекти, регульовані законодавчим актом, прийнятим парламентом

Підсумовуючи, законодавчі акти, ухвалені парламентом, служать потужною гарантією, що забезпечує незалежність наглядових органів. Такі законодавчі акти мають регулювати аспекти, що стосуються незалежності, як-от порядок призначення членів наглядових органів, кваліфікаційні та інші вимоги для призначення членів наглядових органів, строк повноважень членів наглядових органів, підстави для припинення повноважень і звільнення з посади, бюджетні процедури, заробітна плата членів наглядових органів, автономія в питаннях кадрової політики і планування діяльності.

3.4.3. Гарантії захисту від політичного впливу

Слід зазначити, що функціональна незалежність наглядових органів (нема необхідності керуватися будь-якими вказівками при виконанні своїх обов'язків) суттєва, але сама по собі недостатня умова для захисту від зовнішнього впливу. Це чітко зазначив СЄС у рішенні від 16 жовтня 2012 року у справі «Європейська комісія проти Республіки Австрії» C-614/10: «Слід визнати, той факт, що Комісія з питань захисту даних функціонально незалежна, бо, відповідно до пункту 37(1) Закону про державну службу 2000 року, її члени «діють незалежним способом і [не] зв'язані жодними вказівками при виконанні своїх обов'язків», — необхідна умова дотримання цим органом критерію незалежності, передбаченої підпунктом 2 статті 28(1) Директиви 95/46. Втім, всупереч позиції Республіки Австрії, така функціональна незалежність сама по собі не достатня гарантія захисту наглядового органу від будь-якого зовнішнього впливу»[25].

Політичний вплив може набувати різних форм. СЄС у своєму рішенні від 8 квітня 2014 року у справі «Європейська комісія проти Угорщини» постановив: "<…> сам лише ризик, що держава в рамках контролю над державними органами може справляти політичний вплив на рішення наглядового органу, достатній для того, щоб завадити останньому виконувати свої обов'язки незалежним способом. По-перше, існує можливість «конформізму» з боку таких органів у світлі практики ухвалення рішень органу, що веде контроль. По-друге, з огляду на роль таких органів у забезпеченні захисту права на недоторканність приватного життя, підпункт 2 статті 28(1) Директиви 95/46 містить вимоги, згідно з якими їхні рішення — а отже й самі органи — мають залишатися поза будь-якими підозрами в упередженості»[26]. Ба більше, з практики СЄС випливає, що реструктуризація або видозміна організаційної моделі мають відбуватися з дотриманням вимоги щодо незалежності, передбаченої відповідним законодавством (тобто не допускати дострокового припинення повноважень раніше призначених членів наглядового органу).

Пункт 4 статті 53 ЗРЗД передбачає, що кожен член наглядового органу повинен мати кваліфікацію, досвід і вміння, особливо у сфері захисту персональних даних, необхідні для виконання своїх обов'язків і здійснення повноважень, тобто можливість призначення на посаду члена наглядового органу залежить від професійної кваліфікації і досвіду. Очевидно, політичні чи інші переконання, членство в тій чи тій політичній партії та інші подібні умови не можуть бути підставою для призначення або звільнення з посади члена наглядового органу. З цієї причини початок строку повноважень членів наглядового органу не має бути пов'язаний зі строком повноважень органу призначення (за винятком збігу в часі).

Підсумовуючи, регулювання статусу наглядового органу загалом має забезпечувати його незалежність від політичного впливові. Щоб запобігти політичному впливу, початок і завершення строку повноважень членів наглядового органу не мають бути пов'язані зі строком повноважень

25 Рішення СЄС від 16 жовтня 2012 року у справі «Європейська комісія проти Республіки Австрії», C-614/10, ECLI:EU:C:2012:631, п. 42.

26 Рішення СЄС від 8 квітня 2014 року у справі «Європейська комісія проти Угорщини», C-288/12, ECLI:EU:C:2014:237, п. 53. Див. також рішення у справі «Європейська комісія проти Німеччини» EU:C:2010:125, п. 36, та «Європейська комісія проти Австрії» EU:C:2012:631, п. 52.

органу призначення (уряду, парламенту, голови держави). Політичні чи інші переконання не повинні грати жодної ролі у процесі призначення чи звільнення з посади члена наглядового органу. Повноваження члена наглядового органу не може бути припинене достроково, крім як на підставах, передбачених законом.

4

ПОВНОВАЖЕННЯ ЩОДО ПРОВЕДЕННЯ РОЗСЛІДУВАНЬ, ВЖИТТЯ ЗАХОДІВ, РОЗГЛЯДУ СКАРГ І РЕГУЛЯТОРНІ ПОВНОВАЖЕННЯ

4.1. Повноваження, якими наділені органи згідно з Конвенцією 108+

Стаття 15 Конвенції 108+ визначає потребу в створенні органів, наділених такими повноваженнями:

- проведення розслідувань та вжиття заходів;
- виконання функцій, що стосуються передавання даних, передбачених статтею 14, зокрема затвердження стандартних гарантій;
- ухвалювати рішення щодо порушень положень цієї Конвенції та можуть, зокрема, притягати до адміністративної відповідальності;
- брати участь у судовому розгляді або доводити до відома компетентних судових органів інформацію про порушення положень Конвенції 108+;
- надавати консультації щодо пропозицій стосовно будь-яких законодавчих чи адміністративних заходів, які передбачають обробку персональних даних;
- розглядати запити та скарги, подані суб'єктами даних щодо їхніх прав на захист даних, та інформувати суб'єктів даних про результати їх розгляду;
- діяти незалежно та неупереджено під час виконання своїх обов'язків та здійснення своїх повноважень і водночас не просити та не виконувати вказівок.

4.2. Повноваження, якими наділені органи згідно з ЗРЗД

Згідно з пунктом 129 преамбули Регламенту 2016/679, наглядові органи повинні мати в кожній державі-члені однакові завдання та реальні повноваження, зокрема повноваження щодо проведення розслідувань, нагляду, а також дозвільні та консультативні повноваження.

Повноваження на розслідування

Виправні повноваження

Дозвільні та консультативні повноваження

Стаття 58 ЗРЗД визначає, якими повноваженнями наділяється національний наглядовий орган, а саме:

Повноваження щодо проведення розслідувань:

(a) видавати розпорядження контролерові або операторові, у разі необхідності, представникові контролера або оператора надати будь-яку інформацію, яку він вимагає для виконання своїх завдань;

(b) проводити розслідування у формі перевірок захисту даних;

(c) переглядати сертифікації, видані згідно зі статтею 42(7);

(d) повідомляти контролера або оператора про передбачуване порушення цього Регламенту;

(e) отримувати, від контролера або оператора, доступ до всіх персональних даних і до всієї інформації, необхідної для виконання його завдань;

(f) отримувати доступ до будь-яких приміщень контролера або оператора, зокрема до будь-якого обладнання і засобів опрацювання даних згідно з процесуальним законодавством Союзу чи держави-члена.

Повноваження щодо нагляду:

(a) надсилати попередження контролерові або операторові про те, що призначені операції опрацювання ймовірно порушать положення цього Регламенту;

(b) виносити догану контролерові або операторові, якщо операції опрацювання порушують положення цього Регламенту;

(c) наказувати контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до цього Регламенту;

(d) наказувати контролерові або операторові увідповіднити операції опрацювання положенням цього Регламенту, у разі необхідності, у встановленому порядку та протягом встановленого періоду;

(e) наказувати контролерові повідомити суб'єкта даних про порушення захисту персональних даних;

(f) накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання.

(g) наказувати виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17, 18 , і нотифікувати про такі дії кожного одержувача, якому були розкриті персональні дані відповідно до статті 17 (2) і статті 19;

(h) відкликати сертифікацію чи наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються;

(i) накладати адміністративні штрафи відповідно до статті 83 як доповнення до, чи замість заходів, вказаних у цьому параграфі, залежно від обставин кожної індивідуальної справи;

(j) наказувати призупинити потоки даних до одержувача в третій країні чи до міжнародної організації.

Повноваження дозвільного та консультативного характеру:

(a) консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36;

(b) видавати, з власної ініціативи чи на запит, висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних;

(c) надавати дозвіл на опрацювання, вказане в статті 36(5), якщо законодавство держави-члена вимагає надання такого попереднього дозволу;

(d) надавати висновок і затверджувати проєкти кодексів поведінки відповідно до статті 40(5);

(e) надавати акредитацію органам сертифікації відповідно до статті 43;

(f) видавати сертифікації та затверджувати критерії сертифікації відповідно до статті 42(5);

(g) ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пунктів (d) статті 46(2);

(h) надавати дозвіл на договірні положення, вказані в пункті (a) статті 46(3);

(i) надавати дозвіл на адміністративні домовленості, вказані в пункті (b) статті 46(3);

(j) затверджувати зобов'язальні корпоративні правила відповідно до статті 47.

4.3. Сфера компетенції наглядових органів

Обсяг повноважень може бути ширшим, ніж це визначено в ЗРЗД.

Умови застосування Закону «Про захист персональних даних» Естонії та ЗРЗД закріплені статтею 2 цього закону.

Латвійська інспекція лише частково відповідає за обробку даних для журналістських цілей.

Відповідно до статті 36 Закону «Про імплементацію Загального регламенту про захист даних» ОЗПД Хорватії уповноважує співробітників агентства самостійно, а в окремих випадках також за участю представника наглядового органу (далі – уповноважені особи), проводити планові та позапланові перевірки. Особа, щодо якої ведеться перевірка, та контролер або оператор повідомляються про проведення позапланової перевірки на об'єкті та під час перевірки.

Наглядовий орган Республіки Кіпру, уповноважений вести контроль за доступом громадськості до офіційних документів, — уповноважений з питань інформації. Завдання та повноваження, покладені на нього, виконує відповідний уповноважений з питань захисту персональних даних.

Законодавство Італії визначає додаткові сфери в розділі «Положення, що застосовуються до обробки, яка необхідна для дотримання юридичних зобов'язань або для виконання завдання, що виконується в інтересах суспільства, або для здійснення офіційних повноважень та обробки, про яку йдеться в розділі IX регламенту»: юридичні інформаційні послуги, операції з обробки, які виконують поліція, органи із забезпечення реалізації державної політики у сфері оборони та безпеки, операції з обробки в державному секторі (державні реєстри та професійні реєстри), обробка персональних даних у секторі охорони здоров'я, освіти (обробка даних, що стосуються

осіб, які навчаються), обробка для архівних цілей в інтересах суспільства або для проведення історичних досліджень, обробка для статистичних цілей або проведення наукових досліджень, обробка даних трудових відносин між працівниками та роботодавцями, дистанційний нагляд, дистанційна робота, комітети з питань надання допомоги та органи соціального забезпечення, послуги електронного зв'язку.

Окрім повноважень, передбачених статтею 57 ЗРЗД, Інспекція з захисту даних Естонії уповноважена:

1) підвищувати обізнаність та розуміння громадськістю, контролерами та операторами, пов'язаними з обробкою персональних даних, стандартів, гарантій, а також прав, пов'язаних з обробкою персональних даних; Інспекція з захисту даних Естонії може надавати рекомендації щодо виконання цієї функції;

2) надавати суб'єктам даних на запит інформацію про реалізацію прав, що випливають із цього закону, і, в окремих випадках, співпрацювати з цією метою з наглядовими органами інших держав — членів Європейського Союзу;

3) у разі необхідності, розпочати провадження у справі про адміністративне правопорушення та призначити покарання, якщо інші адміністративні заходи не дають змоги забезпечити дотримання вимог, передбачених законом або Регламентом (ЄС) 2016/679 Європейського парламенту та Ради;

4) співпрацювати з міжнародними організаціями з нагляду за захистом даних та іншими органами нагляду за захистом даних, а також з іншими компетентними іноземними органами та особами;

5) відстежувати відповідні зміни тією мірою, якою вони впливають на захист персональних даних, зокрема на розвиток інформаційно-комунікаційних технологій;

6) надавати консультації з питань обробки персональних даних, про які йде мова в пункті 39 цього закону;

7) брати участь у роботі Європейської ради із захисту персональних даних;

8) застосовувати заходи адміністративного примусу з підстав, обсягом та в порядку, передбаченому законами;

9) з власної ініціативи або на запит надавати висновки з питань захисту персональних даних парламентові, урядові, канцлерові юстиції, іншим установам та громадськості;

10) виконувати інші обов'язки, що випливають із законів.

4.4. Органи, уповноважені проводити розслідування

Загалом усі органи мають широке коло повноважень, визначених ЗРЗД, а також додаткові повноваження, як передбачено статтею 58(6)[27].

Водночас працівники ОЗПД повинні мати доступ до приміщень у порядку, встановленому кримінально-процесуальним законодавством, і залучати за потреби правоохоронні органи.

27 https://www.dataprotection.ro/servlet/ViewDocument?id=172.

Наприклад, діяльність румунського наглядового органу щодо ведення контролю регулюється підрозділом 1 розділу IV закону № 102/2005 із відповідними змінами. Стаття 14(2) закону № 102/2005 передбачає, що співробітники, які виконують функцію контролю, мають право проводити розслідування, зокрема без попереднього повідомлення, запитувати та отримувати від контролера та оператора обробки даних, а також, у разі необхідності, від їхніх працівників, на місці та/або за встановлений термін, будь-яку інформацію та документи, незалежно від носія інформації, робити з них копії, мати доступ до будь-якого приміщення контролера та оператора, а також мати доступ та перевіряти будь-яке обладнання, носії інформації або дані, необхідні для проведення розслідування. Пункт 3 тієї ж статті передбачає, що якщо співробітники, які здійснюють функцію контролю, будь-яким чином перешкоджають у виконанні завдань, передбачених пунктом 2, національний наглядовий орган може вимагати судового дозволу, який видає голова Апеляційного суду м. Бухареста або уповноважений ним суддя. До того ж ідентифікація та збереження предметів, а також опечатування проводиться відповідно до положень закону № 135/2010 «Про Кримінально-процесуальний кодекс» з подальшими змінами та доповненнями. Водночас наглядовий орган Румунії може ухвалити рішення про проведення експертизи та заслуховування осіб, заяви яких вважаються важливими та необхідними для проведення розслідування.

ОЗПД Італії дає посилання на закон, що визначає його повноваження: «Щоб правильно відповісти на запитання, ми вважаємо за краще не позначати окремі відповіді (бо вони можуть лише частково відображати повноваження ОЗПД Італії), а послатися на статтю 158 Закону про захист персональних даних Італії»[28].

Слід зазначити, що закон посилається на статтю 58 Регламенту як таку, що визначає повноваження та додатково розширює їх завдяки процесуальним заходам, які сприяють реалізації повноважень. Відповідно, ми можемо дійти висновку, що повноваження органу загалом збігаються з тими, що передбачені в ЗРЗД. Цікаво також додатково визначити завдання цього органу у зв'язку з завданнями, визначеними іншими європейськими нормативними актами, разом з виконанням повноважень та завдань, передбачених Конвенцією 108+.

Пункт 154

1. На додаток до положень, які містяться в конкретних нормативних актах, а також у підрозділі II розділу VI Регламенту та статті 57(1) пункт «v» зазначеного Регламенту, гарант [Garante] з власної ініціативи та за підтримкою бюро відповідно до чинного законодавства стосовно одного або кількох контролерів:

    a) перевіряє, чи операції з обробки даних виконуються відповідно до чинних законів та підзаконних нормативно-правових актів;

    b) розглядає скарги, подані відповідно до регламенту та положень цього кодексу, зокрема шляхом встановлення відповідних правил у своєму регламенті та встановлення пріоритетних питань, що щорічно виникають у зв'язку з такими скаргами і які згодом можуть стати предметом розслідувань протягом відповідного року;

    c) заохочує ухвалення правил етичної поведінки у випадках, передбачених підрозділом 2-c;

    d) повідомляє про факти та/або обставини, що становлять зміст кримінального правопорушення, скоєного посадовою особою, про що йому стало відомо або під час виконання своїх функцій, або у зв'язку з ними;

28 https://www.garanteprivacy.it/data-protection-code.

e) надсилає парламентові та урядові щорічний звіт, складений відповідно до статті 59 регламенту, до 31 травня року, наступного за роком, за який складається звіт;

f) забезпечує захист основних прав і свобод фізичних осіб шляхом імплементації регламенту та цього кодексу, коли того вимагають обставини;

g) виконує такі завдання, які покладені на нього законодавством Союзу або держави, та виконує такі додаткові функції, що передбачені внутрішнім законодавством.

2. Відповідно до пункту 1 гарант також виконує наглядові функції або функції з надання допомоги у зв'язку обробкою персональних даних, як це передбачено законами про ратифікацію міжнародних угод та конвенцій або іншими нормативно-правовими актами Співтовариства або ЄС; особлива увага приділяється такому:

a) Регламент (ЄС) № 1987/2006 Європейського парламенту та Ради від 20 грудня 2006 року про створення, функціонування та використання Шенгенської інформаційної системи другого покоління (SIS II) та рішення Ради 2007/533/JHA від 12 червня 2007 року про створення, функціонування та використання Шенгенської інформаційної системи другого покоління (SIS II);

b) Регламент (ЄС) 2016/794 Європейського парламенту та Ради від 11 травня 2016 року про Агентство Європейського Союзу зі співробітництва у правоохоронній сфері (Європол) та заміну і скасування рішень Ради 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA та 2009/968/JHA;

c) Регламент (ЄС) 2015/1525 Європейського парламенту та Ради від 9 вересня 2015 року про внесення змін до Регламенту Ради (ЄС) № 515/97 про взаємодопомогу між адміністративними органами держав-членів та співпрацю між ними та Комісією для забезпечення правильного застосування законодавства з митних та аграрних питань зі змінами, внесеними розділом 4(1) законодавчого декрету № 109/2008 (імплементаційна директива 2006/24/ЄС) та рішення Ради 2009/917/JHA від 30 листопада 2009 року про використання інформаційних технологій для митних цілей;

d) Регламент (ЄС) № 603/2013 Європейського парламенту та Ради від 26 червня 2013 року про створення системи «Євродак» для ідентифікації за відбитками пальців для ефективного застосування регламенту (ЄС) № 604/2013 про встановлення критеріїв та механізмів визначення держави-члена, відповідальної за розгляд клопотання про міжнародний захист, поданого в одній із держав-членів громадянином третьої країни або особою без громадянства, а також запитів про порівняння даних системи «Євродак» правоохоронними органами держав-членів та Європолом для правопорядку та внесення змін до Регламенту (ЄС) № 1077/2011 про створення Агентства Європейського Союзу з оперативного керування масштабними інформаційними системами у сфері свободи, безпеки та правосуддя;

e) Регламент (ЄС) № 767/2008 Європейського парламенту та Ради від 9 липня 2008 року щодо візової інформаційної системи (VIS) та обміну даними між державами — членами ЄС щодо короткострокових віз (Регламент VIS) та рішення Ради 2008/633/JHA від 23 червня 2008 року про доступ уповноважених органів держав-членів та Європолу до візової інформаційної системи (VIS) з метою запобігання, виявлення та розслідування терористичних злочинів та інших тяжких злочинів;

f) Регламент (ЄС) № 1024/2012 Європейського парламенту та Ради від 25 жовтня 2012 року про адміністративну співпрацю через інформаційну систему внутрішнього ринку та скасування рішення Комісії 2008/49/ЄС («Регламент про IMI»);

g) розділ IV Конвенції № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних, ухваленої у Страсбурзі 28 січня 1981 року та введеної в дію законом № 98 від 21 лютого 1989 року, визначає орган для міждержавного співробітництва відповідно до статті 13 зазначеної Конвенції.

3. Будь-які питання, не врегульовані регламентом чи цим кодексом, регулює гарант шляхом встановлення власних правил на підставі розділу 156(3), і вони стосуються конкретних заходів, пов'язаних із виконанням завдань або здійсненням повноважень, покладених на нього регламентом або цим кодексом.

4. Гарант співпрацює з іншими національними незалежними адміністративними органами для виконання відповідних завдань.

5. З урахуванням стисліших строків, які можуть бути встановлені законом, гарант надає висновок протягом сорока п'яти днів після отримання відповідного запиту, разом з запитами, згаданими у статті 36(4) регламенту. Після спливу цього строку адміністративний орган, який направив запит, може продовжити діяльність незалежно від отримання висновку гаранта. Якщо строк, зазначений у цьому пункті, не може бути дотриманий через обмеження, пов'язані з підготуванням справи, перебіг строку може бути призупинений лише одноразово, і висновок має бути остаточно підготовлений протягом двадцяти днів після отримання інформації від відповідних адміністративних органів, залучених до підготування справи.

6. Копія документа про вжиття судом будь-якого заходу, застосованого на підставі цього кодексу або у зв'язку зі скоєнням комп'ютерних злочинів, надсилає гарантові канцелярія суду.

7. Гарант не орган, уповноваженим вести нагляд за обробкою даних, що проводять судові органи у зв'язку з виконанням ними судових функцій».

Відповідно, ОЗПД може мати інші повноваження, які доповнюють повноваження, передбачені ЗРЗД, але не суперечать йому.

ОЗПД Республіки Кіпру також заявив, що він має додаткові повноваження як наглядовий орган з питань захисту даних, визначені, зокрема, статтею 25(d) закону 125(I)/2018. «Під час здійснення повноважень з проведення розслідування уповноважений може вилучати документи або електронні пристрої на підставі ордеру на обшук відповідно до положень Кримінально-процесуального закону»[29].

ОЗПД Греції проводить у зв'язку з виконанням закріплених за ним повноважень або на підставі скарги розслідування та перевірки, під час яких ведеться контроль за технологічною інфраструктурою та іншими автоматизованими чи неавтоматизованими засобами, що забезпечують обробку персональних даних. Під час проведення таких розслідувань та перевірок відомство має право отримувати від контролера та оператора доступ до всіх оброблених персональних даних та до всієї інформації, необхідної для цілей таких перевірок та виконання своїх завдань, і конфіденційність інформації незалежно від її категорії не може бути підставою для відмови в її наданні. Орган не має доступу до даних, що ідентифікують помічників чи співробітників, які працюють в організаціях, що згадуються в документах, які зберігаються для цілей національної безпеки або розслідування особливо тяжких злочинів.

2) ОЗПД також:

29 http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf.

(a) видає попередження контролерові або операторові;

(b) вимагає від контролера або оператора виконувати положення законодавства про захист даних визначеним способом та в установлений строк, зокрема шляхом видачі припису про зобов'язання виправити чи видалити персональні дані;

(c) видає приписи та накладає тимчасове або постійне обмеження або навіть заборону на обробку персональних даних;

(d) видає приписи та вимагає надання документів, систем збереження інформації, обладнання або засобів для обробки персональних даних, а також їх змісту;

(e) вилучає документи, інформацію, системи збереження інформації кожної одиниці обладнання та засобу порушення недоторканності персональних даних, а також їхній зміст, які стали відомими відомству під час здійснення ним своїх наглядових повноважень.

Орган конфіскує вищезазначені матеріали до ухвалення відповідного рішення компетентними судовими органами та органами прокуратури. Також зазначається, що якщо питання стосується доступу до житлових приміщень, то згідно зі статтею 9 Конституції Греції «обшук житла не проводиться, крім випадків, передбачених законом, і завжди при представниках судової влади».

Інспекція з захисту даних Естонії може звертатися до підприємств електронного зв'язку із запитами про надання даних, необхідних для ідентифікації кінцевого користувача за допомогою ідентифікаційних токенів, що використовуються в загальнодоступних електронних комунікаційних мережах, за винятком даних, що стосуються факту передання повідомлень, якщо ідентифікація кінцевого користувача за допомогою ідентифікаційних токенів неможлива будь-яким іншим способом. З метою ведення державного нагляду, передбаченого національним законодавством, Інспекція з захисту даних Естонії може застосувати спеціальні заходи державного нагляду, передбачені пунктами 30–32, 44, 49–53 Закону «Про правоохоронні органи»[30], на підставі та в порядку, передбаченому Законом «Про правоохоронні органи».

Орган із захисту даних Польщі заявив, що відповідно до закону, який визначає його повноваження, на нього покладені такі функції з проведення розслідувань:

- вимагати від контролера та оператора, а у відповідних випадках від їхнього представника, надання будь-якої інформації, необхідної для виконання завдань наглядового органу з питань захисту даних;
- вимагати від будь-якої фізичної та/або юридичної особи (крім контролера та оператора) надання будь-якої інформації, необхідної для виконання завдань наглядового органу з питань захисту даних;
- проводити обшуки та вилучення у приміщенні оператора/контролера без рішення суду;
- без попереднього повідомлення мати доступ до приміщень/території контролера/оператора.

