А.В. Пазюк

ЗАХИСТ ПРАВ ЛЮДИНИ СТОСОВНО ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ: МІЖНАРОДНІ СТАНДАРТИ

МГО “ПРАЙВЕСІ ЮКРЕЙН”

КИЇВ

“ІНТЕРТЕХНОДРУК”

2000

Пазюк А.В.

Захист прав людини стосовно обробки персональних даних: міжнародні стандарти / МГО Прайвесі Юкрейн - К.: Інтертехнодрук, 2000. – ___ с.

ISBN

Це одне з перших вітчизняних видань, що присвячено питанню захисту права людини на приватність особистої інформації (персональних даних). Значна увага приділяється розвитку концепції приватності та діяльності міжнародних організацій щодо вироблення стандартів для захисту приватності і транскордонних потоків персональних даних. Видання містить збірку міжнародних документів, що присвячено цьому питанню.

Для спеціалістів з інформаційних питань, прав людини і міжнародних відносин. Може бути корисним в практичній роботі політичних діячів і державних службовців для розробки національних положень в цій галузі і співпраці з іншими країнами і міжнародними організаціями.

Видання цієї книги стало можливим за сприянням Посольства Королівства Нідерландів в Україні.

Ключові слова: права людини, приватність, міжнародні стандарти, персональні дані, обробка даних.

ЗМІСТ

When Ukraine joined the Council of Europe on 11 September 1995, it undertook, as does each member state when it accedes, to respect the fundamental standards of this pan-European organisation and adapt its domestic law to conform to these standards.

Should a country wish to become a party to the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (known as Convention 108 because of its place in the European Treaty Series), and wish its legislation to provide a level of equivalent protection permitting the country to exchange data internationally without restriction, it must adopt legislation implementing the fundamental principles set out in this convention.

Convention 108, which was opened for signature on 28 January 1981, was based on the provisions of the *Convention for the Protection of Human Rights and Fundamental Freedoms* and in particular on its Article 8. The Council of Europe has adopted a number of sectional recommendations based on Convention 108, the most recent being Recommendation R (99) 5 on the protection of privacy on the Internet.

Ukraine ratified the *Convention for the Protection of Human Rights and Fundamental Freedoms* – and its Protocol No. 11 establishing a single Court – on 11 September 1997. The developing case law of the European Court of Human Rights has a determining influence on the work of the Council of Europe and also on the legislation of its member states in the field of data protection.

In the decision of *Z. v. Finland* of 25 February 1997, the Court recalled that data protection is a fundamental element of effective protection of the right to the respect for privacy. In the decision *Amman v. Switzerland*, of 16 February 2000, the Court confirmed this jurisprudence by recalling the relevance of Convention 108 in connection with the interference by the public authorities in the private life of an individual with regard to the collection and processing of his personal data.

The publication of basic international texts on data protection in the Ukrainian language, together with the decision by the Constitutional Court of Ukraine of 30 October 1997 and the action by non-governmental organisations such as *Privacy Ukraine* contribute to making citizens, public authorities and economic agents in Ukraine aware of the fundamental importance of data protection in a democratic society, particularly in the age of the information highways.

Spyros Tsovilis
The Head of Data Protection Unit
Directorate General I (Legal Affairs)
Council of Europe

Коли Україна приєдналася до Ради Європи 11 вересня 1995 року, вона зобов'язалася, як це робить кожна держава під час свого вступу, поважати основоположні стандарти цієї Пан Європейської організації і прийняти своє внутрішнє право, узгоджене з цими стандартами. Будь-яка країна, яка бажає стати стороною Конвенції із захисту фізичних осіб стосовно автоматичної обробки персональних даних (відомої як Конвенція 108 за її місцем у серії Європейських договорів) і хоче, щоб її законодавство забезпечувало рівень належного захисту, який дозволяє країні брати участь в міжнародному обміні даними без обмежень, повинна прийняти законодавство на виконання основоположних принципів, викладених у цій Конвенції.
Конвенція 108, яка була відкрита для підписання 28 січня 1981 року, побудована на положеннях Конвенції про захисту прав людини та основних свобод, зокрема, на її статті 8. Рада Європи ухвалила низку галузевих рекомендацій, що спираються на Конвенцію 108; остання з них - це рекомендація R (99)5 із захисту приватності в мережі Інтернет.
Україна ратифікувала Конвенцію про захист прав людини та основних свобод та її протокол № 11, яким запроваджується єдиний Суд, 11 вересня 1997 року.
Розвиток судової практики Європейського Суду з прав людини має вирішальний вплив на