Слід зазначити, що без рішення суду жоден наглядовий орган не має права входити у приміщення, що належить фізичній особі.

30 https://www.riigiteataja.ee/akt/104012019011.

4.5. Органи, уповноважені вести нагляд

Всі без винятку 19 ОЗПД мають повноваження з ведення нагляду відповідно до статті 58 ЗРЗД. Додатково, повноваження органів Естонії та Греції мають свої особливості.

ОЗПД Естонії не накладає адміністративних штрафів, передбачених ЗРЗД. ОЗПД Естонії має право накладати штрафи за правопорушення, водночас адміністративні штрафи не передбачені правовою системою Естонії.

Наглядовий орган Греції уповноважений «вимагати від органу з сертифікації відкликати сертифікат, виданий відповідно до статей 42 та 43 ЗРЗД, або заборонити органові з сертифікації видавати сертифікат, якщо вимоги до сертифікації не виконані або більше не виконуються». Також наглядовий орган: a) має право вимагати від контролера або оператора, або одержувача, або третьої особи припинити обробку персональних даних або повернути, або закрити доступ до відповідних даних (заблокувати), або знищити систему реєстрації або відповідні дані та накласти адміністративні стягнення, передбачені статтями 82.8 та 83 ЗРЗД; б) коли захист особи від обробки персональних даних, що її стосуються, вимагає негайного ухвалення рішення, президент може, за клопотанням зацікавленої особи або у зв'язку з виконанням посадових повноважень, видати тимчасове розпорядження про негайне тимчасове повне або часткове обмеження обробки даних або роботи з даними, яке діє, доки наглядовий орган не ухвалить остаточне рішення; c) з метою забезпечення дотримання ЗРЗД та інших нормативних актів, що стосуються захисту суб'єкта даних щодо обробки персональних даних, наглядовий орган має право ухвалювати адміністративні регуляторні акти для врегулювання конкретних та технічних питань, а також для деталізації питань, що розглядаються в таких актах. Регуляторні акти наглядового органу, які не публікуються в урядовому віснику, публікуються на його вебсайті.

4.6. Органи, наділені повноваженнями дозвільного та консультативного характеру

Наглядові органи заявили, що вони мають усі повноваження, визначені статтею 58 ЗРЗД.

Наглядовий орган Республіки Кіпру зазначив повноваження, передбачені національним законодавством, зокрема статтею 25(g) закону 125 (I)/2018: «Окрім дозвільних та консультативних повноважень, передбачених пунктом 3 статті 58 регламенту, уповноважений має право: i) дозволяти поєднання систем зберігання інформації, передбачених розділом 10 цього закону, та встановлювати умови для його реалізації; ii) встановлювати умови застосування заходів обмеження прав, передбачених у розділі 11 цього закону; iii) встановлювати умови звільнення від обов'язку повідомляти про порушення даних, про який йде мова в розділі 12 цього закону; iv) встановлювати чіткі обмеження щодо передавання окремих категорій персональних даних, зазначених у розділах 17 та 18 цього закону; v) рекомендувати міністрові укладати угоди з іншими країнами й укладати, готувати та підписувати меморандуми про взаєморозуміння, передбачені в розділі 35 цього закону»[31].

Акредитацію органів сертифікації проводить наглядовий орган Латвії спільно з Латвійським національним бюро акредитації.

Відповідно до статті 57 ЗРЗД кожен наглядовий орган в межах своїх територіальних кордонів інформує, згідно з законодавством держави-члена, національний парламент, уряд та інші установи

31 http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf.

й органи щодо законодавчих і адміністративних інструментів, пов'язаних із захистом прав і свобод фізичних осіб у зв'язку з обробкою даних.

Модернізована Конвенція 108 передбачає проведення консультацій з компетентними наглядовими органами щодо пропозицій стосовно будь-яких законодавчих чи адміністративних заходів, які передбачають обробку персональних даних.

Учасникам опитування було запропоновано вказати їхню компетенцію щодо надання рекомендацій парламентові, урядові, іншим державним установам та органам щодо вживання законодавчих та адміністративних заходів. Значна більшість опитаних заявили, що до їхньої компетенції входить право надавати висновки щодо проєктів нормативно-правових актів, коли текст нормативно-правового акта розроблений, а також давати висновки щодо проєктів нормативно-правових актів під час опрацювання тексту нормативно-правового акта.

Відповідно до статті 14 Закону «Про імплементацію Загального регламенту про захист даних» центральні органи державної влади та інші органи державної влади подають до Агентства з захисту персональних даних Хорватії проєкти законів та інших нормативно-правових актів, що регулюють питання, пов'язані з обробкою персональних даних, для надання експертних висновків з питань захисту персональних даних.

Інспекція з захисту даних Естонії та ОЗПД Австрії надають висновки щодо проєктів нормативно-правових актів у межах своєї компетенції під час підготування нормативно-правового акта.

У межах своєї компетенції Управління захисту персональних даних Чеської Республіки надає висновки після ухвалення нормативно-правового акта.

4.7. Органи, наділені регуляторними повноваженнями

Наглядові органи Норвегії, Італії, Естонії, Хорватії, Республіки Кіпру, Литви, Ісландії, Герцогства Люксембургу, Латвії, Республіки Словенії та Болгарії заявили про додаткові повноваження.

Наглядовий орган Хорватії зазначив, що згідно зі статтею 6 Закону «Про імплементацію Загального регламенту про захист даних», окрім повноважень, визначених Загальним регламентом про захист даних, агентство виконує такі обов'язки:

- у випадках, передбачених спеціальним законом, воно може ініціювати та має право брати участь у кримінальних провадженнях, провадженнях у справах про адміністративні правопорушення, адміністративних та інших судових і позасудових провадженнях у зв'язку з порушенням Загального регламенту про захист даних та цього закону;
- встановлює критерії для визначення розміру компенсації адміністративних витрат, зазначених у пункті 2 статті 43 цього закону та критерії для визначення розміру компенсації, зазначеної в пункті 3 статті 43 цього закону;
- публікує акти індивідуальної дії на вебсайті агентства відповідно до статей 18 та 48 цього закону;
- ініціює та проводить відповідні заходи проти відповідальних осіб за порушення Загального регламенту про захист даних і цього закону;
- виконує свої обов'язки незалежного наглядового органу з контролю за виконанням Директиви (ЄС) 2016/680 Європейського парламенту та Ради від 27 квітня 2016 року «Про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами з

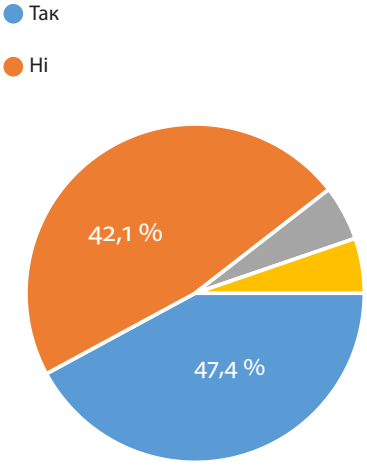
метою попередження, розслідування, виявлення або кримінального переслідування кримінальних злочинів або виконання кримінальних покарань та щодо вільного переміщення таких даних» та скасування рамкового рішення Ради 2008/977/JHA, якщо інше не передбачено спеціальними нормативними актами;

- виконує інші обов'язки, передбачені законом.

Завдання, покладені на уповноваженого з питань інформації, виконує відповідний уповноважений з питань захисту персональних даних Республіки Кіпру. Уповноважений — компетентний наглядовий орган серед інших європейських органів.

Результати опитування наведені нижче (див. рисунок 12).

Рисунок 12. Наглядовий орган із захисту даних наділений регуляторними повноваженнями, не передбаченими GDPR (наприклад, стаття 35 (4) тощо)

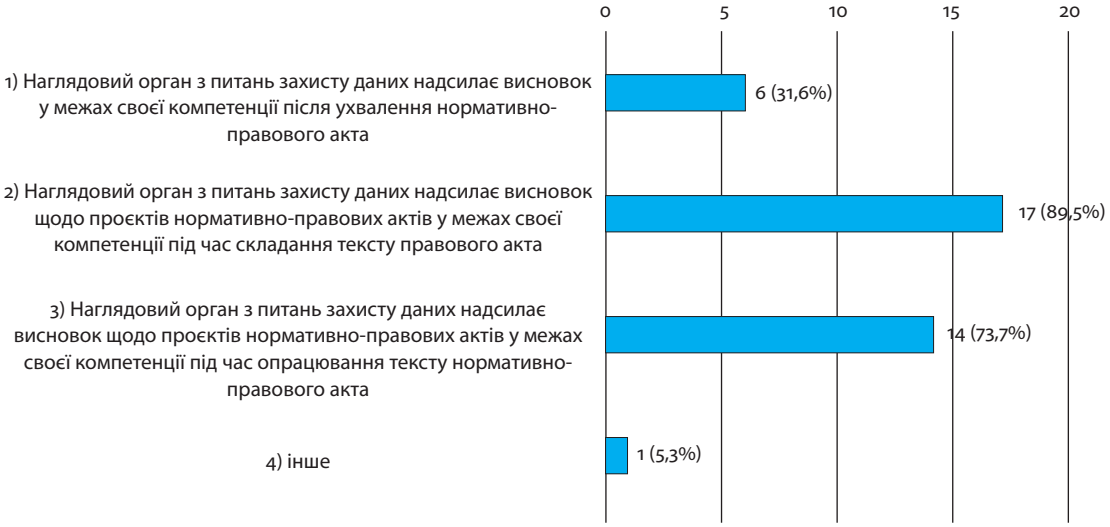


Відповідно до статті 6 Закону про імплементацію Загального регламенту про захист даних додатково до повноважень визначених у Загальному регламенті про захист даних Агентство виконує такі обов'язки: якщо це встановлено спеціальним законом, Агентство може ініціювати та має право брати участь у розгляді кримінальної, дисциплінарної та адміністративної справи внаслідок порушення положень Загального регламенту захисту даних та цього Закону; приймає вимоги щодо визначення розміру компенсації адміністративних витрат, передбачених пунктом 2 статті 43 цього Закону; публікує на вебсайті окремі рішення Агентства відповідно до статтей 18 та 48 цього Закону; ініціює та забезпечує процесуальні дії по відношенню до осіб, які порушують положення Загального регламенту захисту даних та цього Закону; реалізує свої обов'язки незалежного наглядового органу щодо моніторингу за імплементацією Директиви (ЄС) 2016/680 Європейського парламенту та Ради від 27.04.2016 року «Про захист фізичних осіб стосовно обробки персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або переслідування кримінальних злочинів або виконання кримінальних покарань та про вільне переміщення таких даних, і скасування Рамкового рішення Ради 2008/977/JHA», якщо інше не встановлено спеціальним законодавством; реалізує свої інші повноваження відповідно до Закону.

Завдання, покладені на Уповноваженого з питань інформації, виконує відповідний Уповноважений з питань захисту персональних даних. Уповноважений є компетентним наглядовим органом інших європейських інституцій.

Наглядові органи також повідомили про можливість надання рекомендацій національним органам влади. Результати опитування наведені нижче (див. рисунок 13).

Рисунок 13. Компетенція наглядового органу з питань захисту даних щодо рекомендацій парламенту, уряду, іншим державним установам та органам щодо вжиття законодавчих та адміністративних заходів



4.8. Повноваження брати участь у судовому розгляді

Регламент 2016/679 передбачає, що кожен наглядовий орган має право брати участь у судовому розгляді та подавати позов до суду з метою виконання положень цього Регламенту або забезпечення послідовності механізму захисту персональних даних у межах Союзу.

Відповідно до статті 15 модернізованої Конвенції 108 наглядові органи мають право брати участь у судовому розгляді або доводити до відома компетентних судових органів інформацію про порушення положень цієї Конвенції.

Учасникам опитування було запропоновано вказати права наглядового органу з питань захисту даних щодо участі в судовому розгляді. Значна більшість опитаних заявила, що вони мають право брати участь у судовому розгляді щодо ухвалених наглядовим органом рішень.

Повноваження брати участь в судовому процесі

Наприклад, Управління захисту даних Португалії має право оскаржувати нормативно-правові акти, ухвалені органами державної влади, вносити конституційне подання до Конституційного суду та брати участь у судовому розгляді щодо ухвалених наглядовим органом рішень.

Агентство з захисту персональних даних Хорватії може ініціювати та має право брати участь у кримінальних провадженнях, провадженнях у справах про адміністративні правопорушення, адміністративних та інших судових і позасудових провадженнях у зв'язку з порушенням Загального регламенту про захист даних та Закону «Про імплементацію Загального регламенту про захист даних». Агентство з захисту персональних даних Хорватії може ініціювати та вживати відповідних заходів проти відповідальних осіб за порушення Загального регламенту про захист даних та цього закону.

Уповноважений Кіпру з питань захисту персональних даних відповідно до закону має право оскаржувати нормативно-правові акти, ухвалені органами державної влади, та брати участь у судовому розгляді, що стосується рішень, ухвалених наглядовим органом. Уповноважений повідомляє генерального прокурора Республіки та/або поліцію про будь-які порушення положень Регламенту чи закону, які можуть становити склад правопорушення.

Інформаційний уповноважений Республіки Словенії має право вносити конституційне подання до Конституційного суду та брати участь у судовому розгляді щодо ухвалених наглядовим органом рішень.

Управління з питань захисту персональних даних Чеської Республіки має право оскаржувати нормативно-правові акти, ухвалені органами державного управління.

5
ПІДВИЩЕННЯ ОБІЗНАНОСТІ ГРОМАДСЬКОСТІ З ПИТАНЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Органи із захисту персональних даних держав — членів ЄС проводять просвітницькі заходи в рамках власної участі в кампаніях з підвищення обізнаності контролерів і операторів даних та громадськості.

Відповідно до пункту 1 статті 57 ЗРЗД, обов'язки ОЗПД щодо інформування громадськості можна поділити на дві групи. Перша охоплює обов'язки ОЗПД щодо підвищення рівня обізнаності і розуміння ризиків, правил, гарантій захисту і прав у зв'язку з опрацюванням даних. Друга група обов'язків ОЗПД передбачає «підвищення рівня обізнаності контролерів і операторів даних». [Нижче: обізнаності… про їхні обов'язки — обізнаності … з їхніми обов'язками]

Стаття 57 Регламент (ЄС) 2016/679

- Наглядовий орган сприяє обізнаності громадськості та її розумінню ризиків, правил, гарантій і прав у зв'язку з опрацюванням
- Наглядовий орган сприяє обізнаності контролерів і операторів з їхніми обов'язками за цим Регламентом

Модернізована Конвенція 108 передбачає, що наглядові органи забезпечуватимуть:

- інформування громадськості про свої функції і повноваження, а також про свою діяльність;
- інформування громадськості про права суб'єктів даних і реалізацію цих прав;
- інформування контролерів і операторів даних про їхні обов'язки відповідно до цієї Конвенції.

У пункті 132 преамбули ЗРЗД зазначено, що діяльність наглядових органів з інформування громадськості, має передбачати конкретні заходи, спрямовані на контролерів і операторів даних, зокрема представників мікро-, малого та середнього бізнесу, а також суб'єктів даних.

ЗРЗД не містить переліку видів діяльності і заходів, виконання яких передбачає обов'язок з інформування громадськості. Згідно із загальною практикою комунікації, прикладами різних заходів можуть бути (не обмежуючись ними) «оприлюднення пресрелізів, проведення брифінгів та надання коментарів; звіти, дослідження і публікації; співпраця із засобами масової інформації; проведення громадських зібрань і заходів; проведення нарад і семінарів; створення і розповсюдження освітніх матеріалів».

ОЗПД регулярно надають фахові консультації з питань захисту даних — самостійно, спільно з іншими ОЗПД або під егідою Європейської ради із захисту даних. Ці фахові консультації з узгодженого застосування ЗРЗД можуть надаватися у формі настанов, рекомендацій та обміну досвідом.

У цьому звіті ми наводимо деякі найважливіші результати. Учасників опитування попросили назвати заходи з інформування громадськості, а також підвищення рівня обізнаності контролерів і операторів даних з їхніми обов'язками. Значна більшість зазначила, що їхня діяльність передбачає проведення семінарів/вебінарів та надання консультацій контролерам і операторам даних щодо положень Регламенту 2016/679, організацію інформаційних кампаній із захисту даних для контролерів і операторів з метою підвищення кваліфікації державних службовців, відповідальних за забезпечення захисту персональних даних.

За інформацією, наданою Європейською комісією[32], починаючи з 2017 року, Європейський Союз загалом виділив 5 мільйонів євро на реалізацію 19 проєктів з надання підтримки у впровадженні Загального регламенту про захист даних.

Станом на травень 2020 року, у рамках трьох етапів фінансування отримано фінансову підтримку на 5 мільйонів євро. Два останні етапи присвячено підтримці зусиль національних органів із захисту персональних даних з метою налагодження зв'язку з громадянами та малим і середнім бізнесом.

Наприклад, Агентство із захисту персональних даних Хорватії щотижня проводить регулярні тренінги, присвячені низці завдань і функцій інспекторів із захисту персональних даних, що випливають із ЗРЗД. Ці тренінги проводять окремо для державного та приватного секторів, що дає змогу зосередитися на проблемах конкретного сектору, а також додатково на тему окремих видів діяльності, як-от сектор безпеки. Документи та брошури за підсумками цих тренінгів розміщують на вебсайті Агентства із захисту персональних даних Хорватії.

У рамках проєкту ЄС з проведення інформаційних кампаній для малого та середнього бізнесу Агентство із захисту персональних даних Хорватії та Комісія з питань захисту даних Ірландії у своїй повсякденній роботі зауважили, що в застосуванні ЗРЗД малим та середнім бізнесом досі трапляється велика кількість випадків його неоднозначного тлумачення. Ці висновки підтверджуються великою кількістю письмових запитів і навіть більшою кількістю телефонних звернень, що отримують ці два органи щодня. Завдяки цьому проєктові Агентство із захисту персональних даних Хорватії та Комісія з питань захисту даних Ірландії мають додаткову можливість за допомогою практичних семінарів, презентацій та освітніх матеріалів сприяти повномасштабному впровадженню такими суб'єктами ЗРЗД і розумінню ними важливості захисту персональних даних.

Державна інспекція із захисту персональних даних Литви інформує громадськість за допомогою інформаційних інструментів і методичних документів, участі в зустрічах з представниками державного та приватного секторів і презентацій у рамках інших заходів.

Орган із захисту персональних даних Австрії розміщує велику кількість інформації на власному вебсайті і публікує важливі рішення органу в інформаційному бюлетені.

Інспекція із захисту персональних даних Естонії організувала телефонну гарячу лінію для контролерів і операторів даних, суб'єктів даних, інших органів державної влади тощо.

Інспектор із захисту персональних даних Кіпру проводить інформаційну кампанію із захисту даних для контролерів і операторів даних з метою підвищення кваліфікації державних службовців,

32 https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en.

відповідальних за забезпечення захисту персональних даних, а також інформаційні кампанії для широкого загалу і студентів.

Орган із захисту персональних даних Греції робить публічні виступи, організовує інформаційні дні та наукові конференції.

Орган із захисту персональних даних Польщі публікує щомісячний інформаційний бюлетень для інспекторів із захисту даних.

CNIL (Франція) очолює інформаційні кампанії із захисту персональних даних, спрямовані на широку громадськість, у засобах масової інформації, на власному вебсайті, у соціальних мережах та в рамках цільових семінарів. CNIL також бере участь у конференціях, семінарах і практикумах, щоб донести важливу інформацію і знання.

ОЗПД Великої Британії (ICO) розпочав кампанію з інформування про захист персональних даних серед британських споживачів. Кампанія проводиться згідно з рекомендаціями Офісу щодо аналізу даних опитувань для політичних цілей. У рамках кампанії споживачам запропоновано багато ресурсів, зокрема доступні для скачування пам'ятки про захист персональних даних і рекламу, а також інформацію про права людини відповідно до ЗРЗД.

Уповноважена з питань інформації Елізабет Денем зазначила[33]: «Наша мета — сприяти змінам і підвищенню довіри до нашої демократичної системи. Це стане можливим, якщо люди достеменно знатимуть, яким чином організації використовують їхні дані, особливо якщо це відбувається за лаштунками». Уповноважена також зауважила: «Нові технології і методи аналізу даних привели до появи інструментів впливу, що дозволяють організаторам кампаній прямо взаємодіяти з виборцями та безпосередньо адресувати їм послання, сформовані на основі їхніх лайків, свайпів і постів. Втім це не може відбуватися коштом прозорості, добропорядності та дотримання закону».

Заходи, організовані наглядовими органами з питань захисту даних	Бельгія: конфіденційність та інформаційна кампанія GDPR для громадян Болгарія: інноваційні інструменти для МСП та громадян Угорщина: навчальні програми для МСП Латвія: підвищення рівня обізнаності для МСП Латвії та неповнолітніх Ісландія: підвищення обізнаності широкої громадськості Ісландії Словенія: підвищення обізнаності громадськості щодо захисту даних Нідерланди: підвищення обізнаності щодо захисту даних у Нідерландах

Заходи, організовані наглядовими органами з питань захисту даних	Європейський фонд юристів Stichting організував навчання юристів з питань реформи захисту даних ЄС Університет Вріє у Брюсселі підтримав угорське DPA в організації навчальних заходів з реформи захисту даних Центр європейського конституційного права організував в Греції та на Кіпрі тренінги для юристів з питань захисту даних Fondazione Lelio e Basso – ISSOCO організувала з італійським ОЗПД навчання польських, іспанських, болгарських та угорських ОЗПД.

Україна теж робить перші кроки з метою підвищення обізнаності громадськості зі сферою захисту персональних даних.

Секретаріат Уповноваженого Верховної Ради України з прав людини та Офіс Ради Європи в Україні започаткували ініціативу (онлайн-курс) підвищення обізнаності українців зі сферою захисту персональних даних. Цей курс складається з двох частин: перша частина (загальна) — для широкої авдиторії, друга частина (професійна) — для фахівців у сфері захисту персональних даних та громадян, що прагнуть глибше розібратися в цій тематиці[34].

Міністерство цифрової трансформації України випустило освітній серіал під назвою «Персональні дані». Ці відеоматеріали мають навчати людей бути обачливими, розміщуючи особисту інформацію в інтернеті, розуміти свої права щодо захисту персональних даних та як діяти у разі порушення цих прав. Цей серіал має сприяти зменшенню кількості порушень у сфері персональних даних[35].

Міністерство цифрової трансформації України також випустило інструментарій, що має допомогти компаніям забезпечити захист персональних даних[36]. Ініціатива спрямована на зменшення кількості порушень у сфері персональних даних. Інструментарій містить спеціально розроблений тест для оцінювання відповідності компаній до вимог законодавства щодо захисту персональних даних.

6
ВИСНОВКИ І РЕКОМЕНДАЦІЇ

Щодо статусу і місця інституції в системі органів державної влади:

1. Члени наглядового органу у сфері захисту персональних даних можуть бути призначені урядом, парламентом, головою держави або за участю кількох з них з урахуванням критерії незалежності наглядового органу у сфері захисту персональних даних . Статус наглядового органу має бути закріплено у законі або іншому законодавчому акті, ухваленому парламентом.

2. Невіднятна передумова незалежності наглядового органу — його правосуб'єктність, тому він не може входити до структури будь-якого іншого державного органу. Також необхідно уникати підпорядкування наглядового органу міністерству чи іншому державному органові, бо це може призвести до обмеження інших гарантій, спрямованих на забезпечення незалежного статусу наглядового органу.

Щодо сфери нагляду:

3. Один і той самий орган може відповідати за ведення нагляду за законністю опрацювання даних у різних сферах і для різних цілей (у правоохоронній сфері, у сфері електронних комунікацій, для цілей журналістики тощо). Створення єдиного наглядового органу у сфері захисту персональних даних може вважатися ефективнішим та дієвішим з погляду узгодженого застосування принципів захисту персональних даних у різних сферах, а також з погляду правового регулювання (нема потреби в кількох різних нормативних актах) і ресурсів (нема потреби в кількох секретаріатах тощо).

4. Якщо за ведення нагляду за застосуванням законодавства у сфері захисту персональних даних відповідає кілька органів, усі вони повинні мати однаковий незалежний статус, як це передбачено Конвенцією 108+ та ЗРЗД.

5. Наглядовий орган у сфері захисту персональних даних не повинен мати повноважень вести нагляд за операціями з опрацювання даних судами при виконанні ними своїх обов'язків, проте до його компетенції мають входити інші операції опрацювання даних судами.

6. Обмеження завдань і повноважень наглядового органу щодо здійснення нагляду за опрацюванням даних у цілях національної безпеки та оборони, передбачені підпунктами a, b, c і d пункту 2 статті 15 Конвенції 108+, мають бути визначені законом виключно у межах необхідності для досягнення цієї мети і пропорційно цій меті в демократичному суспільстві.

Щодо гарантій незалежності (призначення на посаду і припинення повноважень членів наглядових органів, строк повноважень, бюджет, кадрові ресурси):

7. Строк повноважень членів наглядових органів має становити не менше ніж чотири роки. Члени наглядових органів можуть бути призначені на повторний строк, але можливість повторного призначення не необхідна з погляду забезпечення незалежності.

8. Строк повноважень, можливість повторного призначення, вичерпний перелік підстав для припинення повноважень та звільнення з посади членів наглядового органу мають бути

визначені законом. Процедура звільнення з посади має передбачати обов'язкову участь у ній органів, відповідальних за призначення членів наглядового органу.

9. Через те що підстави для звільнення з посади тісно пов'язані з дотриманням кваліфікаційних та інших вимог до виконання обов'язків, останні теж мають бути чітко визначені законом. Законом також мають бути визначені заборони щодо ведення діяльності, зокрема професійної, та отримання привілеїв, що несумісні зі статусом члена чи співробітника наглядового органу протягом або після завершення строку повноважень, а також їхні обов'язки (наприклад, обов'язок щодо дотримання конфіденційності тощо).

10. Наглядовий орган у сфері захисту персональних даних повинен мати окремий державний річний бюджет, що може бути частиною загального державного чи національного бюджету. Процедура розподілу бюджетних коштів має забезпечувати захист від зовнішнього впливу на діяльність наглядового органу (органи виконавчої влади держави не повинні мати вирішального впливу). Ризик такого зовнішнього впливу може бути значно мінімізований завдяки участі наглядового органу у процесі консультацій та ухвалення рішень щодо розподілу коштів.

11. Наглядовий орган може отримувати фінансування з інших джерел, але обов'язок щодо забезпечення його достатніми ресурсами лежить на державі. Отже, державний бюджет має залишатися основним джерелом фінансування.

12. Бюджет безпосередньо впливає на можливість залучення інших ресурсів (кадрових, технічних тощо). Стосовно чинників, які необхідно врахувати для визначення необхідного обсягу коштів, слід зазначити, що фінансові ресурси мають давати змогу наглядовому органові бути укомплектованим кваліфікованим персоналом із забезпеченням рівня зарплати, що відповідає принаймні середній зарплаті в державному секторі, а також мати необхідні приміщення, технічне обладнання та інфраструктуру. Також необхідно враховувати підготування персоналу та інші потреби.

13. Наглядовий орган повинен мати можливість самостійно набирати співробітників, що підпорядковуватимуться лише членам відповідного наглядового органу. Співробітники наглядового органу у сфері захисту персональних даних не мають підпорядковуватися чи бути підконтрольними будь-якому іншому органові з погляду ієрархії та оплати праці, а також дисциплінарного контролю.

14. Будь-яке організаційне дублювання між наглядовим органом у сфері захисту персональних даних та будь-яким іншим державним органом не дає змоги наглядовому органові бути поза підозрами в упередженості й тому несумісне з вимогою незалежності.

15. Незалежно від статусу співробітників наглядового органу (державних службовців чи співробітників, що працюють за трудовим договором), мають бути забезпечені гарантії їхнього захисту від будь-якого зовнішнього впливу.

16. Наглядовий орган повинен мати автономію в питаннях використання ресурсів і планування своєї діяльності. Рекомендується законодавчо закріпити гарантії автономії в питаннях використання бюджету та інших ресурсів без попереднього дозволу / схвалення / консультацій з боку інших державних органів; ухвалення рішень про внутрішню структуру, кількість та кваліфікацію співробітників наглядового органу; ухвалення рішень щодо планування діяльності. Плани діяльності не повинні підлягати оцінюванню, узгодженню та затвердженню іншими органами.

17. Внутрішня діяльність наглядового органу та використання ним ресурсів не підлягає зовнішньому контролю. Втім фінансовий контроль, що ведеться відповідно до закону і не впливає на незалежність наглядового органу, допустимий.

Щодо інших гарантій захисту від зовнішнього впливу:

18. Законодавчий акт, ухвалений парламентом, служить міцною гарантією незалежності наглядового органу. Отже, він має щонайменше регулювати аспекти, пов'язані з процедурою призначення на посаду членів наглядового органу (хто пропонує кандидатури, хто відповідає за призначення тощо), кваліфікаційні та інші вимоги до призначення на посаду члена наглядового органу, строк повноважень членів наглядового органу (тривалість, можливість повторного призначення), підстави для припинення повноважень і звільнення з посади та відповідні процедури, бюджетні процедури (окремий публічний річний бюджет), автономію в питаннях кадрової політики і планування діяльності, оплату праці членів наглядового органу.

19. Регулювання статусу наглядового органу загалом має забезпечувати його незалежність від політичного впливу. Щоб запобігти політичному впливові, початок і завершення строку повноважень членів наглядового органу не мають бути пов'язані зі строком повноважень органу призначення (уряду, парламенту, голови держави). Членів наглядових органів призначають на посаду і звільняють від виконання обов'язків лише відповідно до закону.

20. Повноваження члена наглядового органу не може бути припинене достроково, крім як на підставах, передбачених законом. Захист чинних членів наглядового органу від дострокового припинення повноважень у разі реструктуризації або видозміни організаційної моделі має бути забезпечений відповідними нормами закону.

21. Оскарження рішень наглядового органу має відповідати принципові верховенства права. Кожен суб'єкт, на якого поширюється рішення наглядового органу, повинен мати можливість оскарження таких рішень у суді.

Стосовно повноважень щодо проведення розслідувань, вжиття заходів, розгляду скарг і регуляторних повноважень:

22. Для забезпечення виконання завдань, передбачених статтею 57 ЗРЗД, наглядовий орган повинен мати повноваження згідно зі статтею 15 Конвенції 108+ та статтею 58 ЗРЗД проводити розслідування, вживати заходів, мати необхідні регуляторні повноваження і водночас повинен дотримуватися основних конституційних прав людини.

23. Пункт 23.ОЗПД має бути наділений достатніми правоохоронними функціями.

24. Після набрання чинності ЗРЗД більшість європейських країн переглянула повноваження свого ОЗПД з метою забезпечення захисту персональних даних і доповнили його відповідні завдання та повноваження.

25. Жоден ОЗПД не має права доступу до житлових приміщень (зокрема приміщень, що орендуються або використовуються на будь-якій іншій підставі) фізичної особи без рішення суду, що дозволяє вхід до житлового приміщення. Питання про допуск до приміщень фізичних осіб-підприємців, у яких вони ведуть діяльність, рекомендується розв'язувати на підставі рішення суду в порядку, передбаченому законом.

26. Необхідно на рівні законодавства закріпити порядок проведення консультацій, але з гарантіями неможливості зловживань і використання ОЗПД як постійного безплатного консультанта.

27. Рекомендується розглянути питання сертифікації після запровадження всіх інших повноважень ОЗПД.

28. Наглядовий орган повинен мати право доводити до відома судових органів інформацію про порушення законодавства про захист персональних даних та, за необхідності, порушувати чи іншим чином брати участь у судовому розгляді.

29. ОЗПД повинно мати право брати участь у судовому розгляді та порушувати справу в суді з метою дотримання положень закону та Конвенції 108+ або задля забезпечення послідовності механізму захисту персональних даних.

30. ОЗПД може мати інші повноваження, які не суперечать ЗРЗД та Конвенції 108+, але прямо чи опосередковано впливають на захист персональних даних. Наприклад, повноваження, передбачені міжнародними угодами, – взаємодія з іншими міжнародними установами (Євроюст, Європол). Рекомендовано делегувати нагляд одному визначеному органу.

31. Що стосується участі у судовому розгляді, то в національному законодавстві про захист даних слід закріпити такі основні права ОЗПД: доводити до відома судових органів про випадки порушення законодаства про захист персональних даних; оскаржувати нормативно-правові акти, прийняті органами державної влади; брати участь у судовому розгляді, що стосується рішень, прийнятих наглядовим органом.

32. ОЗПД надають висновки щодо проєктів нормативно-правових актів у межах своєї компетенції в трьох випадках: після ухвалення нормативно-правового акта; коли текст нормативно-правового акта розроблений; під час опрацювання тексту нормативно-правового акта.

Щодо підвищення обізнаності громадськості:

33. Кампанії з інформування про захист персональних даних – це інструмент, завдяки якому ОЗПД мають можливість за допомогою семінарів, тренінгів, лекцій, настанов та інших матеріалів не лише сприяти підвищенню обізнаності у сфері захисту персональних даних, але й сприяти дотриманню принципів захисту персональних даних.

34. Кампанії з інформування про захист персональних даних мають будуватися з урахуванням загальної мети підвищення обізнаності зі сферою захисту персональних даних суб'єктів даних і контролерів та/або операторів даних.

35. Систематичне проведення семінарів, тренінгів, лекцій, практикумів для державних службовців, присвячених теоретичним і практичним аспектам захисту персональних даних, сприятиме підвищенню кваліфікації державних службовців, відповідальних за забезпечення захисту персональних даних.

36. ОЗПД країн ЄС організовують кампанії з інформування про захист персональних даних по-різному:

- через проведення семінарів/вебінарів;
- консультування контролерів і операторів даних щодо положень Регламенту 2016/679;
- освітні відео;
- кампанії в медіа, на вебсайтах, у соціальних мережах та у форматі цільових семінарів;
- щомісячні інформаційні бюлетені, присвячені захистові персональних даних;
- інформаційні дні та наукові конференції на тему захисту персональних даних;

- гарячі телефонні лінії для контролерів і операторів даних, суб'єктів даних та інших органів державної влади;
- пам'ятки про захист персональних даних і рекламу.

37. Навчання і підвищення кваліфікації державних службовців у сфері захисту персональних даних має фінансувати і централізовано проводити уряд.

Київ, Вільнюс, 6 липня 2021 року

Діана Шинкунєне

Лілія Олексюк

Олександр Шевчук

7

ДОДАТКИ

Додаток 1. Анкета для наглядових органів з питань захисту персональних даних

Країна	Назва	Електронна адреса
Норвегія	Datatilsynet - Norwegian Data Protection Authority (Орган з нагляду за дотриманням законодавства у сфері захисту даних Норвегії)	postkasse@datatilsynet.no
Словацька Республіка	The Office for Personal Data Protection of the Slovak Republic (Офіс із захисту персональних даних Словацької Республіки)	statny.dozor@pdp.gov.sk
Румунія	Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (Національний орган з нагляду за дотриманням законодавства у сфері обробки персональних даних Румунії)	anspdcp@dataprotection.ro
Італія	Il Garante per la protezione dei dati personali (Гарант захисту персональних даних)	a.pierucci@gpdp.it
Естонія	Estonian Data Protection Inspectorate (Інспекція із захисту даних Естонії)	info@aki.ee
Хорватія	Croatian Personal Data Protection Agency (Агентство захисту персональних даних Хорватії)	azop@azop.hr
Республіка Кіпр	Commissioner for Personal Data Protection (Уповноважений з питань захисту персональних даних)	commissioner@dataprotection.gov.cy
Литва	State Data Protection Inspectorate (Державна інспекція з питань захисту даних, далі – ДІЗД)	ada@ada.lt
Ісландія	Persónuvernd (Орган з питань захисту даних Ісландії)	postur@personuvernd.is
Греція	Hellenic Data Protection Authority (Орган з питань захисту даних Греції)	contact@dpa.gr
Князівство Ліхтенштейн	Datenschutzstelle (Управління захисту даних Ліхтенштейну)	marie-louise.gaechter@llv.li
Португалія	Comissão Nacional de Proteção de Dados (Національна комісія з питань захисту даних)	geral@cnpd.pt
Велике Герцогство Люксембург	CNPD (Національна комісія з питань захисту даних)	tine.larsen@cnpd.lu
Латвія	Data State Inspectorate of Latvia (Державна інспекція даних Латвії)	pasts@dvi.gov.lv
Чеська Республіка	Office for Personal Data Protection of the Czech Republic (Управління захисту персональних даних Чеської Республіки)	posta@uoou.cz
Австрія	Austrian Data Protection Authority (Орган з питань захисту даних Австрії)	dsb@dsb.gv.at
Республіка Словенія	Informacijski pooblaščenec (Комісар з питань інформації Республіки Словенії)	gp.ip@ip-rs.si
Болгарія	Commission for Personal Data Protection (Комісія з питань захисту персональних даних)	kzld@cpdp.bg

1. Чи ваш наглядовий орган у сфері захисту персональних даних, колегіальний чи одноособовий:

Норвегія	очолює одна уповноважена особа (директор тощо)
Словацька Республіка	очолює одна уповноважена особа (директор тощо)
Румунія	очолює одна уповноважена особа (директор тощо)
Італія	колегіальний орган (комісія тощо)
Естонія	очолює одна уповноважена особа (директор тощо)
Хорватія	очолює одна уповноважена особа (директор тощо)
Республіка Кіпр	очолює одна уповноважена особа (директор тощо)
Литва	очолює одна уповноважена особа (директор тощо)
Ісландія	Обидва варіанти. Щоденною роботою керує уповноважена особа, але в ОЗД також є рада директорів, яка ухвалює рішення з особливо важливих питань, накладає штрафи тощо.
Греція	колегіальний орган (комісія тощо)
Князівство Ліхтенштейн	очолює одна уповноважена особа (директор тощо)
Португалія	колегіальний орган (комісія тощо)
Велике Герцогство Люксембург	колегіальний орган (комісія тощо)
Латвія	очолює одна уповноважена особа (директор тощо)
Чеська Республіка	очолює одна уповноважена особа (директор тощо)
Австрія	очолює одна уповноважена особа (директор тощо)
Республіка Словенія	очолює одна уповноважена особа (директор тощо)
Болгарія	колегіальний орган (комісія тощо)

2. Ваш наглядовий орган у сфері захисту персональних даних:

Норвегія	володіє правосуб´єктністю
Словацька Республіка	володіє правосуб´єктністю
Румунія	володіє правосуб´єктністю
Італія	володіє правосуб´єктністю
Естонія	підпорядковується міністерству або іншій державній установі, незалежний орган при Міністерстві юстиції
Хорватія	володіє правосуб´єктністю
Республіка Кіпр	володіє правосуб´єктністю
Литва	володіє правосуб´єктністю, ДІЗД – установа, що підпорядковується урядові Литовської Республіки
Ісландія	володіє правосуб´єктністю
Греція	володіє правосуб´єктністю
Князівство Ліхтенштейн	володіє правосуб´єктністю
Португалія	володіє правосуб´єктністю
Велике Герцогство Люксембург	володіє правосуб´єктністю
Латвія	володіє правосуб´єктністю
Чеська Республіка	володіє правосуб´єктністю
Австрія	володіє правосуб´єктністю
Республіка Словенія	володіє правосуб´єктністю
Болгарія	володіє правосуб´єктністю

3. Будь ласка, зазначте статус вашого наглядового органу у сфері захисту персональних даних:

Норвегія	урядова установа зі спеціальним статусом, закріпленим у законі
Словацька Республіка	урядова установа зі спеціальним статусом, закріпленим у законі
Румунія	Державний орган зі статусом юридичної особи, наділений самостійністю і незалежністю у відносинах з іншими органами державного управління, а також будь-якою фізичною або юридичною особою приватного сектору
Італія	незалежний наглядовий орган
Естонія	урядова установа зі спеціальним статусом, закріпленим у законі
Хорватія	Відповідно до частини другої статті 4 Закону про виконання Загального регламенту про захист даних Агентство – незалежний державний орган
Республіка Кіпр	незалежна наглядова установа, статус якої закріплений у законі
Литва	ДІЗД – урядова установа. Це незалежний орган. Директор Інспекції підзвітний урядові Литовської Республіки та міністрові юстиції
Ісландія	державний орган зі спеціальним статусом, закріпленим у законі
Греція	незалежний державний орган, створений відповідно до конституції
Князівство Ліхтенштейн	державний орган зі спеціальним статусом, закріпленим у законі
Португалія	державна установа, передбачена конституцією
Велике Герцогство Люксембург	державний орган зі спеціальним статусом, закріпленим у законі
Латвія	державний орган зі спеціальним статусом, закріпленим у законі
Чеська Республіка	державний орган зі спеціальним статусом, закріпленим у законі
Австрія	державний орган зі спеціальним статусом, закріпленим у законі
Республіка Словенія	незалежний державний орган (функціонує окремо від уряду, подібно до омбудсмана)
Болгарія	державний орган зі спеціальним статусом, закріпленим у законі

4. Ваш наглядовий орган у сфері захисту персональних даних отримує фінансування (можна надати кілька відповідей):

Норвегія	прямо з державного бюджету (наприклад, має окремий бюджет, що становить частину загальнодержавного або національного бюджету)
Словацька Республіка	з бюджету, що виділяється міністерству або іншій державній установі
Румунія	прямо з державного бюджету (наприклад, має окремий бюджет, що становить частину загальнодержавного або національного бюджету)
Італія	прямо з державного бюджету (наприклад, має окремий бюджет, що становить частину загальнодержавного або національного бюджету)
Естонія	з бюджету, що виділяється міністерству або іншій державній установі, окремий рядок у державному бюджеті (в юрисдикції Міністерства юстиції)
Хорватія	прямо з державного бюджету (наприклад, має окремий бюджет, що становить частину загальнодержавного або національного бюджету)
Республіка Кіпр	прямо з державного бюджету (наприклад, має окремий бюджет, що становить частину загальнодержавного або національного бюджету)
Литва	прямо з державного бюджету (наприклад, має окремий бюджет, що становить частину загальнодержавного або національного бюджету). ДІЗД – бюджетна установа, яка утримується коштом державного бюджету Литовської Республіки. Інші кошти, отримані законним шляхом, можуть використовуватися для фінансування ДІЗД. Правова підстава для фінансування ДІЗД – пункт 6 положення про Державну інспекцію з питань захисту даних, затвердженого урядом Литовської Республіки 25 вересня 2001 року № 1156
Ісландія	з бюджету, виділеного міністерству чи іншій державній установі
Греція	Ресурси Органу з питань захисту даних Греції надходять з державного бюджету. Вони становлять частину бюджету Міністерства юстиції та відображаються в ньому окремим рядком.
Князівство Ліхтенштейн	безпосередньо з державного бюджету (наприклад, орган має окремий бюджет, який становить частину державного або національного бюджету)

Португалія	безпосередньо з державного бюджету (наприклад, орган має окремий бюджет, який становить частину державного або національного бюджету), з доходів, отриманих під час виконання завдань, пов'язаних з контролерами / операторами даних, від адміністративних штрафів / інших фінансових санкцій, накладених як покарання за порушення
Велике Герцогство Люксембург	з бюджету, виділеного міністерству чи іншій державній установі
Латвія	безпосередньо з державного бюджету (наприклад, орган має окремий бюджет, який становить частину державного або національного бюджету), з бюджету, виділеного міністерству чи іншій державній установі
Чеська Республіка	безпосередньо з державного бюджету (наприклад, орган має окремий бюджет, який становить частину державного або національного бюджету)
Австрія	з бюджету, виділеного міністерству чи іншій державній установі
Республіка Словенія	безпосередньо з державного бюджету (наприклад, орган має окремий бюджет, який становить частину державного або національного бюджету)
Болгарія	безпосередньо з державного бюджету (наприклад, орган має окремий бюджет, який становить частину державного або національного бюджету)

5. Ваш наглядовий орган у сфері захисту персональних даних (можна надати декілька відповідей):

Норвегія	веде повний контроль над використанням свого бюджету (наприклад, без попереднього дозволу / погодження / консультацій з іншою урядовою установою), самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно розв'язує питання щодо кількості та кваліфікації свого персоналу, а також стосовно планування своєї діяльності (наприклад, стратегічних планів тощо)
Словацька Республіка	самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно розв'язує питання стосовно планування своєї діяльності (наприклад, стратегічних планів тощо)
Румунія	веде повний контроль над використанням свого бюджету (наприклад, без попереднього дозволу / погодження / консультацій з іншою урядовою установою), самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно розв'язує питання щодо кількості свого персоналу в межах, визначених законодавчим актом, а також стосовно планування своєї діяльності (наприклад, стратегічних планів тощо)
Італія	повністю контролює використання свого бюджету (наприклад, без попереднього дозволу / погодження / консультацій з іншою урядовою установою), самостійно ухвалює рішення про затвердження внутрішньої структури органу, розв'язує питання щодо кількості своїх працівників у межах, визначених законодавчим актом, самостійно ухвалює рішення про планування своєї діяльності (наприклад, стратегічні плани тощо)
Естонія	веде повний контроль над використанням свого бюджету (наприклад, без попереднього дозволу / погодження / консультацій з іншою урядовою установою), самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно розв'язує питання щодо кількості та кваліфікації свого персоналу, розв'язує питання щодо кількості своїх працівників у межах, визначених законодавчим актом, самостійно ухвалює рішення про планування своєї діяльності (наприклад, стратегічні плани тощо)
Хорватія	веде повний контроль над використанням свого бюджету (наприклад, без попереднього дозволу / погодження / консультацій з іншою урядовою установою), самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно розв'язує питання щодо кількості та кваліфікації свого персоналу, розв'язує питання щодо кількості своїх працівників у межах, визначених законодавчим актом, самостійно ухвалює рішення про планування своєї діяльності (наприклад, стратегічні плани тощо)
Республіка Кіпр	повністю контролює використання свого бюджету (наприклад, без попереднього дозволу / погодження / консультацій з іншою урядовою установою), самостійно ухвалює рішення про затвердження внутрішньої структури органу, самостійно ухвалює рішення про планування своєї діяльності (наприклад, стратегічні плани тощо)
Литва	веде повний контроль над використанням свого бюджету (наприклад, без попереднього дозволу / погодження / консультацій з іншою урядовою установою), самостійно ухвалює рішення щодо внутрішньої структури органу, розв'язує питання щодо кількості своїх працівників у межах, визначених законодавчим актом, самостійно ухвалює рішення про планування своєї діяльності (наприклад, стратегічні плани тощо)
Ісландія	самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно ухвалює рішення щодо кількості та кваліфікації працівників, самостійно ухвалює рішення щодо планування діяльності (наприклад, стратегічного планування тощо)
Греція	має повний контроль над використанням свого бюджету (наприклад, без отримання попереднього дозволу / схвалення / рекомендації іншої державної установи), ухвалює рішення щодо кількості працівників у рамках, встановлених законодавчим актом, самостійно ухвалює рішення щодо планування діяльності (наприклад, стратегічного планування тощо)

Князівство Ліхтенштейн	має повний контроль над використанням свого бюджету (наприклад, без отримання попереднього дозволу / схвалення / рекомендації іншої державної установи), самостійно ухвалює рішення щодо внутрішньої структури органу, ухвалює рішення щодо кількості працівників у рамках, встановлених законодавчим актом, самостійно ухвалює рішення щодо планування діяльності (наприклад, стратегічного планування тощо)
Португалія	має повний контроль над використанням свого бюджету (наприклад, без отримання попереднього дозволу / схвалення / рекомендації іншої державної установи), ухвалює рішення щодо кількості працівників у рамках, встановлених законодавчим актом, самостійно ухвалює рішення щодо планування діяльності (наприклад, стратегічного планування тощо)
Велике Герцогство Люксембург	самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно ухвалює рішення щодо планування діяльності (наприклад, стратегічного планування тощо)
Латвія	має повний контроль над використанням свого бюджету (наприклад, без отримання попереднього дозволу / схвалення / рекомендації іншої державної установи), самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно ухвалює рішення щодо кількості та кваліфікації працівників, самостійно ухвалює рішення щодо планування діяльності (наприклад, стратегічного планування тощо)
Чеська Республіка	має повний контроль над використанням свого бюджету (наприклад, без отримання попереднього дозволу / схвалення / рекомендації іншої державної установи)
Австрія	має повний контроль над використанням свого бюджету (наприклад, без отримання попереднього дозволу / схвалення / рекомендації іншої державної установи), самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно ухвалює рішення щодо планування діяльності (наприклад, стратегічного планування тощо)
Республіка Словенія	має повний контроль над використанням свого бюджету (наприклад, без отримання попереднього дозволу / схвалення / рекомендації іншої державної установи), самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно ухвалює рішення щодо кількості та кваліфікації працівників, самостійно ухвалює рішення щодо планування діяльності (наприклад, стратегічного планування тощо)
Болгарія	має повний контроль над використанням свого бюджету (наприклад, без отримання попереднього дозволу / схвалення / рекомендації іншої державної установи), самостійно ухвалює рішення щодо внутрішньої структури органу, самостійно ухвалює рішення щодо кількості та кваліфікації працівників, ухвалює рішення щодо кількості працівників у рамках, встановлених законодавчим актом, самостійно ухвалює рішення щодо планування діяльності (наприклад, стратегічного планування тощо)