роботу Ради Європи, а також на законодавства її держав-членів у галузі захисту персональних даних.
Своїм рішенням у справі *"Z проти Фінляндії"* від 25 лютого 1997 року, Суд ще раз проголосив, що захист персональних даних є складовою частиною захисту права на повагу до приватності. У справі *"Амман проти Швейцарії"* від 16 лютого 2000 року, Суд підтвердив цю юридичну доктрину, посилаючись у своєму рішенні на Конвенцію 108 у зв'язку з втручанням державних органів у приватне життя особи з огляду на збирання й обробку її персональних даних.
Опублікування основоположних міжнародних текстів із захисту персональних даних українською мовою, разом із рішенням Конституційного Суду України від 30 жовтня 1997 року, а також дії громадських організацій, таких як МГО "Прайвесі Юкрейн", сприятимуть усвідомленню громадянами, державними органами та суб'єктами економічних відносин в Україні принципової важливості захисту персональних даних у демократичному суспільстві, особливо у вік глобальних інформаційних магістралей.

Спірос Тсовіліс
Голова Секції із захисту даних
Головний Директорат I (Правові питання)
Рада Європи

With the advent of the information society and the introduction of computers into various areas of economic and social life, the Organisation for Economic Co-operation and Development (OECD) was the first intergovernmental organisation to issue guidelines on international policy for the protection of privacy in computerised data processing.

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines) were adopted as a Recommendation of the OECD Council on 23 September 1980 in support of the three principles that bind OECD Member countries: pluralistic democracy, respect for human rights and open market economies. In addition to the OECD Privacy Guidelines, two other international instruments prepared by the Council of Europe and the United Nations were adopted in 1981 and 1990, respectively.

More recently, at the Ottawa Ministerial Conference held in October 1998, OECD Ministers reaffirmed "their commitment to the protection of privacy on global networks in order to ensure the respect of important rights, build confidence in global networks, and to prevent unnecessary restrictions on transborder flows of personal data". In particular, they declared that they would "work to build bridges between the different approaches adopted by Member countries to ensure privacy protection on global networks based on the OECD Privacy Guidelines".

The principles set forth in the OECD Privacy Guidelines are characterised by their clarity and flexibility of application and by their formulation which is sufficiently broad to enable them to adapt to technological change. The principles encompass all media for the computerised processing of data on individuals (from local computers to networks with complex national and international ramifications), all types of personal data processing (from personnel administration to the compilation of consumer profiles) and all categories of data (from traffic data to content data, from the most mundane to the most sensitive). Over the years, the principles have been put to use in a large number of national regulatory or self-regulatory instruments and they are still widely used in both the public and private sectors.

More than 30 countries, including the 15 member states of the European Union, have adopted legislation to protect privacy and personal data, applicable, depending on the country, to the public and private sectors or to the public sector alone. On 13 April 2000, Canada enacted legislation on Personal Information Protection and Electronic Documents which will come into force on 1 January 2001. Australia and Japan are currently considering passing special

legislation to protect privacy in the private sector. In countries that rely more on self-regulation to protect personal data, texts which apply to specific industry sectors are nevertheless applicable. In addition, standards and industry-wide provisions, such as codes of conduct which serve as a reference, have been adopted in many sectors of the economy.

In this context, the recognition of the right to privacy in the Ukrainian Constitution must be welcomed as an important step, and any effort to implement this right and to protect personal data in line with international consensus should be warmly encouraged.

Risaburo Nezu
Director
OECD Directorate for
Science, Technology and Industry

З приходом інформаційного суспільства та впровадженням комп'ютерів у різних сферах економічного та суспільного життя, Організація Економічної Співпраці і Розвитку (ОЕСР) була першою міжурядовою організацією, яка ухвалила керівні принципи щодо міжнародних політики у галузі захисту приватності під час комп'ютеризованої обробки даних.

Керівні принципи про захист приватності та транскордонні потоки персональних даних (Керівні принципи з приватності) були прийняті у вигляді Рекомендації Ради ОЕСР 23 вересня 1980 року у підтримку трьох принципів, якими пов'язані країни члени ОЕСР: плюралистичної демократії, поваги до прав людини та відкритої ринкової економіки. До того ж, окрім Керівних принципів ОЕСР, два інших міжнародних інструменти підготовлені Радою Європи та Організацією Об'єднаних Націй були прийняті у 1981 та 1990 роках відповідно.