6. Керівника / членів вашого наглядового органу у сфері захисту персональних даних призначає:

Норвегія	уряд
Словацька Республіка	парламент
Румунія	президента Наглядового органу Румунії призначає Сенат
Італія	парламент. Будь ласка, зверніть увагу, що група уповноважених складається з чотирьох членів, двох з яких обирає Палата депутатів і двох – Сенат шляхом спеціальної процедури голосування
Естонія	уряд
Хорватія	парламент
Республіка Кіпр	Стаття 19(1) Закону 125(I)/2018: «Уповноваженого з питань захисту персональних даних призначає Рада міністрів за рекомендацією міністра»
Литва	уряд
Ісландія	уряд
Греція	парламент
Князівство Ліхтенштейн	парламент
Португалія	парламент, уряд
Велике Герцогство Люксембург	голова держави (наприклад, президент)
Латвія	уряд
Чеська Республіка	голова держави (наприклад, президент)
Австрія	голова держави (наприклад, президент)
Республіка Словенія	парламент
Болгарія	парламент

7. Будь ласка, зазначте, хто висуває кандидата на посаду керівника / члена наглядового органу у сфері захисту персональних даних:

Норвегія	публічний конкурс, кандидата висуває Комітет з добору кандидатів на найвищі посади державних службовців
Словацька Республіка	кандидата висуває уряд
Румунія	кандидата висуває Постійне бюро Сенату
Італія	Члени органу повинні обиратися з числа осіб, які подали свою кандидатуру в рамках процедури добору, інформація про яку має бути оприлюднена на вебсайтах Сенату Республіки, Палати депутатів і Органу у сфері захисту персональних даних принаймні за шість днів до призначення
Естонія	публічний конкурс, кандидата висуває Міністерство юстиції
Хорватія	кандидата висуває уряд
Республіка Кіпр	Стаття 19(1) Закону 125(I)/2018: «Уповноваженого з питань захисту персональних даних призначає Рада міністрів за рекомендацією міністра»
Литва	Публічний конкурс (не враховуючи деяких винятків у застосуванні Закону Литви про державну службу). Кандидата призначає на посаду уряд
Ісландія	кандидата висуває уряд
Греція	кандидата висуває парламент
Князівство Ліхтенштейн	кандидата висуває уряд
Португалія	кандидата висуває парламент
Велике Герцогство Люксембург	кандидата висуває уряд
Латвія	проводиться публічний конкурс, кандидата висуває номінаційний комітет державних службовців вищого рівня
Чеська Республіка	кандидата висуває парламент
Австрія	кандидата висуває уряд
Республіка Словенія	кандидата висуває президент
Болгарія	проводиться публічний конкурс, кандидата висуває номінаційний комітет державних службовців вищого рівня, кандидата висуває уряд

8. Будь ласка, вкажіть підстави для припинення повноважень / звільнення керівника / членів вашого наглядового органу у сфері захисту персональних даних:

Норвегія	закінчення терміну перебування на посаді, відставка, у разі серйозного проступку
Словацька Республіка	закінчення терміну перебування на посаді, відставка, обов'язковий вихід на пенсію, у разі серйозного проступку
Румунія	закінчення терміну перебування на посаді, відставка, обов'язковий вихід на пенсію, у разі серйозного проступку, керівник / член органу більше не дотримується умов, що обов'язкові для виконання ним/нею своїх обов'язків
Італія	закінчення терміну перебування на посаді, відставка, обов'язковий вихід на пенсію, у разі серйозного проступку, керівник / член органу більше не дотримується умов, що обов'язкові для виконання ним/нею своїх обов'язків
Естонія	закінчення терміну перебування на посаді, відставка, обов'язковий вихід на пенсію, у разі серйозного проступку, керівник / член органу більше не дотримується умов, що обов'язкові для виконання ним/нею своїх обов'язків на цій посаді
Хорватія	Згідно зі статтею 9 Закону про виконання Загального регламенту про захист даних парламент Хорватії звільняє особу від виконання обов'язків директора або заступника директора до завершення терміну перебування на посаді, на яку вони були призначені: – за його або її власною заявою, – у разі виникнення обставин, через які він або вона більше не виконують умов перебування на посаді, – якщо він або вона скоїли серйозний проступок. Вважається, що директор або заступник директора скоїли серйозний проступок, якщо він або вона не виконують своїх обов'язків відповідно до вимог закону. Процедура звільнення від виконання обов'язків директора або заступника директора розпочинається за пропозицією уряду Республіки Хорватії
Республіка Кіпр	закінчення терміну перебування на посаді, відставка, обов'язковий вихід на пенсію, у разі серйозного проступку, керівник / член органу більше не дотримується умов, що обов'язкові для виконання ним/нею своїх обов'язків на цій посаді. Згідно зі статтею 20 Закону 125(I)/2018 «Уповноважений звільняється з посади, якщо під час її обіймання він або вона: – вчиняє будь-яку дію, що несумісна з обов'язками Уповноваженого, або долучається до будь-якого виду діяльності, за винагороду або без неї, що несумісний з посадою Уповноваженого; або за рішенням суду він або вона визнані винними у скоєнні злочину, передбаченого пунктом (3) розділу 21 цього Закону»

Литва	закінчення терміну перебування на посаді, відставка, обов'язковий вихід на пенсію, у разі серйозного проступку, керівник / член органу більше не дотримується умов, що обов'язкові для виконання ним/нею своїх обов'язків на цій посаді
Ісландія	закінчення строку повноважень, вихід на пенсію за віком, скоєння серйозного проступку
Греція	закінчення строку повноважень, відставка, скоєння серйозного проступку, відповідно до статті 12 Закону 4624/2019 (доступний за посиланням: www.dpa.gr (EN) > Information > Legal Framework) «будь-яка особа, яка після свого призначення на посаду: (a) набуває однієї з функцій, що становлять перешкоду для призначення, зазначеного в пункті 1; (b) вчиняє дії або виконує будь-яку роботу чи проєкт, або набуває іншої здатності, яка, на думку органу, несумісна з його / її обов'язками члена органу, автоматично позбавляється права обіймати посаду голови, заступника голови або члена органу»
Князівство Ліхтенштейн	закінчення строку повноважень, відставка, скоєння серйозного проступку
Португалія	закінчення строку повноважень, відставка, вихід на пенсію за віком, скоєння серйозного проступку
Велике Герцогство Люксембург	закінчення строку повноважень, відставка, скоєння серйозного проступку, якщо керівник / член більше не відповідає умовам, необхідним для виконання його обов'язків
Латвія	закінчення строку повноважень, відставка, скоєння серйозного проступку, якщо керівник / член більше не відповідає умовам, необхідним для виконання його обов'язків
Чеська Республіка	закінчення строку повноважень
Австрія	Лише передбачено, що звільняти керівника з посади має федеральний президент за пропозицією федерального уряду.
Республіка Словенія	закінчення строку повноважень, відставка, скоєння серйозного проступку, якщо керівник / член більше не відповідає умовам, необхідним для виконання його обов'язків
Болгарія	закінчення строку повноважень, відставка, вихід на пенсію за віком, скоєння серйозного проступку, якщо керівник / член більше не відповідає умовам, необхідним для виконання його обов'язків

9. Вкажіть, будь ласка, які питання регулюються законодавчим актом, ухваленим парламентом (наприклад, Законом про захист персональних даних або іншим документом):

Норвегія	процедура призначення керівника / членів наглядового органу
Словацька Республіка	обов'язкові кваліфікаційні вимоги та умови для призначення на посаду керівника / членів наглядового органу, термін перебування на посаді керівника / членів наглядового органу, підстави для звільнення з посади керівника / членів наглядового органу, заробітна плата керівника / членів наглядового органу
Румунія	процедура призначення керівника / членів наглядового органу, обов'язкові кваліфікаційні вимоги та умови для призначення на посаду керівника / членів наглядового органу, термін перебування на посаді керівника / членів наглядового органу, підстави для звільнення з посади керівника / членів наглядового органу, процедура звільнення з посади керівника / членів наглядового органу, кадрова політика (наприклад, право самостійно наймати працівників тощо)
Італія	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови, дотримання яких є необхідне для призначення на посаду керівника / членів наглядового органу, термін перебування на посаді керівника / членів наглядового органу, кадрова політика (наприклад, право самостійно наймати працівників тощо), розмір заробітної плати керівника / членів наглядового органу
Естонія	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови, дотримання яких вимагається для призначення на посаду керівника / членів наглядового органу, термін перебування на посаді керівника / членів наглядового органу, процедура звільнення керівника / членів наглядового органу
Хорватія	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови, дотримання яких вимагається для призначення на посаду керівника / членів наглядового органу, термін перебування на посаді керівника / членів наглядового органу, підстави для звільнення керівника / членів наглядового органу, процедура звільнення керівника / членів наглядового органу, бюджетні (фінансові) процедури, кадрова політика (наприклад, право самостійно наймати працівників тощо), розмір заробітної плати керівника / членів наглядового органу
Республіка Кіпр	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови, дотримання яких є вимагається для призначення на посаду керівника / членів наглядового органу, термін перебування на посаді керівника / членів наглядового органу, підстави для звільнення керівника / членів наглядового органу, процедура звільнення керівника / членів наглядового органу, кадрова політика (наприклад, право самостійно наймати працівників тощо)

Литва	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови, дотримання яких вимагається для призначення на посаду керівника / членів наглядового органу, термін перебування на посаді керівника / членів наглядового органу, підстави для звільнення керівника / членів наглядового органу, процедура звільнення керівника / членів наглядового органу, бюджетні (фінансові) процедури, кадрова політика (наприклад, право самостійно наймати своїх працівників тощо), розмір заробітної плати керівника / членів наглядового органу
Ісландія	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови прийнятності, необхідні для призначення на посаду керівника / члена наглядового органу, строк повноважень керівника / членів наглядового органу, підстави для звільнення з посади керівника / членів наглядового органу, кадрова політика (наприклад, право самостійно наймати власних працівників тощо)
Греція	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови прийнятності, необхідні для призначення на посаду керівника / члена наглядового органу, строк повноважень керівника / членів наглядового органу, підстави для звільнення з посади керівника / членів наглядового органу, процедура звільнення з посади керівника / членів наглядового органу, бюджетні (фінансові) процедури, кадрова політика (наприклад, право самостійно наймати власних працівників тощо), зарплата керівника / членів наглядового органу
Князівство Ліхтенштейн	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови прийнятності, необхідні для призначення на посаду керівника / члена наглядового органу, строк повноважень керівника / членів наглядового органу, підстави для звільнення з посади керівника / членів наглядового органу, процедура звільнення з посади керівника / членів наглядового органу, бюджетні (фінансові) процедури, кадрова політика (наприклад, право самостійно наймати власних працівників тощо)
Португалія	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови прийнятності, необхідні для призначення на посаду керівника / члена наглядового органу, строк повноважень керівника / членів наглядового органу, підстави для звільнення з посади керівника / членів наглядового органу, процедура звільнення з посади керівника / членів наглядового органу, бюджетні (фінансові) процедури, кадрова політика (наприклад, право самостійно наймати власних працівників тощо), зарплата керівника / членів наглядового органу
Велике Герцогство Люксембург	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови прийнятності, необхідні для призначення на посаду керівника / члена наглядового органу, строк повноважень керівника / членів наглядового органу, підстави для звільнення з посади керівника / членів наглядового органу, процедура звільнення з посади керівника / членів наглядового органу, бюджетні (фінансові) процедури, кадрова політика (наприклад, право самостійно наймати власних працівників тощо), зарплата керівника / членів наглядового органу
Латвія	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови прийнятності, необхідні для призначення на посаду керівника / члена наглядового органу, строк повноважень керівника / членів наглядового органу, підстави для звільнення з посади керівника / членів наглядового органу, процедура звільнення з посади керівника / членів наглядового органу, кадрова політика (наприклад, право самостійно наймати власних працівників тощо), зарплата керівника / членів наглядового органу
Чеська Республіка	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови прийнятності, необхідні для призначення на посаду керівника / члена наглядового органу, строк повноважень керівника / членів наглядового органу, бюджетні (фінансові) процедури
Австрія	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови прийнятності, необхідні для призначення на посаду керівника / члена наглядового органу, строк повноважень керівника / членів наглядового органу
Республіка Словенія	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови прийнятності, необхідні для призначення на посаду керівника / члена наглядового органу, строк повноважень керівника / членів наглядового органу, підстави для звільнення з посади керівника / членів наглядового органу, процедура звільнення з посади керівника / членів наглядового органу, бюджетні (фінансові) процедури, кадрова політика (наприклад, право самостійно наймати власних працівників тощо), зарплата керівника / членів наглядового органу
Болгарія	процедура призначення керівника / членів наглядового органу, кваліфікаційні вимоги та умови прийнятності, необхідні для призначення на посаду керівника / члена наглядового органу, строк повноважень керівника / членів наглядового органу, підстави для звільнення з посади керівника / членів наглядового органу, бюджетні (фінансові) процедури, зарплата керівника / членів наглядового органу

10. Який строк повноважень керівника / членів наглядового органу у сфері захисту персональних даних:

Норвегія	6 років
Словацька Республіка	5 років
Румунія	5 років
Італія	Сім років (без права переобрання). Будь ласка, зверніть увагу, що цей термін передбачений розділом 47-с Закону № 31/2008. Останнім були внесені зміни до положення щодо терміну перебування на посадах уповноважених, яких призначають у деякі незалежні органи (сім років), зокрема членів органу з питань захисту даних. Термін перебування на посаді, чинний раніше, становив чотири роки з правом одноразового переобрання на такий самий строк
Естонія	5 років
Хорватія	4 роки
Республіка Кіпр	6 років
Литва	5 років
Ісландія	5 років, рада директорів складається з членів, яких призначають на 5-річний термін, що може бути продовжений двічі (загалом – 15 років). Уповноваженого призначають на 5-річний термін, але без обмежень права повторного призначення
Греція	6 років
Князівство Ліхтенштейн	6 років
Португалія	5 років
Велике Герцогство Люксембург	6 років
Латвія	5 років
Чеська Республіка	5 років
Австрія	5 років
Республіка Словенія	5 років
Болгарія	5 років

11. Керівник / члени наглядового органу у сфері захисту персональних даних:

Норвегія	На цей час може бути переобраний, але ця норма наразі переглядається, бо можливість переобрання піддає ризикові його незалежність
Словацька Республіка	можуть бути переобрані на два терміни
Румунія	президент може бути переобраний на цю посаду лише один раз
Італія	не може / не можуть бути призначені на другий термін
Естонія	не врегульовано
Хорватія	може бути переобраний на цю посаду двічі
Республіка Кіпр	може / можуть бути переобрані на цю посаду двічі
Литва	може / можуть бути двічі переобрані на цю посаду
Ісландія	має / мають право на повторне призначення ще на два терміни, Роз'яснення для уникнення плутанини: вони мають право на повторне призначення ще на три терміни.
Греція	не має / мають права на повторне призначення
Князівство Ліхтенштейн	має / мають право на повторне призначення без обмежень за кількістю термінів
Португалія	має / мають право на повторне призначення ще на два терміни
Велике Герцогство Люксембург	має / мають право на повторне призначення ще на два терміни
Латвія	має / мають право на повторне призначення ще на два терміни
Чеська Республіка	має / мають право на повторне призначення ще на два терміни
Австрія	Нема вказівок про обмеження на повторне призначення
Республіка Словенія	має / мають право на повторне призначення ще на два терміни
Болгарія	має / мають право на повторне призначення ще на два терміни

12. Будь ласка, вкажіть статус працівників офісу наглядового органу у сфері захисту персональних даних (можна надати кілька відповідей):

Норвегія	працівники – державні службовці; гарантована законом незалежність у процесуальних питаннях, працівники наймаються на роботу на підставі трудового договору
Словацька Республіка	посадові особи – державні службовці; гарантована законом незалежність у процесуальних питаннях
Румунія	посадові особи – працівники, яких наймають на роботу на підставі трудового договору
Італія	посадові особи – працівники, яких приймають на роботу на підставі трудового договору
Естонія	посадові особи – державні службовці; гарантована законом незалежність у процесуальних питаннях
Хорватія	посадові особи – державні службовці; законом гарантована незалежність у процесуальних питаннях
Республіка Кіпр	Згідно зі статтею 22 Закону 125(I)/2018. «Уповноважений має секретаріат, працівників якого можуть наймати на підставі постійного, тимчасового або безстрокового трудового договору і вони державні службовці»
Литва	посадові особи – державні службовці; гарантована законом незалежність у процесуальних питаннях, посадових осіб наймають на роботу на підставі трудового договору
Ісландія	посадові особи – працівники, які працюють за трудовим договором
Греція	посадові особи – державні службовці; мають гарантовану законом незалежність у процедурних питаннях. Працівники призначаються на посади, визначені організаційною структурою органу, та мають трудові правовідносини, що регулюються публічним чи приватним правом без обмежень щодо строку повноважень
Князівство Ліхтенштейн	посадові особи – державні службовці; мають гарантовану законом незалежність у процедурних питаннях
Португалія	посадові особи – державні службовці; мають гарантовану законом незалежність у процедурних питаннях
Велике Герцогство Люксембург	посадові особи – державні службовці; мають гарантовану законом незалежність у процедурних питаннях
Латвія	посадові особи – державні службовці; мають гарантовану законом незалежність у процедурних питаннях, посадові особи – працівники, які працюють за трудовим договором
Чеська Республіка	посадові особи – державні службовці; мають гарантовану законом незалежність у процедурних питаннях, посадові особи – працівники, які працюють за трудовим договором
Австрія	посадові особи – працівники, які працюють за трудовим договором
Республіка Словенія	посадові особи – державні службовці; мають гарантовану законом незалежність у процедурних питаннях
Болгарія	посадові особи – державні службовці; мають гарантовану законом незалежність у процедурних питаннях, посадові особи – працівники, які працюють за трудовим договором

13. Будь ласка, вкажіть рівень заробітної плати працівників офісу наглядового органу у сфері захисту персональних даних:

Норвегія	рівень заробітної плати може бути вищим за середню зарплату державних службовців державного сектору
Словацька Республіка	рівень заробітної плати дорівнює середній зарплаті державних службовців у державному секторі
Румунія	не застосовується
Італія	рівень заробітної плати визначається у процентному відношенні до зарплат в інших наглядових органах
Естонія	рівень заробітної плати дорівнює середньому рівневі зарплати державних службовців у державному секторі
Хорватія	рівень заробітної плати дорівнює середній зарплаті державних службовців у державному секторі, рівень заробітної плати дорівнює середній зарплаті найманих працівників у державному секторі
Республіка Кіпр	рівень заробітної плати дорівнює середньому рівневі зарплати державних службовців у державному секторі
Литва	рівень заробітної плати дорівнює середньому рівневі зарплати державних службовців у державному секторі
Ісландія	рівень заробітної плати – середній серед усіх зайнятих у державному секторі
Греція	рівень заробітної плати – середній серед державних службовців у державному секторі

Князівство Ліхтенштейн	рівень заробітної плати – середній серед державних службовців у державному секторі
Португалія	рівень заробітної плати – середній серед державних службовців у державному секторі
Велике Герцогство Люксембург	рівень заробітної плати – середній серед державних службовців у державному секторі, рівень заробітної плати – середній серед усіх зайнятих у державному секторі
Латвія	рівень заробітної плати – середній серед державних службовців у державному секторі
Чеська Республіка	
Австрія	рівень заробітної плати – середній серед усіх зайнятих у державному секторі
Республіка Словенія	рівень заробітної плати – середній серед державних службовців у державному секторі
Болгарія	рівень заробітної плати – середній серед державних службовців у державному секторі

14. Будь ласка, вкажіть кому доповідає керівник вашого наглядового органу у сфері захисту персональних даних:

Норвегія	парламентові, урядові
Словацька Республіка	парламентові
Румунія	президент національного наглядового органу представляє щороку доповіді про свою діяльність на пленарному засіданні Сенату
Італія	Орган у сфері захисту даних Італії (ОЗД) подає свою щорічну доповідь урядові та парламентові, як зазначено нижче. У рамках взаємодії парламент/уряд проводять консультації з Органом у сфері захисту даних перед ухваленням законодавчих актів, які матимуть вплив на захист даних; у разі необхідності, ОЗД може привернути увагу уряду і парламенту до потреби в ухваленні конкретних законів або інших нормативних актів у різних сферах; ОЗД бере участь в обговореннях з питань законотворчої діяльності в рамках слухань у парламенті.
Естонія	парламентові
Хорватія	парламентові
Республіка Кіпр	уповноважений з питань захисту персональних даних – незалежний наглядовий орган
Литва	урядові, міністрові юстиції
Ісландія	Через те що ОЗД – незалежний орган, уповноважений ні перед ким не звітує, крім бюджетних питань. Однак ОЗД зобов'язаний надсилати річний звіт урядові та парламентові.
Греція	перед парламентом
Князівство Ліхтенштейн	перед парламентом
Португалія	перед парламентом
Велике Герцогство Люксембург	перед парламентом
Латвія	перед парламентом, урядом
Чеська Республіка	перед парламентом
Австрія	перед урядом
Республіка Словенія	перед парламентом
Болгарія	перед парламентом

15. Щорічна доповідь про діяльність вашого наглядового органу у сфері захисту персональних даних (можна надати кілька відповідей):

Норвегія	подається урядові, подається парламентові, затверджує парламент, доводиться до відома громадськості
Словацька Республіка	подається урядові, подається парламентові, доводиться до відома громадськості
Румунія	подається урядові, подається парламентові. Щорічна доповідь подається Сенатові Румунії, Палаті депутатів, урядові Румунії, Європейській комісії та Європейській раді із захисту даних
Італія	подається урядові, подається парламентові. Щорічна доповідь публікується на сайті ОЗД www.garanteprivacy.it
Естонія	подається парламентові, подається іншому органові, подається канцлерові юстиції та Конституційному комітету парламенту
Хорватія	подається парламентові

Республіка Кіпр	Відповідно до статті 26 Закону 125(I)/2018. «Комісар подає щорічну доповідь про свою діяльність президентові Республіки та голові Палати представників, доповідь має бути також опублікована на вебсайті Секретаріату»
Литва	подається урядові, подається парламентові, доводиться до відома громадськості
Ісландія	направляється урядові, направляється парламентові, доводиться до відома громадськості
Греція	направляється парламентові, доводиться до відома громадськості, також направляється прем'єр-міністрові
Князівство Ліхтенштейн	направляється урядові, направляється парламентові, схвалюється парламентом, доводиться до відома громадськості
Португалія	доводиться до відома громадськості
Велике Герцогство Люксембург	направляється урядові, направляється парламентові, доводиться до відома громадськості
Латвія	направляється урядові, направляється парламентові, доводиться до відома громадськості
Чеська Республіка	направляється парламентові, доводиться до відома громадськості
Австрія	направляється урядові, доводиться до відома громадськості
Республіка Словенія	направляється парламентові, також направляється Європейській раді із захисту даних (GDPR)
Болгарія	направляється парламентові, схвалюється парламентом, доводиться до відома громадськості, Європейській раді із захисту даних (GDPR)

16. Будь ласка, вкажіть з якою періодичністю керівник наглядового органу у сфері захисту персональних даних доповідає про свою діяльність:

Норвегія	раз на рік
Словацька Республіка	раз на рік
Румунія	раз на рік
Італія	раз на рік
Естонія	раз на рік
Хорватія	раз на рік
Республіка Кіпр	раз на рік
Литва	раз на рік
Ісландія	один раз на рік
Греція	один раз на рік
Князівство Ліхтенштейн	один раз на рік
Португалія	один раз на рік
Велике Герцогство Люксембург	один раз на рік
Латвія	один раз на рік
Чеська Республіка	один раз на рік
Австрія	один раз на рік
Республіка Словенія	один раз на рік
Болгарія	один раз на рік

17. Чи наділений ваш наглядовий орган у сфері захисту персональних даних повноваженнями щодо нагляду за:

Норвегія	обробкою даних уповноваженими органами для запобігання, розслідування, виявлення або переслідування за кримінальні правопорушення, органами з виконання кримінальних покарань
Словацька Республіка	доступом широкої громадськості до офіційних документів, обробкою даних уповноваженими органами для запобігання, розслідування, виявлення або переслідування за кримінальні правопорушення, органами з виконання кримінальних покарань
Румунія	обробкою даних для журналістських цілей та цілей самовираження в науковій, художній чи літературній сферах, обробкою даних уповноваженими органами для запобігання, розслідування, виявлення або переслідування за кримінальні правопорушення, виконання кримінальних покарань, захисту конфіденційності в сфері використання електронних засобів зв'язку. У контексті обробки даних для журналістських цілей та цілей самовираження в науковій, художній чи літературній сферах ми беремо до уваги статтю 85 Регламенту та статтю 7 Закону № 190/2018

Італія	обробкою даних для журналістських цілей та цілей самовираження в науковій, художній чи літературній сферах, обробкою даних уповноваженими органами для запобігання, розслідування, виявлення або переслідування за кримінальні правопорушення, виконання кримінальних покарань, обробкою даних для цілей національної безпеки й оборони, захисту конфіденційності у сфері використання електронних засобів зв'язку
Естонія	обробкою даних для журналістських цілей та цілей самовираження в науковій, художній чи літературній сферах, обробкою даних уповноваженими органами для запобігання, розслідування, виявлення або переслідування за кримінальні правопорушення, виконання кримінальних покарань, обробкою даних для цілей національної безпеки та оборони, захисту конфіденційності у сфері використання електронних засобів зв'язку. Конкретніша інформація щодо сфери застосування Закону про захист персональних даних Естонії і Регламенту міститься у статті 2 цього Закону: https://www.riigiteataja.ee/en/eli/523012019001/consolide
Хорватія	Відповідно до статті 36 Закону про виконання Загального регламенту про захист даних уповноважені працівники Агентства можуть самостійно, а в деяких справах також за участю представника іншого наглядового органу, який надає їм підтримку (далі – уповноважені особи), проводити інспекції з попереднім повідомленням і без попередження. Особа, щодо якої ведеться перевірка, і контролер або оператор даних мають бути поінформовані про інспекцію без попередження на місці та під час її проведення
Республіка Кіпр	обробкою даних для журналістських цілей та цілей самовираження в науковій, художній чи літературній сферах, обробкою даних уповноваженими органами для запобігання, розслідування, виявлення або переслідування за кримінальні правопорушення, виконання кримінальних покарань, обробкою даних для цілей національної безпеки та оборони. Інформаційний комісар – наглядовий орган, уповноважений вести нагляд за реалізацією права на доступ до офіційних документів. Завдання і повноваження, покладені на інформаційного комісара, виконує відповідний уповноважений з питань захисту персональних даних
Литва	обробкою даних уповноваженими органами для запобігання, розслідування, виявлення або переслідування за кримінальні правопорушення, органами з виконання кримінальних покарань, захисту конфіденційності у сфері використання електронних засобів зв'язку
Ісландія	опрацюванням даних компетентними органами для запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, виконання кримінальних покарань
Греція	опрацюванням даних для цілях журналістики та з метою академічного, художнього чи літературного вираження, опрацюванням даних компетентними органами для запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, виконання кримінальних покарань, опрацюванням даних для цілей національної безпеки та оборони, захистом конфіденційності в секторі електронних комунікацій
Князівство Ліхтенштейн	опрацюванням даних компетентними органами для запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, виконання кримінальних покарань, захистом конфіденційності в секторі електронних комунікацій
Португалія	опрацюванням даних для цілей журналістики та з метою академічного, художнього чи літературного вираження, доступом громадськості до офіційних документів, опрацюванням даних компетентними органами для запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, виконання кримінальних покарань, опрацюванням даних для цілей національної безпеки та оборони, захистом конфіденційності в секторі електронних комунікацій
Велике Герцогство Люксембург	опрацюванням даних для цілей журналістики та з метою академічного, художнього чи літературного вираження, опрацюванням даних компетентними органами для запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, виконання кримінальних покарань, опрацюванням даних для цілей національної безпеки та оборони, захистом конфіденційності в секторі електронних комунікацій
Латвія	опрацюванням даних для цілей журналістики та з метою академічного, художнього чи літературного вираження, опрацюванням даних компетентними органами для запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, виконання кримінальних покарань, захистом конфіденційності в секторі електронних комунікацій; нагляд за опрацюванням даних для цілей журналістики лише частково входить у компетенцію наглядового органу
Чеська Республіка	опрацюванням даних для цілей журналістики та з метою академічного, художнього чи літературного вираження, доступом громадськості до офіційних документів, опрацюванням даних компетентними органами для запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, виконання кримінальних покарань, захистом конфіденційності в секторі електронних комунікацій
Австрія	опрацюванням даних компетентними органами для запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, виконання кримінальних покарань, опрацюванням даних для цілей національної безпеки та оборони, захистом конфіденційності в секторі електронних комунікацій, опрацюванням даних з метою академічного, художнього чи літературного вираження
Республіка Словенія	опрацюванням даних для цілей журналістики та з метою академічного, художнього чи літературного вираження, доступом громадськості до офіційних документів, опрацюванням даних компетентними органами для запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, виконання кримінальних покарань, опрацюванням даних для цілей національної безпеки та оборони

Болгарія	опрацюванням даних для цілей журналістики та з метою академічного, художнього чи літературного вираження, опрацюванням даних компетентними органами для запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, виконання кримінальних покарань, захистом конфіденційності в секторі електронних комунікацій

18. Вкажіть, будь ласка, якими повноваженнями з проведення розслідувань наділений ваш наглядовий орган у сфері захисту персональних даних:

Норвегія	дати вказівки контролерові й операторові даних і, в разі потреби, їхньому представникові щодо надання будь-якої інформації, необхідної для виконання завдань наглядового органу у сфері захисту персональних даних; отримати від контролера / оператора даних доступ до інформаційних баз і систем зберігання документів, обладнання та засобів для обробки даних; отримати доступ, за умови попереднього письмового повідомлення, до приміщень / території контролера / оператора даних; отримати доступ, без попереднього повідомлення, до приміщень / території контролера / оператора даних; у будь-який час мати доступ до приміщень / території юридичної особи
Словацька Республіка	давати вказівки контролерові та операторові даних і, в разі потреби, їхньому представникові щодо надання будь-якої інформації, необхідної для виконання завдань наглядового органу у сфері захисту персональних даних; давати вказівки будь-якій фізичній або юридичній особі (крім контролера та оператора) щодо надання будь-якої інформації, необхідної для виконання завдань наглядового органу у сфері захисту персональних даних; отримати від контролера та оператора даних доступ до інформаційних баз і систем зберігання документів, обладнання та засобів для обробки даних; проводити обшуки та вилучення у приміщеннях оператора / контролера даних без ухвали суду про надання відповідного дозволу; проводити обшуки та вилучення в приміщеннях контролера / оператора даних після отримання ухвали суду про надання відповідного дозволу; отримати доступ, за умови попереднього письмового повідомлення, до приміщень / території контролера / оператора даних; у будь-який час мати доступ до приміщень / території юридичної особи
Румунія	давати вказівки контролерові та операторові даних і, в разі потреби, їхньому представникові щодо надання будь-якої інформації, необхідної для виконання завдань наглядового органу у сфері захисту персональних даних; отримати від контролера / оператора даних доступ до інформаційних баз і систем зберігання документів, обладнання та засобів для обробки даних; отримати доступ, без попереднього повідомлення, до приміщень / території контролера / оператора даних; отримати доступ до приміщень / території юридичної особи лише в робочий час цієї юридичної особи. Контрольна діяльність Наглядового органу Румунії передбачена розділом IV глави 1 Закону № 102/2005, повторно опублікована версія. Стаття 14 (2) Закону № 102/2005 передбачає, що персонал, уповноважений вести контроль, має право проводити розслідування, зокрема позапланові, запитувати та отримувати від контролера та оператора даних, а також, у разі необхідності, від їхнього представника, на місці та/або протягом визначеного строку, будь-яку інформацію та документи, незалежно від носія даних, вилучати їх копії, мати доступ до будь-якого приміщення контролера та оператора даних, а також мати доступ та перевірити будь-яке обладнання, програмний носій або носій для збереження даних, необхідні для проведення розслідування згідно із законом. Пунктом (3) цієї ж статті передбачено, що, коли персоналові, уповноваженому вести контроль, будь-яким чином перешкоджають виконувати завдання, передбачені пунктом (2), Національний наглядовий орган може вимагати судового дозволу, що надає голова Бухарестського апеляційного суду або суддя, якому він делегував цю функцію. Крім того, ідентифікація та збереження об'єктів, а також накладення печаток проводиться відповідно до положень Закону № 135/2010 про затвердження Кримінального процесуального кодексу з наступними змінами та доповненнями. Поряд з цим, Наглядовий орган Румунії може дати вказівку про проведення експертизи та заслуховування осіб, свідчення яких вважаються актуальними та необхідними в рамках проведення розслідування
Італія	Для надання правильної відповіді на це запитання ми вважаємо за краще не зазначати окремі варіанти відповідей (бо вони лише частково відображують повноваження ОЗД Італії), але відсилаємо до статті 158 Кодексу захисту даних, який можна знайти за цим посиланням: https://www.garanteprivacy.it/documents/10160/0/Data+Protection+Code.pdf/7f4dc718-98e4-1af5-fb44-16a313f4e70f?version=1.3
Естонія	давати вказівки контролерові та операторові даних і, в разі потреби, їхньому представникові щодо надання будь-якої інформації, необхідної для виконання завдань наглядового органу у сфері захисту персональних даних; давати вказівки будь-якій фізичній або юридичній особі (крім контролера та оператора) щодо надання будь-якої інформації, необхідної для виконання завдань наглядового органу у сфері захисту персональних даних; отримати від контролера / оператора даних доступ до інформаційних баз і систем зберігання документів, обладнання та засобів для обробки даних; проводити обшуки та вилучення в приміщеннях контролера / оператора даних після отримання ухвали суду про надання відповідного дозволу; отримати доступ, за умови попереднього письмового повідомлення, до приміщень / території контролера / оператора даних; отримати без попереднього повідомлення доступ до приміщень / території контролера / оператора даних; у будь-який час мати доступ до приміщень / території юридичної особи; мати доступ до житлових приміщень фізичної особи (зокрема приміщень, що використовуються на підставі договору оренди або на будь-якій іншій підставі) за умови

	отримання ухвали суду про надання дозволу на допуск до цих житлових приміщень; у разі потреби залучати поліцію до виконання повноважень наглядового органу у сфері захисту даних
Хорватія	Відповідно до статті 58 Регламенту Агентство має такі повноваження з проведення розслідувань: (a) давати вказівки контролерові та операторові даних і, в разі потреби, їх представникові щодо надання будь-якої інформації, необхідної для виконання ним своїх завдань; (b) проводити розслідування у формі перевірок захисту даних; (c) переглядати сертифікації, видані згідно зі статтею 42(7); (d) повідомляти контролера і оператора даних про вірогідне порушення цього Регламенту; (e) отримувати від контролера і оператора даних доступ до всіх персональних даних і до всієї інформації, необхідної для виконання ним своїх завдань; (f) отримувати доступ до будь-яких приміщень контролера і оператора даних, зокрема до будь-якого обладнання і засобів обробки даних згідно з процесуальним законодавством Союзу чи держави-члена
Республіка Кіпр	давати вказівки контролерові та операторові даних і, в разі потреби, їхньому представникові щодо надання будь-якої інформації, необхідної для виконання завдань наглядового органу у сфері захисту персональних даних; давати вказівки будь-якій фізичній або юридичній особі (крім контролера і оператора даних) щодо надання будь-якої інформації, необхідної для виконання завдань наглядового органу у сфері захисту персональних даних; отримати від контролера / оператора даних доступ до інформаційних баз і систем зберігання документів, обладнання та засобів для обробки даних; отримати без попереднього повідомлення доступ до приміщень / території контролера / оператора даних; у будь-який час мати доступ до приміщень / території юридичної особи; у разі потреби залучати поліцію до виконання повноважень наглядового органу у сфері захисту даних. Згідно зі статтею 25(d) Закону 125(I)/2018 «Під час виконання своїх повноважень щодо проведення розслідувань уповноважений може вилучити документи або електронне обладнання на підставі розпорядження суду про проведення обшуку відповідно до вимог Кримінального процесуального законодавства»
Литва	давати вказівки контролерові та операторові даних і, в разі потреби, їхньому представникові щодо надання будь-якої інформації, необхідної для виконання завдань наглядового органу у сфері захисту персональних даних; давати вказівки будь-якій фізичній або юридичній особі (крім контролера і оператора даних) щодо надання будь-якої інформації, необхідної для виконання завдань наглядового органу у сфері захисту персональних даних; отримати від контролера / оператора даних доступ до інформаційних баз і систем зберігання документів, обладнання та засобів для обробки даних; проводити обшуки та вилучення в приміщеннях оператора /обробника даних без отримання ухвали суду про надання відповідного дозволу; отримати без попереднього повідомлення доступ до приміщень / території контролера / оператора даних; отримати доступ до приміщень / території юридичної особи лише в робочий час цієї юридичної особи; у будь-який час мати доступ до приміщень / території юридичної особи; мати доступ до житлових приміщень фізичної особи (зокрема приміщень, що використовуються на підставі договору оренди або на будь-якій іншій підставі) лише за умови отримання ухвали суду про надання дозволу на допуск до цих житлових приміщень; у разі потреби залучати поліцію до виконання повноважень наглядового органу у сфері захисту даних
Ісландія	видавати розпорядження контролерові та операторові і, якщо це можливо, їхньому представникові надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, отримувати в контролера / оператора доступ до банків даних і систем реєстрації, обладнання та засобів опрацювання даних, отримувати доступ (за умови попереднього письмового повідомлення) до приміщень / території контролера / оператора, отримувати доступ (без попереднього повідомлення) до приміщень / території контролера / оператора, отримувати доступ до приміщень / території юридичних осіб у будь-який час, за потреби залучати поліцію для виконання своїх повноважень наглядового органу з питань захисту даних
Греція	видавати розпорядження контролерові та операторові і, якщо це можливо, їхньому представникові надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, видавати розпорядження будь-якій фізичній та / або юридичній особі (яка не контролер чи оператор) надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, отримувати в контролера / оператора доступ до банків даних і систем реєстрації, обладнання та засобів опрацювання даних, проводити обшуки та вилучення у приміщеннях контролера / оператора даних без отримання судового розпорядження, проводити обшуки та вилучення у приміщеннях контролера / оператора даних після отримання судового розпорядження, отримувати доступ (за умови попереднього письмового повідомлення) до приміщень / території контролера / оператора, отримувати доступ (без попереднього повідомлення) до приміщень / території контролера / оператора, отримувати доступ до приміщень / території юридичної особи лише в робочий час цієї юридичної особи, отримувати доступ до приміщень / території юридичних осіб у будь-який час, за потреби залучати поліцію для виконання своїх повноважень наглядового органу з питань захисту даних; Ex officio або отримавши скаргу орган проводить розслідування та авдити, у ході яких під контроль підпадає технологічна інфраструктура та інші автоматизовані чи неавтоматизовані засоби, які допомагають опрацьовувати персональні дані. Проводячи такі розслідування та перевірки, орган має право отримувати від контролера та оператора доступ до всіх опрацьованих персональних даних та до всієї інформації, необхідної для цілей таких авдитів та для виконання своїх завдань, і цьому не може завадити жодне посилання на конфіденційність. Орган не має доступу до даних, що ідентифікують членів чи працівників організацій, про які йдеться в документах, що зберігаються для цілей національної безпеки або для розслідування особливо тяжких злочинів. 2) Орган також: (a) надсилає попередження контролерові чи операторові, (b) наказує контролерові чи операторові виконати положення

	законодавства про захист даних у встановленому порядку та протягом встановленого періоду, зокрема виправити чи стерти особисті дані; (c) наказує та накладає тимчасове чи остаточне обмеження або навіть заборону на опрацювання персональних даних; (d) наказує та розпоряджається передати йому документи, системи реєстрації, обладнання чи засоби для опрацювання персональних даних, а також їх зміст; (e) вилучає документи, інформацію, системи реєстрації кожної одиниці обладнання, а також їх зміст, якщо під час здійснення органом своїх наглядових повноважень йому стає відомо про порушення правил захисту персональних даних. Орган – секвестратор зазначеного матеріалу до моменту ухвалення компетентними судовими органами та органами прокуратури відповідного рішення. Також зазначається, що стосовно доступу до житлових приміщень стаття 9 Конституції Греції передбачає, що «не дозволяється проводити обшук житла, крім випадків, коли це визначено законом та завжди при представниках судової влади».
Князівство Ліхтенштейн	видавати розпорядження контролерові та операторові і, якщо це можливо, їхньому представникові надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, видавати розпорядження будь-якій фізичній та / або юридичній особі (яка не контролер чи оператор) надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, отримувати в контролера / оператора доступ до банків даних і систем реєстрації, обладнання та засобів опрацювання даних, отримувати доступ (за умови попереднього письмового повідомлення) до приміщень / території контролера / оператора, отримувати доступ до приміщень / території юридичної особи лише в робочий час цієї юридичної особи
Португалія	видавати розпорядження контролерові та операторові і, якщо це можливо, їхньому представникові надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, видавати розпорядження будь-якій фізичній та / або юридичній особі (яка не контролер чи оператор) надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, отримувати в контролера / оператора доступ до банків даних та систем реєстрації, обладнання та засобів опрацювання даних, проводити обшуки та вилучення у приміщеннях контролера / оператора даних без отримання судового розпорядження, отримувати доступ (без попереднього повідомлення) до приміщень / території контролера / оператора, отримувати доступ до приміщень / території юридичних осіб у будь-який час, отримувати доступ до житлових приміщень (разом з приміщеннями, які перебувають в оренді чи використовуються на будь-якій іншій основі) фізичної особи лише після пред'явлення судового розпорядження, що дозволяє проникнення до житлових приміщень, за потреби залучати поліцію для виконання своїх повноважень наглядового органу з питань захисту даних
Велике Герцогство Люксембург	видавати розпорядження контролерові та операторові і, якщо це можливо, їхньому представникові надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, отримувати в контролера / оператора доступ до банків даних і систем реєстрації, обладнання та засобів опрацювання даних, отримувати доступ (без попереднього повідомлення) до приміщень / території контролера / оператора, отримувати доступ до приміщень / території юридичної особи лише в робочий час цієї юридичної особи
Латвія	видавати розпорядження контролерові та операторові і, якщо це можливо, їхньому представникові надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, видавати розпорядження будь-якій фізичній та / або юридичній особі (яка не контролер чи оператор) надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, отримувати в контролера / оператора доступ до банків даних і систем реєстрації, обладнання та засобів опрацювання даних, отримувати доступ (за умови попереднього письмового повідомлення) до приміщень / території контролера / оператора, отримувати доступ до приміщень / території юридичної особи лише в робочий час цієї юридичної особи, за потреби залучати поліцію для виконання своїх повноважень наглядового органу з питань захисту даних
Чеська Республіка	видавати розпорядження контролерові та операторові і, якщо це можливо, їхньому представникові надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, видавати розпорядження будь-якій фізичній та / або юридичній особі (яка не контролер чи оператор) надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, проводити обшуки та вилучення у приміщеннях контролера / оператора даних після отримання судового розпорядження, отримувати доступ (за умови попереднього письмового повідомлення) до приміщень / території контролера / оператора
Австрія	видавати розпорядження контролерові та операторові і, якщо це можливо, їхньому представникові надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, видавати розпорядження будь-якій фізичній та / або юридичній особі (яка не контролер чи оператор) надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, отримувати в контролера / оператора доступ до банків даних і систем реєстрації, обладнання та засобів опрацювання даних, проводити обшуки та вилучення у приміщеннях контролера / оператора даних без отримання судового розпорядження, отримувати доступ (за умови попереднього письмового повідомлення) до приміщень / території контролера / оператора; з метою проведення перевірки орган з питань захисту даних має право (після повідомлення про це власника приміщення та контролера або оператора) проникати до приміщень, у яких опрацьовуються дані

Республіка Словенія	видавати розпорядження контролерові та операторові і, якщо це можливо, їхньому представникові надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, видавати розпорядження будь-якій фізичній та / або юридичній особі (яка не контролер чи оператор) надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, отримувати в контролера / оператора доступ до банків даних і систем реєстрації, обладнання та засобів опрацювання даних, проводити обшуки та вилучення у приміщеннях контролера / оператора даних без отримання судового розпорядження, проводити обшуки та вилучення у приміщеннях контролера / оператора даних після отримання судового розпорядження, отримувати доступ (без попереднього повідомлення) до приміщень / території контролера / оператора, отримувати доступ до приміщень / території юридичних осіб у будь-який час, отримувати доступ до житлових приміщень (разом з приміщеннями, які перебувають в оренді чи використовуються на будь-якій іншій основі) фізичної особи лише після пред'явлення судового розпорядження, що дозволяє проникнення до житлових приміщень, за потреби залучати поліцію для виконання своїх повноважень наглядового органу з питань захисту даних
Болгарія	видавати розпорядження контролерові та операторові і, якщо це можливо, їхньому представникові надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, видавати розпорядження будь-якій фізичній та / або юридичній особі (яка не контролер чи оператор) надати будь-яку інформацію, необхідну для виконання завдань наглядового органу з питань захисту даних, отримувати в контролера / оператора доступ до банків даних і систем реєстрації, обладнання та засобів опрацювання даних, проводити обшуки та вилучення у приміщеннях контролера / оператора даних без отримання судового розпорядження, за потреби залучати поліцію для виконання своїх повноважень наглядового органу з питань захисту даних

19. Будь ласка, зазначте повноваження щодо усунення виявлених порушень, якими наділений ваш наглядовий орган у сфері захисту персональних даних:

Норвегія	робити попередження контролерові та операторові даних про те, що заплановані операції з обробки даних, ймовірно, призведуть до порушення положення Регламенту; робити догани контролерові або оператору даних, якщо під час операцій з обробки даних були порушені положення Регламенту; давати вказівки контролерові або операторові даних щодо виконання запитів суб'єкта даних, пов'язаних з реалізацією його прав відповідно до Регламенту; надавати вказівки контролерові або операторові даних щодо увідповіднення операцій з обробки даних положенням Регламенту; у разі необхідності, визначеним способом і протягом визначеного терміну давати вказівки контролерові даних щодо інформування суб'єкта даних про факт порушення його права на захист персональних даних; запроваджувати тимчасове або остаточне обмеження, зокрема заборону на обробку даних; давати вказівки щодо виправлення або знищення персональних даних або застосування обмеження щодо їх обробки відповідно до статей 16, 17 і 18 та щодо повідомлення про такі дії одержувачів, яким персональні дані були розкриті на підставі статті 17 (2) та статті 19 Регламенту; відкликати сертифікацію або дати вказівку органові сертифікації відкликати сертифікацію, надану відповідно до статей 42 та 43 Регламенту; або дати вказівку органові сертифікації не надавати сертифікацію, якщо вимоги до сертифікації не виконуються або більше не виконуються; накладати адміністративний штраф відповідно до статті 83 Регламенту, на додаток до або замість заходів, зазначених у цьому пункті, залежно від обставин кожного окремого випадку; давати вказівки про призупинення потоків даних до одержувача в третій країні або міжнародної організації. Ми можемо також накладати штрафи, що підлягають примусовому виконанню
Словацька Республіка	робити попередження контролерові або операторові даних про те, що заплановані операції з обробки даних, ймовірно, призведуть до порушення положення Регламенту; давати вказівки контролерові або операторові даних щодо виконання запитів суб'єкта даних, пов'язаних з реалізацією його прав відповідно до Регламенту; надавати вказівки контролерові або операторові даних щодо увідповіднення операцій з обробки даних положенням Регламенту; у разі необхідності, визначеним способом і протягом визначеного терміну давати вказівки контролерові даних щодо інформування суб'єкта даних про факт порушення його права на захист персональних даних; запроваджувати тимчасове або остаточне обмеження, зокрема заборону на обробку даних; давати вказівки щодо виправлення або знищення персональних даних або застосування обмеження щодо їх обробки відповідно до статей 16, 17 і 18 та щодо повідомлення про такі дії одержувачів, яким персональні дані були розкриті на підставі статті 17 (2) та статті 19 Регламенту; відкликати сертифікацію або дати вказівку органові сертифікації відкликати сертифікацію, надану відповідно до статей 42 і 43 Регламенту; або дати вказівку органові сертифікації не надавати сертифікацію, якщо вимоги до сертифікації не виконуються або більше не виконуються; накладати адміністративний штраф відповідно до статті 83 Регламенту, на додаток до або замість заходів, зазначених у цьому пункті, залежно від обставин кожної окремої справи; давати вказівки про призупинення потоків даних до одержувача в третій країні або міжнародної організації