Нещодавно на Конференції Міністрів у Отаві у жовтні 1998 року, міністри ОЕСР підтвердили "своє намагання захистити приватність у глобальних мережах з метою забезпечення поваги до важливих прав, побудови конфіденційності у глобальних мережах та запобіганню непотрібних обмежень під час трансокрдонних потоків персональних даних". Зокрема, вони проголосили, що вони будуть "працювати для побудови мостів між різними підходами прийнятими країнами членами для забезпечення захисту приватності у глобальних мережах на базі Керівних принципів з приватності ОЕСР".

Положення, що їх містять Керівні принципи з приватності ОЕСР, характеризуються своєю яністю та гнучкістю для застосування та своїми формулюваннями, достатньо широкими для пристосування до технологічного прогресу.

Принципи орієнтують усіх інформаційних агентів на їх дотримання під час комп'ютеризованої обробки даних про індивідів (від локальних комп'ютерів до мереж національного та міжнародного рівня) усіх типів персональних даних, що оброблятимуться (від адміністрування даних службою кадрів до складання профілю споживача), та усіх категорій даних (від допоміжних операційних до основних, від пересічних до вразливих). За минувши роки, ці принципи були впроваджені у величезній кількості національних регуляційних або саморегуляційних інструментах та до цього часу широко використовуються як у публічному, так і приватному секторах.

Більше 30 країн, включаючи 15 держав членів Європейського Союзу, прийняли законодавство для захисту приватності та персональних даних, яке має застосовуватися, у залежності від країни, до публічного та приватного секторів, чи лише до публічного сектора. 13 квітня 2000 року, Канада прийняла національні положення з питань захисту персональної інформації та електроних докуметів, які вступять у дію з 1 січня 2001 року. Австралія і Японія розглядають питання законодавчого регулювання захисту приватності у публічному секторі. В країнах, які більше використовують підхід саморегуляції у питанні захисту персональної інформації, національні положення, що орієнтовані на специфічні сектори індустрії, тим не менш, застосовуються. Крім того, стандарти та положення поширені в індустрії, такі як кодекси поведінки, які слугують як рекомендації, були прийняті у багатьох секторах економіки.

У цьому контексті, визнання права на приватність у Конституції України має відзначатися як важливий крок, та будь-які зусилля срямовані на імплементацію цих прав та захисту

персональних даних у відповідності з міжнародними домовленностями мають бути дружньо схвалені.

Різабуро Нецу
Директор
Директорату ОЕСР з питань науки, технологій та індустрії

El derecho a la privacidad y a la intimidad personal y familiar forma parte del núcleo esencial del ser humano y, como tal, ha sido reconocido tanto en la Declaración Universal de los Derechos del Hombre de las Naciones Unidas como en el Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales del Consejo de Europa.
En el territorio de la UE, este derecho ha sido armonizado por la promulgación de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que establece un alto estándar de protección de la privacidad de los ciudadanos de la Unión Europea al mismo tiempo que garantiza, mediante dicha armonización, la libre circulación de datos personales entre los Estados miembros.
Asimismo, establece restricciones para la transferencia de datos personales a terceros países que no garanticen una protección adecuada, evaluándose dicho nivel en función, entre otros aspectos, de las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate.
Por lo tanto, dado que el derecho a la privacidad está constitucionalmente reconocido en Ucrania, al igual que ocurre en España, me complace dar la bienvenida a este compendio de las normas de Derecho internacional más relevantes en esta materia que, sin duda, resultará de sumo interés para todas aquellas personas e instituciones interesadas en su estudio y en el desarrollo legislativo de la Constitución ucraniana en tan relevante aspecto.

Juan Manuel Fernández López
Director de la Agencia de Protección de Datos

Право на приватність, а також на приватну сферу особистого і сімейного життя становить серцевину сутності людини, і як таке було визнане в Універсальній Декларації прав людини ООН та в Європейській Конвенції про захист прав людини та основних свобод Ради Європи.

Публікація Директиви ЄС 95/46/СЕ про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних, що встановлює високий стандарт захисту приватності громадян Європейського Союзу і одночасно гарантує вільний рух персональних даних між країнами-членами, стала одним із чинників забезпечення реалізації цього права на території ЄС.

Директива також встановлює обмеження щодо передачі персональних даних третім країнам, які не гарантують адекватного захисту, оцінюючи цей рівень з урахуванням, серед іншого, стану законності під час реалізації норм права – як загальних, так і галузевих, - що діють у цій третій країні.

Отже, з огляду на те, що право на приватність є конституційно визнаним в Україні, так само як і в Іспанії, я із задоволенням схвалюю цей збірник основних норм міжнародного права, який безперечно викличе великий інтерес в осіб і інституцій, які зацікавлені у дослідженні та законодавчому розвитку відповідних положень Конституції України.

Хуан Мануель Фернандес Лопес
Директор Агенції з захисту даних

ВСТУП

Ця книга присвячується питанню захисту приватності особистої інформації або персональних даних людини. Останнє формулювання більше відповідає духу нового "цифрового віку" (digital age), в якому інформація оброблятиметься автоматизованими системами, а тому матиме форму "даних".

Питання поводження з персональними даними є надзвичайно актуальним для нашої держави, з огляду на впровадження вітчизняних комп'ютерних баз персональних даних у податковому, пенсійному та інших секторах.

Між тим, в Україні відсутній спеціальний закон, який би гарантував громадянам право на правомірне поводження з особистою інформацією, що оброблятиметься в цих базах даних.

Так, ще у 1997 році, під час розгляду справи про порушення права людини на доступ до персональних даних, Конституційний Суд України встановив "наявність у нормативно-правовій базі в частині інформаційних правовідносин нечітко визначених, колізійних положень і прогалин, що негативно впливає на забезпечення конституційних прав і свобод людини і громадянина" (Рішення від 30.10.1997 року, справа К. Г. Устименка). Ця справа мала б привернути увагу законодавців на існуючу проблему, але на жаль цього не сталося.

Правовий вакуум в питанні захисту прав людини на приватність особистої інформації, не можна заповнити загальними положеннями законодавства України про інформацію. Оскільки правовий режим особистої інформації охоплюється поняттям "приватність" (privacy), яке бере свої витоки з фундаментального права людини на повагу до її приватного життя. З метою ознайомлення вітчизняних спеціалістів з цим поняттям перший розділ цього видання присвячено саме розвитку концепції права на приватність.

Однак інформація це не тільки один з аспектів прав людини. Інформація також є економічна категорія. Зважаючи на такий дуалізм, необхідно враховувати обидва фактори при встановлені державою пріоритетів регулятивної політики в цій галузі. Оскільки невідповідність національного законодавства міжнародним стандартам з питань поводження з персональними даними, зокрема тим, що наведено у другому розділі цієї книги, матиме наслідком не лише порушення прав людини, а і економічні проблеми під час транскордонних передач персональних даних.

Наше видання покликано привернути увагу зацікавлених осіб до вирішення проблеми захисту права на приватність персональних даних в Україні і має бути використано для розробки національних положень, які б відповідали міжнародним стандартам у цій галузі.

РОЗДІЛ 1. РОЗВИТОК КОНЦЕПЦІЇ

1. Право на приватність: розвиток концепції.

Право на приватність (‘right to privacy’) увійшло до переліку фундаментальних прав і свобод людини не так давно. Хоча елементи цього поняття можна зустріти в самих ранніх джерелах права, для формування правового інституту приватності знадобився певний розвиток цивілізації, при якому автономність життя стала вкрай необхідною для збереження і реалізації людиною своєї особистості. “Зростаюча інтенсивність та складність життя зробили необхідним набуття певного притулку від цього світу; а людина під впливом культури, стала більш чутливою до гласності, через це усамітнення і приватність життя стали ще більш необхідними для індивіда…[1]”

Безпосередньою причиною для створення першої правової концепції приватності стала публікація на шпальтах газет Бостона (США) дрібниць одного весілля. Обурений батько нареченої, бостонський юрист Самуель Воррен та його колега Луїз Брандез вирішили розробити правове поняття, що змогло б захистити приватне життя людини від втручання з боку інших осіб. У своїй статті, в 1890 році, вони писали: “сучасні винаходи і бізнес-методи вимагають уваги до наступних кроків, що мають бути зроблені для захисту індивідів”. На їхню думку право на приватність – це право “бути залишеним у спокої”(let to be alone) [2].

Міжнародне визнання право на приватність отримало з прийняттям 10 грудня 1948 року Генеральною Асамблеєю ООН Загальної декларації прав людини. Стаття 12 Декларації проголосила:

Ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, тайну його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань.

На європейському рівні першою за порядком та значенням залишається Європейська Конвенція про захист прав та основних свобод людини, яка була відкрита для підписання державами учасницями Ради Європи 4 листопада 1950 року. Право на захист приватної сфери життя людини гарантується у першій частині Статті 8 Конвенції:

Кожна людина має право на повагу до її особистого і сімейного життя, житла і таємниці кореспонденції.

Така редакція статті є результатом узгодження позицій творців проекту Конвенції та свідчить про їх намір залишити за державами учасницями право самостійно визначати правові рамки здійснення проголошеного у статті права.

Конвенція не дала чіткого визначення поняттю “право на повагу…”. Але це не завадило Комісії та Суду, - контрольним органам Конвенції, - під час розгляду справ про порушення права на приватність конкретизувати зміст цієї правової норми. В одному з своїх рішень з цього питання Комісія відзначила [3]:

Для багатьох англосаксонських та французьких авторів, право на повагу до приватного життя це право на конфіденційність, право жити так як людина бажає, бути захищеним від розголосу ... На думку Комісії, право на повагу не обмежується цим. Воно містить також, до визначеного рівня, право встановлювати та розвивати стосунки з іншими людьми, особливо у емоційній сфері, для розвитку та реалізації людиною своєї особистості.

Концепція приватності розвивалась і на національному рівні. У 1960 році юрист Вільям Л. Проссер після вивчення прецедентів створених американськими судами під час розгляду справ щодо втручання у приватне життя людини, запропонував класифікацію можливих деліктів в цій сфері. Серед них: розкриття фактів, що стосуються приватного життя; повідомлення неправдивої інформації про людину; неправомірне використання зображень, голосу людини; і нарешті останнє, фізичне домагання [4].

За однією із сучасних класифікацій, пропонується розмежувати сфери, в яких реалізується суспільна активність людини, що дозволяє розбити загальну проблему захисту приватності людини на сектори, які вимагають окремого законодавчого регулювання. Серед іншого, така класифікація дозволяє зрозуміти комплексність і взаємопов’язаність усіх елементів цього правового поняття. За цим критерієм приватність поділяється на чотири види [5]:

- інформаційна приватність, якою охоплюються правила стосовно збору і обробки інформації про людину (персональних даних);
- тілесна (фізична) приватність, яка стосується захисту фізичної недоторканності людини від примусових процедур, таких як наркологічне тестування та ін.;
- комунікаційна приватність, яка охоплює безпеку і конфіденційність поштових відправлень, телефонних розмов, електронної кореспонденції та інших форм зв’язку;
- територіальна приватність, яка стосується встановлення правових рамок для захисту від втручання в сімейну сферу, інше оточення, скажімо на робочому місці або в транспортному засобі.

Предметом нашого дослідження є саме інформаційна приватність, тобто приватність інформації про людину. Стрімкий розвиток інформаційних технологій, їх неоднозначний вплив на життя кожної окремої людини і всього суспільства вимагає окремої уваги питанню

забезпечення прав людини, і права на приватність, зокрема, під час користування можливостями, що їх надає інформаційне суспільство.

Сама концепція інформаційної приватності також зазнає вплив цих технологій. Російським вченим В.П. Іванским відповідно до періодизації фаз розвитку інформаційного суспільства запропоновані так звані “еволюційні форми” інформаційної приватності, серед яких “мас-медійна”, “комп’ютерна” і “мережева” [6]. Перелічені форми відповідають домінуючим у визначений час засобам збору і обробки інформації про людину (“основні носії інформації”). У якості таких основних носіїв інформації поступово виступають засоби масової інформації, комп’ютерні бази даних і телекомунікаційні мережі.

З появою перших комп’ютерів і автоматизованої обробки персональних даних постало питання регулювання правил поводження з даними. Перші законодавчі акти були прийнятті деякими Європейськими країнами на початку 80-х років двадцятого століття [7]. Разом з тим обрані цими державами підходи багато у чому не співпадали. До того ж виникла проблема обміну даними з країнами, що на той час не мали відповідного регулювання з цього питання.

Неузгодженість національних підходів і діяльності відповідних органів мала наслідком появу заборон на передачу персональних даних через кордони, що стало бар’єром для зовнішньоекономічних стосунків партнерів по бізнесу у різних країнах.

Так, у 1978 році один з Комітетів Великої Британії доповідав про два випадки відмови з боку владних структур Швеції дозволити експорт персональних даних з тих підстав, що національне законодавство Великої Британії на той час не містило положень, які б гарантували захист персональних даних. У свою чергу, у грудні 1990 року, Реєстратор персональних даних Великої Британії заборонив передачу даних до США, ґрунтуючи своє рішення на тому, що законодавство США не надає адекватного рівня захисту персональних даних у приватному секторі [8].

Вирішити цю проблему на національному рівні було неможливо з огляду на існуючі розбіжності у національних підходах. Зростаючий транскордонний обмін інформацією вимагав вжиття негайних заходів на міжнародному рівні.

2. Захист приватності і транскордонних потоків персональних даних в діяльності міжнародних організацій.

Зусилля, спрямовані на створення міжнародних стандартів для узгодження національних положень щодо захисту персональних даних, були вжиті трьома організаціями: Організацією Економічної Співпраці і Розвитку (ОЕСР), Радою Європи та Європейськими Співтовариствами - Європейським Союзом.

Починаючи з 70-х років, створені цими організаціями групи експертів займаються розробкою і вдосконаленням стандартів у галузі захисту приватності і транскордонних потоків персональних даних.

Рада Європи

На відміну від ОЕСР та Європейських Співтовариств, які створені на основі спільного економічного інтересу держав-членів, основною задачею Ради Європи був і залишається захист прав людини та основних свобод. І на Раді Європі лежить відповідальність за розвиток права на повагу до приватного життя, яке гарантовано статтею 8 Європейської Конвенції про захист прав людини та основних свобод 1950 року.

Комітет Ради Європи з правових питань сформував Комісію експертів з приватності та комп'ютерів у 1971 році. Перші кроки були зроблені у напрямку встановлення спеціальних принципів та норм для запобігання неправомірному збору і обробки персональних даних в електронних базах даних. Комісія підготувала проекти двох резолюцій: однієї – для застосування у приватному секторі економіки (№22), другої – у публічному (№29). Комітет Міністрів затвердив першу в 1973 році, другу – в 1974 році.

Під час підготовки цих документів стало зрозумілим, що для досягнення ефективності у захисті персональних даних необхідно укріпити існуючі національні норми, використовуючи міжнародні інструменти. Така ж сама пропозиція пролунала під час 7-ої конференції Європейських міністрів юстиції у 1972 році і була відзначена у її резолюції №3 [9].

Комітет Ради Європи з правових питань зважив на вказану пропозицію і почав розробку проекту майбутньої конвенції. У 1976 році для цього була сформована нова комісія. Комісія експертів із захисту даних, як її назвали, збиралася чотири рази на пленарні засідання і підготовила проект у травні 1979 році, а його фінальну версію у квітні 1980 року. У тому ж році, Парламентська Асамблея Ради Європи прийняла Рекомендацію № 890, у якій зазначалося про необхідність ефективного захисту персональних даних і було запропоновано включити відповідне положення до тексту Європейської Конвенції про захист прав людини та основних свобод [10].

Конвенція Ради Європи № 108 Про захист осіб стосовно автоматизованої обробки персональних даних була відкрита для підписання 28 січня 1981 року і набрала сили 1 жовтня 1985 року, після того, як п'ять держав-членів Ради Європи висловили своє бажання бути пов'язаними положеннями Конвенції. Ними стали Швеція, Франція, Норвегія, Іспанія та ФРГ. Серед цих країн, усі за виключенням Іспанія, мали національні акти про захист даних на час ратифікації.

Станом на квітень 2000 року учасниками Конвенції є 20 країн, ще п'ять її підписали, але не ратифікувала. Конвенція Про захист осіб стосовно автоматизованої обробки персональних

даних є одним з перших міжнародних інструментів, який завдяки своєму обов'язковому характеру закріпив мінімальні стандарти у галузі захисту інформаційної приватності.

Конвенція складається з трьох основних частин: основних принципів, спеціальних правил стосовно передачі даних через кордони і механізмів співпраці і консультацій між державами-учасниками Конвенції.

Центральною частиною Конвенції є Глава 2, яка містить основні принципи захисту персональних даних, що становить "стрижень" цього документа. Слід відзначити, Конвенція лише вказує на мету, яка має бути досягнута через застосування цих принципів, але залишає кожній державі-учасниці право визначати спосіб у який вони повинні бути імплементовані у національному законодавстві.

Глава 3 Конвенції стосується питань транскордонної передачі даних і покликана погодити, збалансувати одночасно існуючі вимоги щодо вільного потоку інформації і захисту даних. Проголошується, що транскордонні потоки даних між державами-членами Конвенції не можуть бути об'єктом будь-якого спеціального контролю.

Глави четверта і п'ята встановлюють механізми взаємодії між державами-учасницями у справах, що стосуються окремих індивідів (Глава 4), та стосовно Конвенції в цілому (Глава 5).

Слід звернути увагу на те, що Конвенція № 108 не є "європейською", що відрізняє її від інших конвенцій Ради Європи. У цьому розумінні, Стаття 23 несе в собі важливий елемент, оскільки дозволяє вступ до Конвенції держав, які не є членами Ради Європи. Це зроблено для того, щоб закласти фундамент для досягнення міжнародного консенсусу в питаннях захисту персональних даних, особливо з третіми, неєвропейськими країнами.

Із прийняттям Конвенції активність Ради Європи у цій галузі не зменшилася. Проектна група з питань захисту даних (CJ-PD), до складу якої входять експерти з кожної держави-члена Конвенції, підготувала серію рекомендацій, які значною мірою розширюють та конкретизують принципи, що їх було проголошено у Конвенції.

Оскільки умови і методи роботи з даними певним чином залежать від виду даних, рекомендації розраховані на обробку даних, що відбувається у таких секторах, як: медичний і науково-дослідний, сектор рекламного бізнесу, соціального забезпечення, сектор поліцейських записів і даних з працевлаштування, даних у сфері фінансових розрахунків, і телекомунікаційних послуг, а також під час передачі публічними органами даних третім сторонам. Остання з затверджених Комітетом Міністрів рекомендацій стосується питання забезпечення приватності під час користування мережею ІНТЕРНЕТ та розрахована на її застосування користувачами та постачальниками інформаційних послуг [11].

Вказаний спосіб адаптації принципів приватності до нових умов роботи з персональними даними виявився вдалим через те, що процедура прийняття рекомендації і їх затвердження

Комітетом Міністрів є простішою за процедуру внесення змін до тексту Конвенції, що вимагало б їх ратифікації кожною державою-учасницею Конвенції.

Окрім рекомендацій експерти Проектної Групи здійснили у 1991 році дослідження питань, що виникають під час застосування персональних ідентифікаційних номерів [12]. А представниками Консультативного Комітету за активної участі експертів Європейських Співтовариств і Міжнародної Торгової Палати розроблено "Модельний контракт на забезпечення еквівалентного захисту персональних даних у контексті питання транскордонних потоків даних" 1992 року. Положення модельного контракту є спрямовані на регулювання умов передачі даних до країн, в яких рівень захисту даних не відповідає стандартам Ради Європи [13].

Консультативним Комітетом підготовлено проект додаткового протоколу до Конвенції, метою прийняття якого є запровадження інституту наглядової інстанції у питаннях захисту персональних даних [14].

В цьому ж протоколі запропоновано встановити правило, що принципово змінює підхід до регулювання питань транскордонної передачі даних. Так, стаття 12 Конвенції встановлює правило, за яким забороняється застосування обмежень на експорт даних до іншої держави, яка надає еквівалентний захист. Тобто тут нема позитивної вимоги на обмеження експорту персональних даних. Це залишається на розсуд держави-учасниці Конвенції.

Стаття 2 Додаткового протоколу пропонує наступне:

"Кожна Сторона здійснює передачу персональних даних одержувачу, який перебуває під юрисдикцією Держави чи організації, яка не є Стороною цієї Конвенції лише за умов, що ця Держава чи організація забезпечують адекватний рівень захисту для запропонованої передачі даних…"

Цим положенням, зокрема, встановлюється, що передача даних до третіх країн або організацій заборонена, якщо вони не гарантують адекватний рівень захисту приватності щодо визначеної передачі персональних даних.

Такий підхід у регулюванні транскордонних потоків даних є аналогічний