Румунія	робити попередження контролерові або операторові даних про те, що заплановані операції з обробки даних, ймовірно, призведуть до порушення положення Регламенту; робити догани контролерові або операторові даних, якщо під час операцій з обробки даних були порушені положення Регламенту; давати вказівки контролерові або операторові даних щодо виконання запитів суб'єкта даних, пов'язаних з реалізацією його прав відповідно до Регламенту; надавати вказівки контролерові або операторові даних щодо увідповіднення операцій з обробки даних положенням Регламенту; у разі необхідності, визначеним способом і протягом визначеного терміну давати вказівки контролерові даних щодо інформування суб'єкта даних про факт порушення його права на захист персональних даних; запроваджувати тимчасове або остаточне обмеження, зокрема заборону на обробку даних; давати вказівки щодо виправлення або знищення персональних даних або застосування обмеження щодо їх обробки відповідно до статей 16, 17 і 18 та щодо повідомлення про такі дії одержувачів, яким персональні дані були розкриті на підставі статті 17 (2) та статті 19 Регламенту; відкликати сертифікацію або дати вказівку органові сертифікації відкликати сертифікацію, надану відповідно до статей 42 та 43 Регламенту; або дати вказівку органові сертифікації не надавати сертифікацію, якщо вимоги до сертифікації не виконуються або більше не виконуються; накладати адміністративний штраф відповідно до статті 83 Регламенту, на додаток до або замість заходів, зазначених у цьому пункті, залежно від обставин кожної окремої справи; давати вказівки про призупинення потоків даних одержувачу в третій країні або міжнародній організації. Наглядовий орган Румунії наділений повноваженнями, передбаченими у статті 58 Регламенту
Італія	робити попередження контролерові або операторові даних про те, що заплановані операції з обробки даних, ймовірно, призведуть до порушення положення Регламенту; робити догани контролерові або операторові даних, якщо під час операцій з обробки даних були порушені положення Регламенту; давати вказівки контролерові або операторові даних щодо виконання запитів суб'єкта даних, пов'язаних з реалізацією його прав відповідно до Регламенту; надавати вказівки контролерові або операторові даних щодо увідповіднення операцій з обробки даних положенням Регламенту; у разі необхідності, визначеним способом і протягом визначеного терміну давати вказівки контролерові даних щодо інформування суб'єкта даних про факт порушення його права на захист персональних даних; запроваджувати тимчасове або остаточне обмеження, зокрема заборону на обробку даних; давати вказівки щодо виправлення чи знищення персональних даних або застосування обмеження стосовно їх обробки відповідно до статей 16, 17 і 18 та щодо повідомлення про такі дії одержувачів, яким персональні дані були розкриті на підставі статті 17 (2) та статті 19 Регламенту; відкликати сертифікацію або дати вказівку органові сертифікації відкликати сертифікацію, надану відповідно до статей 42 та 43 Регламенту, або дати вказівку органові сертифікації не надавати сертифікацію, якщо вимоги до сертифікації не виконуються або більше не виконуються; накладати адміністративний штраф відповідно до статті 83 Регламенту, на додаток до або замість заходів, зазначених у цьому пункті, залежно від обставин кожної конкретної справи; давати вказівки про призупинення потоків даних одержувачеві в третій країні або міжнародній організації
Естонія	робити попередження контролерові або операторові даних про те, що заплановані операції з обробки даних, ймовірно, призведуть до порушення положення Регламенту; робити догани контролерові або операторові даних, якщо під час операцій з обробки даних були порушені положення Регламенту; давати вказівки контролерові або операторові даних щодо виконання запитів суб'єкта даних, пов'язаних з реалізацією його або її прав відповідно до Регламенту; надавати вказівки контролерові або операторові даних щодо увідповіднення операцій з обробки даних положенням Регламенту; у разі необхідності, визначеним способом і протягом визначеного терміну давати вказівки контролерові даних щодо інформування суб'єкта даних про факт порушення його права на захист персональних даних; запроваджувати тимчасове або остаточне обмеження, зокрема заборону на обробку даних; давати вказівки щодо виправлення чи знищення персональних даних або застосування обмеження стосовно їх обробки відповідно до статей 16, 17 і 18 та щодо повідомлення про такі дії одержувачів, яким персональні дані були розкриті на підставі статті 17 (2) та статті 19 Регламенту; давати вказівки про призупинення потоків даних одержувачеві в третій країні або міжнародній організації. Законодавство Естонії містить положення щодо звільнення від сплати адміністративних штрафів, передбачених у Регламенті. Ми маємо право застосовувати штрафи за скоєння незначних правопорушень, судова система Естонії не передбачає адміністративних штрафів
Хорватія	робити попередження контролерові або операторові даних про те, що заплановані операції з обробки даних, ймовірно, призведуть до порушення положень Регламенту; робити догани контролерові або операторові даних, якщо під час операцій з обробки даних були порушені положення Регламенту; давати вказівки контролерові або операторові даних щодо виконання запитів суб'єкта даних, пов'язаних з реалізацією його або її прав відповідно до Регламенту; надавати вказівки контролерові або операторові даних щодо увідповіднення операцій з обробки даних положенням Регламенту; у разі необхідності, визначеним способом і протягом визначеного терміну давати вказівки контролерові даних щодо інформування суб'єкта даних про факт порушення його права на захист персональних даних; накладати тимчасове або остаточне обмеження, зокрема заборону на обробку даних; давати вказівки щодо виправлення чи знищення персональних даних або застосування обмеження стосовно їх обробки відповідно до статей 16, 17 і 18 та щодо повідомлення про такі дії одержувачів, яким персональні дані були розкриті на підставі статті 17 (2) та статті 19 Регламенту; відкликати сертифікацію чи наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43, або наказати

	органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконані або більше не виконуються; накладати адміністративні штрафи відповідно до статті 83 Регламенту, як доповнення до чи замість заходів, вказаних у цій частині статті, залежно від обставин кожної індивідуальної справи; давати вказівки про призупинення потоків даних одержувачеві в третій країні або міжнародній організації
Республіка Кіпр	робити попередження контролерові або операторові даних про те, що заплановані операції з обробки даних, ймовірно, призведуть до порушення положень Регламенту; робити догани контролерові або операторові даних, якщо під час операцій з обробки даних були порушені положення Регламенту; давати вказівки контролерові або операторові даних щодо виконання запитів суб'єкта даних, пов'язаних з реалізацією його або її прав відповідно до Регламенту; надавати вказівки контролерові або операторові даних щодо увідповіднення операцій з обробки даних положенням Регламенту; у разі необхідності, визначеним способом і протягом визначеного терміну давати вказівки контролерові даних щодо інформування суб'єкта даних про факт порушення його права на захист персональних даних; накладати тимчасове або остаточне обмеження, зокрема заборону на обробку даних; давати вказівки щодо виправлення чи знищення персональних даних або застосування обмеження стосовно їх обробки відповідно до статей 16, 17 і 18 та щодо повідомлення про такі дії одержувачів, яким персональні дані були розкриті на підставі статті 17 (2) та статті 19 Регламенту; відкликати сертифікацію чи наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43 Регламенту, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконані або більше не виконуються; накладати адміністративні штрафи відповідно до статті 83 Регламенту, як доповнення до чи замість заходів, наведених у цій частині статті, залежно від обставин кожної індивідуальної справи; давати вказівки про призупинення потоків даних одержувачеві в третій країні або міжнародній організації. Згідно зі статтею 25(f) Закону 125(I)/2018 «Уповноважений доповідає Європейській комісії про бездіяльність Організації з питань підвищення якості Кіпру в разі, якщо ця організація не відкликає акредитацію органу сертифікації відповідно до пунктів (3) і (4) цього Закону»
Литва	робити попередження контролерові або операторові даних про те, що заплановані операції з обробки даних, ймовірно, призведуть до порушення положень Регламенту; робити догани контролерові або операторові даних, якщо під час операцій з обробки даних були порушені положення Регламенту; давати вказівки контролерові або операторові даних щодо виконання запитів суб'єкта даних, пов'язаних з реалізацією його або її прав відповідно до Регламенту; надавати вказівки контролерові або операторові даних щодо увідповіднення операцій з обробки даних положенням Регламенту; у разі необхідності, визначеним способом і протягом визначеного терміну давати вказівки контролерові даних щодо інформування суб'єкта даних про факт порушення його права на захист персональних даних; накладати тимчасове або остаточне обмеження, зокрема заборону на обробку даних; давати вказівки щодо виправлення чи знищення персональних даних або застосування обмеження стосовно їх обробки відповідно до статей 16, 17 і 18 та щодо повідомлення про такі дії одержувачів, яким персональні дані були розкриті на підставі статті 17 (2) та статті 19 Регламенту; відкликати сертифікацію чи наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконані або більше не виконуються; накладати адміністративні штрафи відповідно до статті 83 Регламенту, як доповнення до чи замість заходів, вказаних у цій частині статті, залежно від обставин кожної індивідуальної справи; давати вказівки про призупинення потоків даних одержувачеві в третій країні або міжнародній організації. ДІЗД має повноваження з проведення розслідувань, передбачені статтею 58 Регламенту, а також право на застосування заходів, закріплених у статті 41 Закону Литовської Республіки про правовий захист персональних даних, що обробляються з метою запобігання, розслідування, виявлення або переслідування за кримінальні правопорушення, виконання кримінальних покарань, національної безпеки або оборони, що транспонує Директиву Європейського парламенту і Ради (ЄС) 2016/680 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних уповноваженими органами для цілей запобігання, розслідування, виявлення або переслідування за кримінальні правопорушення, виконання кримінальних покарань, і про вільний рух таких даних, та про скасування Рамкового рішення Ради 2008/977/JHA. Секретаріат інспектора з питань журналістської етики (далі – Секретаріат, https://www.zeit.lt/en) веде моніторинг застосування Регламенту і Закону Литовської Республіки про правовий захист персональних даних (далі – Закон) та забезпечує, щоб це законодавство застосовувалося до обробки персональних даних для журналістських, наукових, художніх чи літературних цілей. Секретаріат має повноваження, передбачені статтею 58 Регламенту, за винятком повноважень, закріплених у пунктах (b) і (c) частини (1), пунктах (e), (g), (h) та (j) частини (2), а також пунктах (a), (c) і (e) - (j) частини (3) цієї статті Регламенту
Ісландія	надсилати попередження контролерові або операторові про те, що призначені операції з опрацювання даних, імовірно, порушать положення ЗРЗД, робити догану контролерові або операторові, якщо операції опрацювання порушують положення ЗРЗД, видавати розпорядження контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до ЗРЗД, видавати розпорядження контролерові або операторові увідповіднити операції опрацювання положенням ЗРЗД, у разі необхідності, у встановленому порядку та протягом встановленого періоду, видавати розпорядження контролерові повідомити суб'єкта даних про порушення захисту персональних даних, накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання даних, видавати розпорядження виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17 та 18, а також повідомити про такі дії одержувачів, яким були розкриті

	персональні дані відповідно до статті 17 (2) і статті 19 ЗРЗД, відкликати сертифікацію або наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43 ЗРЗД, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються, накладати адміністративний штраф відповідно до статті 83 ЗРЗД як доповнення до, чи замість, заходів, вказаних у цьому параграфі, залежно від обставин кожної окремої справи, видавати розпорядження призупинити потоки даних до одержувача в третій країні чи до міжнародної організації
Греція	надсилати попередження контролерові або операторові про те, що призначені операції з опрацювання даних, імовірно, порушать положення ЗРЗД, робити догану контролерові або операторові, якщо операції опрацювання порушують положення ЗРЗД, видавати розпорядження контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до ЗРЗД, видавати розпорядження контролерові або операторові увідповіднити операції опрацювання положенням ЗРЗД, у разі необхідності, у встановленому порядку та протягом встановленого періоду, видавати розпорядження контролерові повідомити суб'єкта даних про порушення захисту персональних даних, накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання даних, видавати розпорядження виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17 та 18, а також повідомити про такі дії одержувачів, яким були розкриті персональні дані відповідно до статті 17 (2) і статті 19 ЗРЗД, накладати адміністративний штраф відповідно до статті 83 ЗРЗД як доповнення до, чи замість, заходів, вказаних у цьому параграфі, залежно від обставин кожної окремої справи, видавати розпорядження призупинити потоки даних до одержувача в третій країні чи до міжнародної організації; Орган має повноваження «наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43 ЗРЗД, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються». Ба більше, орган a) має коригувальне повноваження видавати розпорядження контролерові, операторові, одержувачеві або третій стороні припинити опрацювання персональних даних, повернути чи заблокувати відповідні дані або знищити систему реєстрації чи відповідні дані та накласти адміністративні стягнення, передбачені статтями 82.8 та 83 ЗРЗД, b) якщо захист особи від обробки персональних даних, що стосуються її, вимагає негайного ухвалення рішення, керівник органу може, на вимогу зацікавленої особи або за посадою, видати тимчасове розпорядження про негайне тимчасове обмеження, повністю або частково, опрацювання файлу чи роботи з ним. Розпорядження діє до ухвалення органом остаточного рішення, c) для забезпечення відповідності до положень ЗРЗД та інших положень, що стосуються захисту суб'єкта даних у питанні опрацювання персональних даних, орган має повноваження ухвалювати адміністративно-правові акти для регулювання конкретних, технічних і детальних питань, яких стосуються ці акти. Нормативні акти органу захисту даних, які не публікуються в Урядовому віснику, розміщуються на вебсайті цього органу
Князівство Ліхтенштейн	надсилати попередження контролерові або операторові про те, що призначені операції з опрацювання даних, імовірно, порушать положення ЗРЗД, робити догану контролерові або операторові, якщо операції опрацювання порушують положення ЗРЗД, видавати розпорядження контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до ЗРЗД, видавати розпорядження контролерові або операторові увідповіднити операції опрацювання положенням ЗРЗД, у разі необхідності, у встановленому порядку та протягом встановленого періоду, видавати розпорядження контролерові повідомити суб'єкта даних про порушення захисту персональних даних, накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання даних, видавати розпорядження виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17 та 18, а також повідомити про такі дії одержувачів, яким були розкриті персональні дані відповідно до статті 17 (2) і статті 19 ЗРЗД, відкликати сертифікацію або наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43 ЗРЗД, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються, накладати адміністративний штраф відповідно до статті 83 ЗРЗД як доповнення до, чи замість, заходів, вказаних у цьому параграфі, залежно від обставин кожної окремої справи, видавати розпорядження призупинити потоки даних до одержувача в третій країні чи до міжнародної організації
Португалія	надсилати попередження контролерові або операторові про те, що призначені операції з опрацювання даних, імовірно, порушать положення ЗРЗД, робити догану контролерові або операторові, якщо операції опрацювання порушують положення ЗРЗД, видавати розпорядження контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до ЗРЗД, видавати розпорядження контролерові або операторові увідповіднити операції опрацювання положенням ЗРЗД, у разі необхідності, у встановленому порядку та протягом встановленого періоду, видавати розпорядження контролерові повідомити суб'єкта даних про порушення захисту персональних даних, накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання даних, видавати розпорядження виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17 та 18, а також повідомити про такі дії одержувачів, яким були розкриті персональні дані відповідно до статті 17 (2) і статті 19 ЗРЗД, відкликати сертифікацію або наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43 ЗРЗД, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються, накладати адміністративний штраф відповідно до статті 83 ЗРЗД як доповнення до, чи замість, заходів, вказаних у цьому параграфі, залежно від обставин кожної окремої справи, видавати розпорядження призупинити потоки даних до одержувача в третій країні чи до міжнародної організації

Велике Герцогство Люксембург	надсилати попередження контролерові або операторові про те, що призначені операції з опрацювання даних, імовірно, порушать положення ЗРЗД, робити догану контролерові або операторові, якщо операції опрацювання порушують положення ЗРЗД, видавати розпорядження контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до ЗРЗД, видавати розпорядження контролерові або операторові увідповіднити операції опрацювання положенням ЗРЗД, у разі необхідності, у встановленому порядку та протягом встановленого періоду, видавати розпорядження контролерові повідомити суб'єкта даних про порушення захисту персональних даних, накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання даних, видавати розпорядження виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17 та 18, а також повідомити про такі дії одержувачів, яким були розкриті персональні дані відповідно до статті 17 (2) і статті 19 ЗРЗД, відкликати сертифікацію або наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43 ЗРЗД, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються, накладати адміністративний штраф відповідно до статті 83 ЗРЗД як доповнення до, чи замість, заходів, вказаних у цьому параграфі, залежно від обставин кожної окремої справи, видавати розпорядження призупинити потоки даних до одержувача в третій країні чи до міжнародної організації
Латвія	надсилати попередження контролерові або операторові про те, що призначені операції з опрацювання даних, імовірно, порушать положення ЗРЗД, робити догану контролерові або операторові, якщо операції опрацювання порушують положення ЗРЗД, видавати розпорядження контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до ЗРЗД, видавати розпорядження контролерові або операторові увідповіднити операції опрацювання положенням ЗРЗД, у разі необхідності, у встановленому порядку та протягом встановленого періоду, видавати розпорядження контролерові повідомити суб'єкта даних про порушення захисту персональних даних, накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання даних, видавати розпорядження виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17 та 18, а також повідомити про такі дії одержувачів, яким були розкриті персональні дані відповідно до статті 17 (2) і статті 19 ЗРЗД, відкликати сертифікацію або наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43 ЗРЗД, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються, накладати адміністративний штраф відповідно до статті 83 ЗРЗД як доповнення до, чи замість, заходів, вказаних у цьому параграфі, залежно від обставин кожної окремої справи, видавати розпорядження призупинити потоки даних до одержувача в третій країні чи до міжнародної організації
Чеська Республіка	надсилати попередження контролерові або операторові про те, що призначені операції з опрацювання даних, імовірно, порушать положення ЗРЗД, робити догану контролерові або операторові, якщо операції опрацювання порушують положення ЗРЗД, видавати розпорядження контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до ЗРЗД, видавати розпорядження контролерові або операторові увідповіднити операції опрацювання положенням ЗРЗД, у разі необхідності, у встановленому порядку та протягом встановленого періоду, видавати розпорядження контролерові повідомити суб'єкта даних про порушення захисту персональних даних, накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання даних, видавати розпорядження виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17 та 18, а також повідомити про такі дії одержувачів, яким були розкриті персональні дані відповідно до статті 17 (2) і статті 19 ЗРЗД, відкликати сертифікацію або наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43 ЗРЗД, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються, накладати адміністративний штраф відповідно до статті 83 ЗРЗД як доповнення до, чи замість, заходів, вказаних у цьому параграфі, залежно від обставин кожної окремої справи, видавати розпорядження призупинити потоки даних до одержувача в третій країні чи до міжнародної організації
Австрія	надсилати попередження контролерові або операторові про те, що призначені операції з опрацювання даних, імовірно, порушать положення ЗРЗД, робити догану контролерові або операторові, якщо операції опрацювання порушують положення ЗРЗД, видавати розпорядження контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до ЗРЗД, видавати розпорядження контролерові або операторові увідповіднити операції опрацювання положенням ЗРЗД, у разі необхідності, у встановленому порядку та протягом встановленого періоду, видавати розпорядження контролерові повідомити суб'єкта даних про порушення захисту персональних даних, накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання даних, видавати розпорядження виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17 та 18, а також повідомити про такі дії одержувачів, яким були розкриті персональні дані відповідно до статті 17 (2) і статті 19 ЗРЗД, відкликати сертифікацію або наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43 ЗРЗД, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються, накладати адміністративний штраф відповідно до статті 83 ЗРЗД як доповнення до, чи замість, заходів, вказаних у цьому параграфі, залежно від обставин кожної окремої справи, видавати розпорядження призупинити потоки даних до одержувача в третій країні чи до міжнародної організації

Республіка Словенія	надсилати попередження контролерові або операторові про те, що призначені операції з опрацювання даних, імовірно, порушать положення ЗРЗД, робити догану контролерові або операторові, якщо операції опрацювання порушують положення ЗРЗД, видавати розпорядження контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до ЗРЗД, видавати розпорядження контролерові або операторові увідповіднити операції опрацювання положенням ЗРЗД, у разі необхідності, у встановленому порядку та протягом встановленого періоду, видавати розпорядження контролерові повідомити суб'єкта даних про порушення захисту персональних даних, накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання даних, видавати розпорядження виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17 та 18, а також повідомити про такі дії одержувачів, яким були розкриті персональні дані відповідно до статті 17 (2) і статті 19 ЗРЗД, видавати розпорядження призупинити потоки даних до одержувача в третій країні чи до міжнародної організації
Болгарія	надсилати попередження контролерові або операторові про те, що призначені операції з опрацювання даних, імовірно, порушать положення ЗРЗД, робити догану контролерові або операторові, якщо операції опрацювання порушують положення ЗРЗД, видавати розпорядження контролерові або операторові дотримуватися запитів суб'єкта даних для реалізації його прав відповідно до ЗРЗД, видавати розпорядження контролерові або операторові увідповіднити операції опрацювання положенням ЗРЗД, у разі необхідності, у встановленому порядку та протягом встановленого періоду, видавати розпорядження контролерові повідомити суб'єкта даних про порушення захисту персональних даних, накладати тимчасове чи остаточне обмеження, зокрема заборону, на опрацювання даних, видавати розпорядження виправити чи стерти персональні дані або обмежити опрацювання згідно зі статтями 16, 17 та 18, а також повідомити про такі дії одержувачів, яким були розкриті персональні дані відповідно до статті 17 (2) і статті 19 ЗРЗД, відкликати сертифікацію або наказати органові сертифікації відкликати сертифікацію, видану відповідно до статей 42 і 43 ЗРЗД, або наказати органові сертифікації не видавати сертифікацію, якщо вимоги для сертифікації не виконано або більше не виконуються, накладати адміністративний штраф відповідно до статті 83 ЗРЗД як доповнення до, чи замість, заходів, вказаних у цьому параграфі, залежно від обставин кожної окремої справи, видавати розпорядження призупинити потоки даних до одержувача в третій країні чи до міжнародної організації

20. Будь ласка, зазначте які дозвільні та консультативні повноваження здійснює ваш наглядовий орган у сфері захисту персональних даних:

Норвегія	Дає поради контролерові відповідно до процедури попередньої консультації, визначеної у статті 36 Регламенту, надає, з власної ініціативи або на підставі запиту, висновки національному парламентові, урядові держави-члена або, відповідно до законодавства держави-члена, іншим установам та органам, а також громадськості з будь-якого питання, пов'язаного із захистом персональних даних; дозволяє обробку даних, зазначену у статті 36 (5) Регламенту, якщо законодавство держави-члена вимагає, щоб такий дозвіл був попередньо отриманий; надає висновок і затверджує проєкти кодексів поведінки відповідно до статті 40 (5) Регламенту; акредитує органи сертифікації відповідно до статті 43 Регламенту, видає сертифікацію та затверджує критерії сертифікації відповідно до статті 42 (5) Регламенту; ухвалює стандартні положення щодо захисту даних відповідно до статті 28 (8) та пункту (d) частини другої статті 46 Регламенту; погоджує положення договорів, зазначених у пункті (a) частини третьої статті 46 Регламенту; погоджує адміністративні домовленості, зазначені в пункті (b) частині третьої статті 46 Регламенту; затверджує зобов'язальні корпоративні правила відповідно до статті 47 Регламенту
Словацька Республіка	дає поради контролерові відповідно до процедури попередньої консультації, визначеної у статті 36 Регламенту; надає, з власної ініціативи або на підставі запиту, висновки національному парламентові, урядові держави-члена або, відповідно до законодавства держави-члена, іншим установам та органам, а також громадськості з будь-якого питання, пов'язаного із захистом персональних даних; надає дозвіл на обробку даних, зазначену у статті 36 (5) Регламенту, якщо законодавство держави-члена вимагає попереднього отримання такого дозволу; надає висновок і затверджує проєкти кодексів поведінки відповідно до статті 40 (5) Регламенту; акредитує органи сертифікації відповідно до статті 43 Регламенту; видає сертифікацію та затверджує критерії сертифікації відповідно до статті 42 (5) Регламенту; ухвалює стандартні положення щодо захисту даних відповідно до статті 28 (8) та пункту (d) частини другої статті 46 Регламенту; погоджує положення договорів, зазначених у пункті (a) частини третьої статті 46 Регламенту; погоджує адміністративні домовленості, зазначені в пункті (b) частині третьої статті 46 Регламенту; затверджує зобов'язальні корпоративні правила відповідно до статті 47 Регламенту
Румунія	дає поради контролерові відповідно до процедури попередньої консультації, передбаченої статтею 36 Регламенту; надає, з власної ініціативи або за запитом, висновки національному парламентові, урядові держави-члена або, відповідно до законодавства держави-члена, іншим установам та органам, а також громадськості з будь-якого питання, пов'язаного із захистом персональних даних; надає дозвіл на обробку даних, згадану у статті 36 (5) Регламенту, якщо законодавство держави-члена вимагає попереднього отримання такого дозволу; надає висновок та затверджує проєкти кодексів поведінки відповідно до статті 40 (5) Регламенту; акредитує органи сертифікації відповідно до статті 43 Регламенту; видає сертифікацію та затверджує критерії сертифікації відповідно до статті 42 (5) Регламенту; ухвалює стандартні положення щодо захисту даних відповідно до статті

	28 (8) та пункту (d) частини другої статті 46 Регламенту; погоджує положення договорів, зазначених у пункті (a) частини третьої статті 46 Регламенту; погоджує адміністративні домовленості, зазначені в пункті (b) частині третьої статті 46 Регламенту; затверджує зобов'язальні корпоративні правила відповідно до статті 47 Регламенту
Італія	дає поради контролерові відповідно до процедури попередньої консультації, передбаченої статтею 36 Регламенту; надає, з власної ініціативи або за запитом, висновки національному парламентові, урядові держави-члена або, відповідно до законодавства держави-члена, іншим установам та органам, а також громадськості з будь-якого питання, пов'язаного із захистом персональних даних; надає дозвіл на обробку даних, згадану у статті 36 (5) Регламенту, якщо законодавство держави-члена вимагає попереднього отримання такого дозволу; надає висновок і затверджує проєкти кодексів поведінки відповідно до статті 40 (5) Регламенту; акредитує органи сертифікації відповідно до статті 43 Регламенту; видає сертифікації та затверджує критерії сертифікації відповідно до статті 42 (5) Регламенту; ухвалює стандартні положення щодо захисту даних, передбачені у статті 28 (8) та пункті (d) частини другої статті 46 Регламенту; погоджує положення договорів, зазначених у пункті (a) частини третьої статті 46 Регламенту; погоджує адміністративні домовленості, згадані в пункті (b) частині третьої статті 46 Регламенту; затверджує зобов'язальні корпоративні правила відповідно до статті 47 Регламенту
Естонія	дає поради контролерові даних відповідно до процедури попередньої консультації, передбаченої статтею 36 Регламенту; з власної ініціативи або за запитом надає висновки національному парламентові, урядові держави-члена або, відповідно до законодавства держави-члена, іншим установам та органам, а також громадськості з будь-якого питання, пов'язаного із захистом персональних даних; надає висновок та затверджує проєкти кодексів поведінки відповідно до статті 40 (5) Регламенту; акредитує органи сертифікації відповідно до статті 43 Регламенту; ухвалює стандартні положення щодо захисту даних, передбачені у статті 28 (8) та пункті (d) частини другої статті 46 Регламенту; погоджує положення договорів, зазначених у пункті (a) частини третьої статті 46 Регламенту; погоджує адміністративні домовленості, згадані в пункті (b) частині третьої статті 46 Регламенту; затверджує зобов'язальні корпоративні правила відповідно до статті 47 Регламенту
Хорватія	дає поради контролерові даних відповідно до процедури попередньої консультації, передбаченої статтею 36 Регламенту; з власної ініціативи або за запитом надає висновки національному парламентові, урядові держави-члена або, відповідно до законодавства держави-члена іншим установам та органам, а також громадськості з будь-якого питання, пов'язаного із захистом персональних даних; надає дозвіл на обробку даних, передбачену статтею 36(5) Регламенту, якщо законодавство держави-члена вимагає попереднього отримання такого дозволу; надає висновок і затверджує проєкти кодексів поведінки відповідно до статті 40 (5) Регламенту; акредитує органи сертифікації відповідно до статті 43 Регламенту; видає сертифікації та затверджує критерії сертифікації відповідно до статті 42 (5) Регламенту; ухвалює стандартні положення щодо захисту даних, передбачені у статті 28 (8) та пункті (d) частини другої статті 46 Регламенту; погоджує положення договорів, зазначених у пункті (a) частини третьої статті 46 Регламенту; погоджує адміністративні домовленості, згадані в пункті (b) частині третьої статті 46 Регламенту; затверджує зобов'язальні корпоративні правила відповідно до статті 47 Регламенту
Республіка Кіпр	дає поради контролерові даних відповідно до процедури попередньої консультації, передбаченої статтею 36 Регламенту; з власної ініціативи або за запитом надає висновки національному парламентові, урядові держави-члена або, відповідно до законодавства держави-члена, іншим установам та органам, а також громадськості з будь-якого питання, пов'язаного із захистом персональних даних; надає дозвіл на обробку даних, передбачену статтею 36(5) Регламенту, якщо законодавство держави-члена вимагає попереднього отримання такого дозволу; надає висновок і затверджує проєкти кодексів поведінки відповідно до статті 40 (5) Регламенту; акредитує органи сертифікації відповідно до статті 43 Регламенту; видає сертифікації та затверджує критерії сертифікації відповідно до статті 42 (5) Регламенту; ухвалює стандартні положення щодо захисту даних, передбачені у статті 28 (8) та пункті (d) частини другої статті 46 Регламенту; погоджує положення договорів, зазначених у пункті (a) частини третьої статті 46 Регламенту; погоджує адміністративні домовленості, згадані в пункті (b) частині третьої статті 46 Регламенту; затверджує зобов'язальні корпоративні правила відповідно до статті 47 Регламенту. Згідно зі статтею 25(g) Закону 125(I)/2018 «На додаток до дозвільних і консультативних повноважень, передбачених у частині третій статті 58 Регламенту, Уповноважений з питань захисту персональних даних має такі повноваження: i) надавати дозвіл на об'єднання систем обліку даних, передбачене розділом 10 цього закону, та визначати умови і порядок реалізації такого об'єднання, ii) визначати умови і порядок застосування заходів, спрямованих на обмеження прав, передбачених у розділі 11 цього Закону, iii) визначати умови і порядок звільнення від виконання обов'язку щодо повідомлення даних про порушення, згадане в розділі 12 цього закону, iv) запроваджувати чітко визначені обмеження щодо передання спеціальних категорій персональних даних, передбачених розділами 17 і 18 цього закону, v) рекомендувати міністрові укласти угоди з іншими країнами, а також укласти і підписати Меморандуми про взаєморозуміння, передбачені в розділі 35 цього закону»

Литва	дає поради контролерові даних відповідно до процедури попередньої консультації, передбаченої статтею 36 Регламенту; з власної ініціативи або за запитом надає висновки національному парламентові, урядові держави-члена або, відповідно до законодавства держави-члена, іншим установам та органам, а також громадськості з будь-якого питання, пов'язаного із захистом персональних даних; надає дозвіл на обробку даних, передбачену статтею 36(5) Регламенту, якщо законодавство держави-члена вимагає попереднього отримання такого дозволу; надає висновок та затверджує проєкти кодексів поведінки відповідно до статті 40 (5) Регламенту; акредитує органи сертифікації відповідно до статті 43 Регламенту; видає сертифікації та затверджує критерії сертифікації відповідно до статті 42 (5) Регламенту; ухвалює стандартні положення щодо захисту даних, передбачені у статті 28 (8) та пункті (d) частини другої статті 46 Регламенту; погоджує положення договорів, зазначених у пункті (a) частини третьої статті 46 Регламенту; погоджує адміністративні домовленості, згадані в пункті (b) частині третьої статті 46 Регламенту; затверджує зобов'язальні корпоративні правила відповідно до статті 47 Регламенту
Ісландія	консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36 ЗРЗД, видавати з власної ініціативи чи на запит висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних, надавати дозвіл на опрацювання, вказане в статті 36(5) ЗРЗД, якщо законодавство держави-члена вимагає надання такого попереднього дозволу, надавати висновок і затверджувати проєкти кодексів поведінки відповідно до статті 40(5) ЗРЗД, видавати сертифікації та затверджувати критерії сертифікації відповідно до статті 42(5) ЗРЗД, ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2) ЗРЗД, надавати дозвіл на договірні положення, вказані в пункті (a) статті 46(3) ЗРЗД, надавати дозвіл на адміністративні домовленості, вказані в пункті (b) статті 46(3) ЗРЗД, затверджувати зобов'язальні корпоративні правила відповідно до статті 47 ЗРЗД
Греція	консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36 ЗРЗД, видавати, з власної ініціативи чи на запит, висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних, надавати висновок і затверджувати проєкти кодексів поведінки відповідно до статті 40(5) ЗРЗД, ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2) ЗРЗД, надавати дозвіл на договірні положення, вказані в пункті (a) статті 46(3) ЗРЗД, надавати дозвіл на адміністративні домовленості, вказані в пункті (b) статті 46(3) ЗРЗД, «затверджувати критерії сертифікації відповідно до статті 42(5) ЗРЗД»
Князівство Ліхтенштейн	консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36 ЗРЗД, видавати, з власної ініціативи чи на запит, висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних, надавати дозвіл на опрацювання, вказане в статті 36(5) ЗРЗД, якщо законодавство держави-члена вимагає надання такого попереднього дозволу, надавати висновок і затверджувати проєкти кодексів поведінки відповідно до статті 40(5) ЗРЗД, видавати сертифікації та затверджувати критерії сертифікації відповідно до статті 42(5) ЗРЗД, ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2) ЗРЗД, надавати дозвіл на договірні положення, вказані в пункті (a) статті 46(3) ЗРЗД, надавати дозвіл на адміністративні домовленості, вказані в пункті (b) статті 46(3) ЗРЗД, затверджувати зобов'язальні корпоративні правила відповідно до статті 47 ЗРЗД
Португалія	консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36 ЗРЗД, видавати, з власної ініціативи чи на запит, висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних, надавати дозвіл на опрацювання, вказане в статті 36(5) ЗРЗД, якщо законодавство держави-члена вимагає надання такого попереднього дозволу, надавати висновок і затверджувати проєкти кодексів поведінки відповідно до статті 40(5) ЗРЗД, надавати акредитацію органам сертифікації відповідно до статті 43, ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2) ЗРЗД, надавати дозвіл на договірні положення, вказані в пункті (a) статті 46(3) ЗРЗД, надавати дозвіл на адміністративні домовленості, вказані в пункті (b) статті 46(3) ЗРЗД, затверджувати зобов'язальні корпоративні правила відповідно до статті 47 ЗРЗД
Велике Герцогство Люксембург	консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36 ЗРЗД, видавати, з власної ініціативи чи на запит, висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних, надавати дозвіл на опрацювання, вказане в статті 36(5) ЗРЗД, якщо законодавство держави-члена вимагає надання такого попереднього дозволу, надавати висновок і затверджувати проєкти кодексів поведінки відповідно до статті 40(5) ЗРЗД, надавати акредитацію органам сертифікації відповідно до статті 43, видавати сертифікації та затверджувати критерії сертифікації відповідно до статті 42(5) ЗРЗД, ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2) ЗРЗД, надавати дозвіл на договірні положення, вказані в пункті (a) статті 46(3) ЗРЗД, надавати дозвіл на адміністративні домовленості, вказані в пункті (b) статті 46(3) ЗРЗД, затверджувати зобов'язальні корпоративні правила відповідно до статті 47 ЗРЗД

Латвія	консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36 ЗРЗД, видавати, з власної ініціативи чи на запит, висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних, надавати дозвіл на опрацювання, вказане в статті 36(5) ЗРЗД, якщо законодавство держави-члена вимагає надання такого попереднього дозволу, надавати висновок і затверджувати проєкти кодексів поведінки відповідно до статті 40(5) ЗРЗД, видавати сертифікації та затверджувати критерії сертифікації відповідно до статті 42(5) ЗРЗД, ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2) ЗРЗД, надавати дозвіл на договірні положення, вказані в пункті (a) статті 46(3) ЗРЗД, надавати дозвіл на адміністративні домовленості, вказані в пункті (b) статті 46(3) ЗРЗД, затверджувати зобов'язальні корпоративні правила відповідно до статті 47 ЗРЗД; акредитація органів сертифікації проводиться спільно з Латвійським національним бюро акредитації (https://www.latak.gov.lv/index.php?lang=en)
Чеська Республіка	видавати, з власної ініціативи чи на запит, висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних, ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2) ЗРЗД, затверджувати зобов'язальні корпоративні правила відповідно до статті 47 ЗРЗД
Австрія	консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36 ЗРЗД, видавати, з власної ініціативи чи на запит, висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних, надавати дозвіл на опрацювання, вказане в статті 36(5) ЗРЗД, якщо законодавство держави-члена вимагає надання такого попереднього дозволу, надавати висновок і затверджувати проєкти кодексів поведінки відповідно до статті 40(5) ЗРЗД, надавати акредитацію органам сертифікації відповідно до статті 43, ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2) ЗРЗД, затверджувати зобов'язальні корпоративні правила відповідно до статті 47 ЗРЗД
Республіка Словенія	консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36 ЗРЗД, видавати, з власної ініціативи чи на запит, висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних, надавати висновок і затверджувати проєкти кодексів поведінки відповідно до статті 40(5) ЗРЗД, ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2) ЗРЗД, надавати дозвіл на договірні положення, вказані в пункті (a) статті 46(3) ЗРЗД, надавати дозвіл на адміністративні домовленості, вказані в пункті (b) статті 46(3) ЗРЗД, затверджувати зобов'язальні корпоративні правила відповідно до статті 47 ЗРЗД
Болгарія	консультувати контролера відповідно до процедури попередніх консультацій, вказаної в статті 36 ЗРЗД, видавати, з власної ініціативи чи на запит, висновки для національного парламенту, уряду держави-члена чи, відповідно до законодавства держави-члена, інших установ і органів, а також громадськості щодо будь-якого питання, пов'язаного з захистом персональних даних, надавати дозвіл на опрацювання, вказане в статті 36(5) ЗРЗД, якщо законодавство держави-члена вимагає надання такого попереднього дозволу, надавати висновок і затверджувати проєкти кодексів поведінки відповідно до статті 40(5) ЗРЗД, надавати акредитацію органам сертифікації відповідно до статті 43, видавати сертифікації та затверджувати критерії сертифікації відповідно до статті 42(5) ЗРЗД, ухвалювати стандартні положення щодо захисту даних, вказані в статті 28(8) та пункті (d) статті 46(2) ЗРЗД, надавати дозвіл на договірні положення, вказані в пункті (a) статті 46(3) ЗРЗД, надавати дозвіл на адміністративні домовленості, вказані в пункті (b) статті 46(3) ЗРЗД, затверджувати зобов'язальні корпоративні правила відповідно до статті 47 ЗРЗД

21. Чи наділений ваш наглядовий орган у сфері захисту персональних даних іншими розпорядчими повноваження, ніж ті, що вказані в Загальному регламенті про захист даних Європейського парламенту і Ради ЄС (далі - Регламент), наприклад у статті 35 (4) та ін.:

Норвегія	так
Словацька Республіка	ні
Румунія	ні
Італія	так
Естонія	так
Хорватія	Згідно зі статтею 6 Закону про виконання Загального регламенту про захист даних, на додаток до повноважень, визначених Загальним регламентом про захист даних, Агентство виконує такі обов'язки: – за умови наявності відповідних положень у спеціальному законі, Агентство може ініціювати та має право брати участь у кримінальних, пов'язаних з незначними правопорушеннями, адміністративних судових і позасудових провадженнях, у разі порушення положень Загального
	регламенту захисту даних та цього закону; – затверджує критерії для визначення розміру компенсації адміністративних витрат, передбачених у частині 2 статті 43 цього закону, а також критерії визначення розміру компенсації, зазначеної в частині 3 статті 43 цього закону; – публікує власні рішення на вебсайті Агентства відповідно до вимог статей 18 та 48 цього закону – ініціює та виконує відповідні процедури стосовно відповідальних осіб у зв'язку з порушеннями положень Загального регламенту захисту даних та цього закону; – здійснює свої обов'язки незалежного наглядового органу з моніторингу виконання Директиви (ЄС) 2016/680 Європейського парламенту та Ради (ЄС) від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних уповноваженими органами для цілей запобігання, розслідування, виявлення чи переслідування за скоєння кримінальних правопорушень або виконання кримінальних покарань, і про вільний рух таких даних, а також про визнання таким, що втратив чинність, Рамкового рішення Ради 2008/977/ ЈНА, якщо інше не встановлено спеціальними нормативними актами; та – виконує інші обов'язки, передбачені законодавством
Республіка Кіпр	Завдання, покладені на інформаційного комісара, виконує відповідний уповноважений з питань захисту персональних даних. Уповноважений – компетентний наглядовий орган для інших європейських органів
Литва	так
Ісландія	так
Греція	ні
Князівство Ліхтенштейн	ні
Португалія	ні
Велике Герцогство Люксембург	так
Латвія	так
Чеська Республіка	ні
Австрія	ні
Республіка Словенія	так
Болгарія	так

22. Вкажіть, будь ласка, повноваження вашого наглядового органу у сфері захисту персональних даних стосовно надання рекомендацій парламентові, урядові, іншим державним установам та органам з приводу вжиття законодавчих та адміністративних заходів

Норвегія	орган у сфері захисту персональних даних надає в межах своєї компетенції висновок після ухвалення нормативно-правового акта; орган у сфері захисту персональних даних у межах своєї компетенції надає висновок щодо проєктів нормативно-правових актів, коли їх текст уже підготовлений; орган у сфері захисту персональних даних у межах своєї компетенції надає висновок щодо проєктів нормативно-правових актів під час розроблення їх тексту
Словацька Республіка	орган у сфері захисту персональних даних надає в межах своєї компетенції висновок після ухвалення нормативно-правового акту; орган у сфері захисту персональних даних у межах своєї компетенції надає висновок щодо проєктів нормативно-правових актів, коли їх текст уже підготовлений; орган у сфері захисту персональних даних у межах своєї компетенції надає висновок щодо проєктів нормативно-правових актів під час розроблення їх тексту
Румунія	орган у сфері захисту персональних даних у межах своєї компетенції надає висновок щодо проєктів нормативно-правових актів, коли їх текст уже підготовлений; орган у сфері захисту персональних даних надає в межах своєї компетенції висновок щодо проєктів нормативно-правових актів під час розроблення їх тексту
Італія	орган у сфері захисту персональних даних у межах своєї компетенції надає висновок щодо проєктів нормативно-правових актів, коли їх текст уже підготовлений; орган у сфері захисту персональних даних надає в межах своєї компетенції висновок щодо проєктів нормативно-правових актів під час розроблення їх тексту
Естонія	орган у сфері захисту персональних даних у межах своєї компетенції надає висновок щодо проєктів нормативно-правових актів після завершення підготування їх текстів
Хорватія	Відповідно до статті 14 Закону про виконання Загального регламенту про захист даних центральні органи державного управління та інші державні органи подають Агентству проєкти законів і проєкти інших нормативно-правових актів, які врегульовують питання, пов'язані з обробкою персональних даних, з метою забезпечення надання експертних висновків у сфері захисту персональних даних
Республіка Кіпр	орган у сфері захисту персональних даних у межах своєї компетенції надає висновок щодо проєктів нормативно-правових актів, коли їх текст уже підготовлений; орган у сфері захисту персональних даних надає в межах своєї компетенції висновок щодо проєктів нормативно-правових актів під час розроблення їх тексту
Литва	орган у сфері захисту персональних даних у межах своєї компетенції надає висновок щодо проєктів нормативно-правових актів, коли їх текст уже підготовлений; орган у сфері захисту персональних даних надає в межах своєї компетенції висновок щодо проєктів нормативно-правових актів під час розроблення їх тексту
Ісландія	орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після того як складено текст цих проєктів, орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, у процесі розроблення тексту цих нормативно-правових актів
Греція	орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після того як складено текст цих проєктів
Князівство Ліхтенштейн	орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після того як складено текст цих проєктів, орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, у процесі розроблення тексту цих нормативно-правових актів
Португалія	орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після того як складено текст цих проєктів, орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, у процесі розроблення тексту цих нормативно-правових актів
Велике Герцогство Люксембург	орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після того як складено текст цих проєктів, орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, у процесі розробки тексту цих нормативно-правових актів
Латвія	орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після того як складено текст цих проєктів, орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, у процесі розроблення тексту цих нормативно-правових актів
Чеська Республіка	орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після ухвалення цих нормативно-правових актів

Австрія	орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після того як складено текст цих проєктів
Республіка Словенія	орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після ухвалення цих нормативно-правових актів, орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після того як складено текст цих проєктів, орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, у процесі розроблення тексту цих нормативно-правових актів
Болгарія	орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після ухвалення цих нормативно-правових актів, орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, після того як складено текст цих проєктів, орган з питань захисту даних надає висновки щодо проєктів нормативно-правових актів, що входять до його компетенції, у процесі розроблення тексту цих нормативно-правових актів

23. Чи виконує ваш наглядовий орган у сфері захисту персональних даних свої завдання на безплатній основі:

Норвегія	Так, це стосується всіх зазначених вище суб'єктів відносин, пов'язаних із персональними даними
Словацька Республіка	для суб'єкта персональних даних
Румунія	Так, це стосується всіх зазначених вище суб'єктів відносин, пов'язаних із персональними даними
Італія	ОЗПД Італії виконує свої завдання на безплатній основі
Естонія	застосовуються всі відповіді
Хорватія	Відповідно до статті 43 Закону про виконання Загального регламенту про захист даних Агентство виконує свої завдання, не вимагаючи відшкодування, щодо суб'єктів даних, посадових осіб у сфері захисту персональних даних, журналістів і державних органів. Агентство отримує розумне відшкодування розміром адміністративних витрат або відмовляє в задоволенні запиту, якщо такі запити суб'єктів даних явно необґрунтовані або надмірні та особливо через їх повторюваність. Агентство вимагає відшкодування за надання висновків підприємницьким структурам (юридичним фірмам, консультантам тощо), якщо запити цих підприємницьких структур пов'язані з виконанням ними своєї звичайної діяльності або наданням послуг
Республіка Кіпр	Так, це стосується всіх зазначених вище суб'єктів відносин, пов'язаних із персональними даними
Литва	безплатно
Ісландія	Загалом виконання завдань ОЗД безплатне для всіх, але за певних обставин орган може стягувати з контролера/оператора плату за проведення перевірок за тарифами цього ОЗД
Греція	безплатно для всіх зазначених сторін
Князівство Ліхтенштейн	безплатно для суб'єктів даних, співробітників з питань захисту даних, а також контролерів та операторів
Португалія	для суб'єкта даних
Велике Герцогство Люксембург	може стягуватися плата у сфері акредитації органів сертифікації
Латвія	встановлюється плата за проведення іспитів співробітників з питань захисту даних, семінарів, організованих інспекцією, акредитацію кодексів поведінки, акредитацію кредитних бюро, а виконання інших завдань безплатне
Чеська Республіка	для контролерів та операторів
Австрія	для суб'єкта даних
Республіка Словенія	для всіх зазначених варіантів
Болгарія	для всіх зазначених варіантів

24. Рішення вашого наглядового органу у сфері захисту персональних даних:

Норвегія	можуть бути оскаржені в суді відповідно до законодавства держави-члена, можуть бути оскаржені до іншої установи / органу
Словацька Республіка	можуть бути оскаржені до вищої управлінської структури / органу, можуть бути оскаржені в суді відповідно до законодавства держави-члена
Румунія	можуть бути оскаржені в суді відповідно до законодавства держави-члена
Італія	можуть бути оскаржені в суді відповідно до законодавства держави-члена, можуть бути оскаржені до іншої установи / органу
Естонія	можуть бути оскаржені в суді відповідно до законодавства держави-члена
Хорватія	Відповідно до статті 34 Закону про виконання Загального регламенту про захист даних будь-яка особа, яка вважає, що будь-яке з його або її прав, гарантованих цим законом або Загальним регламентом про захист даних, було порушене, має право звернутися до Агентства із запитом про встановлення факту порушення цього права. Агентство ухвалює постанову про те, чи сталося порушення права. Постанова Агентства вважається адміністративним (управлінським) актом. Постанова Агентства не підлягає оскарженню, але можливе відкриття адміністративного провадження шляхом подання скарги до уповноваженого адміністративного суду
Республіка Кіпр	можуть бути оскаржені в суді відповідно до законодавства держави-члена
Литва	можуть бути оскаржені в суді відповідно до законодавства держави-члена
Ісландія	можуть бути оскаржені до суду відповідно до законодавства держави-члена
Греція	можуть бути оскаржені до Державної ради
Князівство Ліхтенштейн	можуть бути оскаржені до вищої адміністративної установи / органу
Португалія	можуть бути оскаржені до суду відповідно до законодавства держави-члена
Велике Герцогство Люксембург	можуть бути оскаржені до суду відповідно до законодавства держави-члена, до адміністративного суду
Латвія	можуть бути оскаржені до суду відповідно до законодавства держави-члена
Чеська Республіка	можуть бути оскаржені до вищої адміністративної установи / органу
Австрія	можуть бути оскаржені до суду відповідно до законодавства держави-члена
Республіка Словенія	можуть бути оскаржені до суду відповідно до законодавства держави-члена
Болгарія	можуть бути оскаржені до суду відповідно до законодавства держави-члена

25. Якщо йдеться про участь у судочинстві, ваш наглядовий орган у сфері захисту персональних даних відповідно до закону має право (можливі кілька відповідей):

Норвегія	брати участь у судових провадженнях стосовно рішень, ухвалених цим органом
Словацька Республіка	брати участь у судових провадженнях стосовно рішень, ухвалених цим органом
Румунія	брати участь у судових провадженнях стосовно рішень, ухвалених цим органом
Італія	брати участь у судових провадженнях стосовно рішень, ухвалених цим органом
Естонія	не розуміємо запитання та можливі відповіді на нього
Хорватія	Згідно зі статтею 6 Закону про виконання Загального регламенту про захист даних Агентство, якщо це передбачено спеціальним законом, може ініціювати та має право брати участь у кримінальних, пов'язаних з незначними правопорушеннями, адміністративних судових і позасудових провадженнях у разі порушення положень Загального регламенту захисту даних та цього закону, а також ініціює та проводить відповідні процедури стосовно відповідальних осіб у разі порушення ними вимог Загального регламенту про захист даних
Республіка Кіпр	оскаржувати нормативно-правові акти, ухвалені органами державного управління, брати участь у судових провадженнях стосовно рішень, ухвалених вашим органом. Стаття 25(h) Закону 125(I)/2018: «З урахуванням положень частини 5 статті 58 Регламенту уповноважений зобов'язаний повідомляти генерального прокурора Республіки і / або поліцію про будь-яке порушення положень Регламенту або цього закону, яке може становити злочин відповідно до положень глави 33 цього закону»
Литва	брати участь у судових провадженнях стосовно рішень, ухвалених цим органом
Ісландія	брати участь у судовому провадженні щодо рішень, ухвалених вашим органом
Греція	брати участь у судовому провадженні щодо рішень, ухвалених вашим органом
Князівство Ліхтенштейн	брати участь у судовому провадженні щодо рішень, ухвалених вашим органом

Португалія	оскаржувати нормативно-правові акти, ухвалені установами державного управління, направляти питання до Конституційного суду, брати участь у судовому провадженні щодо рішень, ухвалених вашим органом
Велике Герцогство Люксембург	брати участь у судовому провадженні щодо рішень, ухвалених вашим органом
Латвія	брати участь у судовому провадженні щодо рішень, ухвалених вашим органом
Чеська Республіка	оскаржувати нормативно-правові акти, ухвалені установами державного управління, брати участь у судовому провадженні щодо рішень, ухвалених вашим органом
Австрія	брати участь у судовому провадженні щодо рішень, ухвалених вашим органом
Республіка Словенія	направляти питання до Конституційного суду, брати участь у судовому провадженні щодо рішень, ухвалених вашим органом
Болгарія	оскаржувати нормативно-правові акти, ухвалені установами державного управління, брати участь у судовому провадженні щодо рішень, ухвалених вашим органом

26. Чи взаємодіє ваш наглядовий орган у сфері захисту персональних даних з іншими регуляторними органами та державними органами у разі інцидентів, пов'язаних з витоком персональних даних?

		Якщо ваша відповідь «так», якою мірою визначені механізми такої взаємодії:
Норвегія	Так	співпраця на добровільних засадах
Словацька Республіка	Ні	
Румунія	Так	на підставі визначених законом повноважень
Італія	Ні	
Естонія	Так	співпраця між європейськими органами у сфері захисту даних передбачена в Регламенті, співпраця з іншими органами на національному рівні врегульовується на підставі угод
Хорватія	Так	коли необхідно, ми взаємодіємо з іншими наглядовими органами шляхом надання взаємної допомоги на добровільних засадах
Республіка Кіпр	Так	усе, наведене вище
Литва	Так	законодавство про повноваження органу; нормативно-правові акти, що врегульовують діяльність органу; законодавство про кібербезпеку; законодавство щодо електронних засобів зв'язку
Ісландія	Так	закон про кібербезпеку
Греція	Так	закон про електронні комунікації
Князівство Ліхтенштейн	Ні	
Португалія	Так	регламент органу
Велике Герцогство Люксембург	Так	закон про електронні комунікації
Латвія	Так	закон про орган
Чеська Республіка	Ні	
Австрія	Ні	
Республіка Словенія	Так	незалежне рішення наглядового органу, залежно від кожного окремого випадку
Болгарія	Так	усі зазначені варіанти

27. Щодо адміністративних штрафів, які накладаються у вашій країні на державні органи:

Норвегія	Адміністративні штрафи, як зазначено у статті 83 Регламенту
Словацька Республіка	Адміністративні штрафи, як зазначено у статті 83 Регламенту
Румунія	Мінімум - 10,000 леїв і максимум 200,000 леїв
Італія	Адміністративні штрафи передбачені національним законодавством
Естонія	В Естонії існують штрафи за скоєння незначних правопорушень (пункт 151 у Регламенті), ці штрафи не можуть бути накладені на державні органи, розмір цих штрафів передбачений Законом про захист персональних даних, Розділ 6: https://www.riigiteataja.ee/en/eli/523012019001/consolide
Хорватія	Адміністративні штрафи не можуть накладатися на державні органи
Республіка Кіпр	Відповідно до статті 32(3) Закону 125(I)/2018 «Розмір адміністративного штрафу, що накладається на державну установу або орган, пов'язаного з діяльністю, яка не має за мету отримання прибутку, не повинен перевищувати двісті тисяч (200,000) євро"
Литва	Адміністративні штрафи передбачені національним законодавством
Ісландія	Адміністративні штрафи, передбачені статтею 83 ЗРЗД
Греція	Відповідно до параграфа 1 статті 39 Закону 4624/2019, у конкретному вмотивованому рішенні та після попереднього повідомлення зацікавлених сторін із закликом надати пояснення орган може накласти на органи державного сектору адміністративний штраф розміром до десяти мільйонів євро (10000000 євро)
Князівство Ліхтенштейн	Адміністративні штрафи не можуть накладатися на органи державної влади
Португалія	Адміністративні штрафи встановлені законом. Проте органи державної влади можуть направляти запит щодо звільнення від їх накладення
Велике Герцогство Люксембург	Адміністративні штрафи не можуть накладатися на органи державної влади
Латвія	до 1000 євро для фізичної особи (державного службовця)
Чеська Республіка	Адміністративні штрафи, передбачені статтею 83 ЗРЗД
Австрія	Адміністративні штрафи не можуть накладатися на органи державної влади
Республіка Словенія	Адміністративні штрафи встановлені національним законодавством
Болгарія	Адміністративні штрафи, передбачені статтею 83 ЗРЗД

28. Щодо процедури попередніх консультацій, яка визначена статтею 36 Регламенту:

Норвегія	консультації з наглядовим органом у сфері захисту персональних даних обов'язкові під час підготування пропозиції щодо законодавчого заходу, який має ухвалити національний парламент
Словацька Республіка	процедура проведення оператором даних попередніх консультацій, визначених статтею 36 Регламенту, врегульована національним законодавством
Румунія	консультація з наглядовим органом у сфері захисту персональних даних обов'язкова під час підготування пропозиції щодо законодавчого заходу, який затверджує національний парламент
Італія	Процедура проведення попередніх консультацій визначена статтею 36 Регламенту, на яку ми посилаємося: отже, консультації з нашим наглядовим органом обов'язкові під час підготування пропозиції щодо законодавчого заходу або підготування управлінського заходу, що виконуватиметься на підставі цього законодавчого заходу, якщо вони мають стосунок до обробки персональних даних. Будь ласка, візьміть до уваги, що розділ 110 Кодексу захисту даних (медичне, біомедичне та епідеміологічне дослідження) також містить положення щодо необхідності попередньої консультації відповідно до статті 36 Регламенту. Стосовно статті 36.5 Регламенту ми відсилаємо до розділу 2-р (Обробка, що створює високий ризик для виконання завдання, яке виконується в публічних інтересах) Кодексу захисту даних (дивись вище посилання)
Естонія	
Хорватія	Відповідно до статті 36 Регламенту контролер консультується з наглядовим органом перед обробкою даних, коли оцінення впливу на захист даних згідно зі статтею 35 вказує на те, що така обробка може бути дуже ризикованою, якщо не буде заходів з боку контролера даних для зменшення такого ризику
Республіка Кіпр	консультації з наглядовим органом з питань захисту даних обов'язкові під час підготування пропозиції щодо законодавчого заходу, який затверджує національний парламент, консультації з наглядовим органом з питань захисту даних обов'язкові під час підготування управлінського заходу, що виконується на підставі законодавчого заходу, затвердженого національним парламентом, статті 10(2), 11(2), 12(2) і 18(1) Закону 125(I)/2018

Литва	процедура попередніх консультацій відповідно до частини (1) статті 36 Регламенту врегульована в національному законодавстві. Погодження (з наглядовим органом з питань захисту даних) проєктів законодавчих актів відбувається відповідно до Закону Литовської Республіки про законодавчий процес та Регламенту уряду Литовської Республіки від 11 серпня 1994 року
Ісландія	консультації з наглядовим органом з питань захисту даних добровільні під час підготування пропозиції для законодавчого інструменту, який повинен ухвалити національний парламент, консультації з наглядовим органом з питань захисту даних добровільні під час підготування регуляторного інструменту на підставі законодавчого інструменту, ухваленого національним парламентом
Греція	консультації з наглядовим органом з питань захисту даних добровільні під час підготування пропозиції для законодавчого інструменту, який повинен ухвалити національний парламент, консультації з наглядовим органом з питань захисту даних обов'язкові під час підготування регуляторного інструменту на підставі законодавчого інструменту, ухваленого національним парламентом
Князівство Ліхтенштейн	процедура попередньої консультації, яку має проводити контролер відповідно до статті 36 (1) ЗРЗД, регулюється національним законодавством, консультації з наглядовим органом з питань захисту даних добровільні під час підготування пропозиції для законодавчого інструменту, який повинен ухвалити національний парламент, консультації з наглядовим органом з питань захисту даних добровільні під час підготування регуляторного інструменту на підставі законодавчого інструменту, ухваленого національним парламентом
Португалія	процедура попередньої консультації, яку має проводити контролер відповідно до статті 36 (1) ЗРЗД, регулюється національним законодавством
Велике Герцогство Люксембург	Конкретних положень національного законодавства, у яких би згадувалася стаття 36 ЗРЗД, немає
Латвія	консультації з наглядовим органом з питань захисту даних добровільні під час підготування пропозиції для законодавчого інструменту, який повинен ухвалити національний парламент, консультації з наглядовим органом з питань захисту даних добровільні під час підготування регуляторного інструменту на підставі законодавчого інструменту, ухваленого національним парламентом
Чеська Республіка	консультації з наглядовим органом з питань захисту даних добровільні під час підготування пропозиції для законодавчого інструменту, який повинен ухвалити національний парламент, процедура попередньої консультації, яку має проводити контролер відповідно до статті 36 (1) ЗРЗД, регулюється національним законодавством
Австрія	процедура попередньої консультації, яку має проводити контролер відповідно до статті 36 (1) ЗРЗД, регулюється національним законодавством
Республіка Словенія	консультації з наглядовим органом з питань захисту даних добровільні під час підготування пропозиції для законодавчого інструменту, який повинен ухвалити національний парламент, консультації з наглядовим органом з питань захисту даних добровільні під час підготування регуляторного інструменту на підставі законодавчого інструменту, ухваленого національним парламентом
Болгарія	процедура попередньої консультації, яку має проводити контролер відповідно до статті 36 (1) ЗРЗД, регулюється національним законодавством, консультації з наглядовим органом з питань захисту даних обов'язкові під час підготування пропозиції для законодавчого інструменту, який повинен ухвалити національний парламент, консультації з наглядовим органом з питань захисту даних обов'язкові під час підготування регуляторного інструменту на підставі законодавчого інструменту, ухваленого національним парламентом, консультації з наглядовим органом з питань захисту даних добровільні під час підготування регуляторного інструменту на підставі законодавчого інструменту, ухваленого національним парламентом, національне законодавство вимагає від контролерів проводити консультації та отримувати попередній дозвіл від наглядового органу щодо опрацювання контролером для реалізації завдання, яке виконує контролер в інтересах суспільства, зокрема опрацювання у сфері соціального захисту та охорони здоров'я (пункт 5 статті 36 ЗРЗД), відповідь 4 – якщо йдеться про виправлення

29. Вкажіть, будь ласка, вашу діяльність у сфері просування обізнаності громадськості, а також поінформованості контролерів і операторів даних стосовно їхньої відповідальності:

Норвегія	проведення семінарів/вебінарів і консультування контролерів і операторів даних щодо положень Регламенту 2016/679
Словацька Республіка	проведення семінарів/вебінарів і консультування контролерів і операторів даних щодо положень Регламенту 2016/679
Румунія	проведення семінарів/вебінарів і консультування контролерів і операторів даних з приводу положень Регламенту 2016/679
Італія	проведення семінарів/вебінарів і консультування контролерів і операторів даних щодо положень Регламенту 2016/679, запуск інформаційних кампаній щодо захисту даних для контролерів і розпорядників даних з метою підвищення кваліфікації державних службовців, які обійматимуть посаду, пов'язану з відповідальністю за захист даних, кампанії з підвищення обізнаності з обов'язками/правами згідно з Регламентом
Естонія	проведення семінарів/вебінарів і консультування контролерів і операторів даних щодо положень Регламенту 2016/679, запуск інформаційних кампаній щодо захисту даних для контролерів або операторів даних з метою підвищення кваліфікації державних службовців, які обійматимуть посаду, пов'язану з відповідальністю за захист даних, у нас також діє служба підтримки для контролерів/операторів даних, суб'єктів даних, інших органів тощо
Хорватія	проведення семінарів/вебінарів і консультування контролерів і операторів даних щодо положень Регламенту 2016/679. Агентство проводить регулярні щотижневі тренінги, які відображають низку завдань і ролей посадових осіб, відповідальних за захист даних, пов'язаних з виконанням Загального регламенту про захист даних. Згадані тренінги проводяться окремо для державного та приватного секторів, щоб зосередитися на проблемах конкретного сектору; існують додаткові відмінності для певних видів діяльності, таких як сектор безпеки. За наслідками проведення згаданих тренінгів розробляються відповідні документи та брошури, доступні на нашому вебсайті. У рамках проєкту EU ARC (Кампанія з підвищення обізнаності для малих і середніх підприємств) Агентство захисту персональних даних Хорватії та Комісія з питань захисту даних Ірландії під час своєї повсякденної роботи помітили, що залишається багато неоднозначних моментів у застосуванні Регламенту малими і середніми підприємствами. Ці висновки підтверджуються також значною кількістю письмових запитів та ще більшою кількістю телефонних дзвінків, які ці два органи отримують щодня. Завдяки цьому проєктові Агентство захисту персональних даних Хорватії та Комісія з питань захисту даних Ірландії мають додаткові можливості, щоб допомогти цим суб'єктам у забезпеченні повного виконання вимог Регламенту та розумінні важливості захисту персональних даних шляхом проведення семінарів, презентацій та підготування навчальних матеріалів
Республіка Кіпр	проведення семінарів/вебінарів і консультування контролерів і операторів даних щодо положень Регламенту 2016/679, запуск інформаційних кампаній щодо захисту даних для контролерів і операторів даних з метою підвищення кваліфікації державних службовців, які обійматимуть посаду, пов'язану з відповідальністю за захист персональних даних, проведення публічних інформаційних кампаній і кампаній для студентів
Литва	проведення семінарів/вебінарів і консультування контролерів і операторів даних щодо положень Регламенту 2016/679, запуск інформаційних кампаній щодо захисту даних для контролерів і операторів даних з метою підвищення кваліфікації державних службовців, які обійматимуть посаду, пов'язану з відповідальністю за захист персональних даних. ДІЗД також підвищує обізнаність, ведучи таку діяльність: розробляє засоби інформування громадськості, готує методологічні документи, відвідує зустрічі з представниками публічного і приватного секторів, робить презентації під час заходів
Ісландія	проведення семінарів / вебінарів і консультацій для контролера та оператора стосовно положень Регламенту 2016/679
Греція	проведення семінарів / вебінарів і консультацій для контролера та оператора стосовно положень Регламенту 2016/679, виголошення промов, організація інформаційних днів і наукових конференцій
Князівство Ліхтенштейн	проведення семінарів / вебінарів і консультацій для контролера та оператора стосовно положень Регламенту 2016/679, проведення для контролерів та операторів інформаційних кампаній на тему захисту даних з метою підвищення кваліфікації державних службовців, що необхідно для обіймання посади особами, відповідальними за захист персональних даних
Португалія	проведення семінарів / вебінарів і консультацій для контролера та оператора стосовно положень Регламенту 2016/679
Велике Герцогство Люксембург	проведення семінарів / вебінарів і консультацій для контролера та оператора стосовно положень Регламенту 2016/679, проведення для контролерів та операторів інформаційних кампаній на тему захисту даних з метою підвищення кваліфікації державних службовців, що необхідно для обіймання посади особами, відповідальними за захист персональних даних

Латвія	проведення семінарів / вебінарів і консультацій для контролера та оператора стосовно положень Регламенту 2016/679, проведення для контролерів та операторів інформаційних кампаній на тему захисту даних з метою підвищення кваліфікації державних службовців, що необхідно для обіймання посади особами, відповідальними за захист персональних даних
Чеська Республіка	проведення для контролерів та операторів інформаційних кампаній на тему захисту даних з метою підвищення кваліфікації державних службовців, що необхідно для обіймання посади особами, відповідальними за захист персональних даних
Австрія	Австрійський ОЗД розміщує великий обсяг інформації на своєму вебсайті та випускає інформаційні бюлетені стосовно важливих рішень органу
Республіка Словенія	проведення семінарів / вебінарів і консультацій для контролера та оператора стосовно положень Регламенту 2016/679
Болгарія	проведення семінарів / вебінарів і консультацій для контролера та оператора стосовно положень Регламенту 2016/679, проведення для контролерів та операторів інформаційних кампаній на тему захисту даних з метою підвищення кваліфікації державних службовців, що необхідно для обіймання посади особами, відповідальними за захист персональних даних, проведення міжнародних конференцій, випуск інформаційних брошур, розроблення мобільного додатка, розроблення інструментів самооцінювання та інформування громадськості

30. Поінформуйте, будь ласка, чи орган має право передавати матеріали перевірок, які містять ознаки злочину, правоохоронному органові?

Норвегія	Це залежить від того, чи поширюється на цю інформацію наш обов'язок, закріплений у законі, щодо забезпечення конфіденційності, і, якщо так, чи передбачає цей обов'язок будь-які винятки
Словацька Республіка	Ні
Румунія	Ні
Італія	Так
Естонія	Так
Хорватія	Згідно зі статтею 38 Закону про виконання Загального регламенту про захист даних, якщо під час ведення контролю виявлені інформація або об'єкти, що вказують на скоєння кримінального правопорушення особою, яка діяла в рамках виконання своїх службових обов'язків, уповноважені особи повинні за найкоротший строк повідомити про цей факт відділ поліції або державного прокурора
Республіка Кіпр	Так
Литва	Так
Ісландія	Так
Греція	Так
Князівство Ліхтенштейн	Так
Португалія	Так
Велике Герцогство Люксембург	Так
Латвія	Так
Чеська Республіка	Так
Австрія	Так
Республіка Словенія	Так
Болгарія	Так

Діана ШИНКУНЄНЄ обіймала посаду заступниці директора Державної інспекції із захисту персональних даних Литовської Республіки (2001–2018), на якій, поміж іншим, відповідала за правовий аналіз проєктів законодавчих актів, а також чинного законодавства Литовської Республіки, зокрема надання пропозицій стосовно формулювання, внесення змін і скасування норм щодо захисту персональних даних і недоторканості приватного життя. У 2017–2018 роках вона брала участь у підготовці до здійснення на державному рівні реформи у сфері захисту персональних даних у Європейському Союзі – була керівником робочої групи, відповідальної за підготовку змін до Закону про правовий захист персональних даних у контексті Загального регламенту про захист даних (ЄС) 2016/679. Наразі вона є консультантом з питань захисту персональних даних і недоторканості приватного життя, співзасновником фірми, що працює у цій сфері, а також викладачем технологій конфіденційності і безпеки в Університеті Миколаса Ромеріса (Вільнюс, Литва).

Лілія ОЛЕКСЮК – юристка, магістр управління соціальним розвитком, кандидат наук з державного управління. З 2011 по 2014 роки працювала першою заступницею Голови Державної служби України з питань захисту персональних даних. Входить до складу Платформи громадянського суспільства, що є одним із органів відповідно до Угоди про асоціацію Україна–ЄС, має досвід громадської діяльності – є головою ГО «ВАІБІТ». Має власну практику і з 2018 року надає консультації із захисту персональних даних, розроблення державних автоматизованих систем, електронних довірчих послуг, розвитку цифрової економіки та інтеграції до Єдиного цифрового ринку ЄС. З 2019 року є позаштатним радником Комітету Верховної Ради з питань цифрової трансформації, а також є одним з авторів проєкту Закону «Про захист персональних даних» (реєстраційний №5628 від 7 червня 2021 р.).

Олександр ШЕВЧУК – кандидат юридичних наук. У 2019–2020 роках обіймав посаду національного експерта з електронного правосуддя за напрямком удосконалення захисту персональних даних у рамках проекту ЄС «Право–Justice». Наразі є національним консультантом у сфері захисту персональних даних у рамках спільного проекту ЄС та Ради Європи з посилення спроможностей Омбудсмана для захисту прав людини. У 2019–2021 роках брав участь у підготовці реформи системи захисту персональних даних в Україні. Олександр Шевчук є одним з авторів проєкту Закону «Про захист персональних даних» (реєстраційний №5628 від 7 червня 2021 р.).

Рада Європи є провідною організацією із захисту прав людини на континенті. Вона нараховує 47 держав-членів, включно з усіма державами – членами Європейського Союзу. Усі держави – члени Ради Європи приєдналися до Європейської конвенції з прав людини – договору, спрямованого на захист прав людини, демократії та верховенства права. Європейський суд з прав людини здійснює нагляд за виконанням Конвенції у державах-членах.

www.coe.int

Держави – учасниці Європейського Союзу вирішили поєднати свої ноу-хау, ресурси та долі. Разом вони збудували зону стабільності, демократії та сталого розвитку, зберігаючи при цьому культурне розмаїття, толерантність та громадянські свободи. Європейський Союз прагне поділитися своїми досягненнями та цінностями з країнами та народами за його межами.

www.europa.eu

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE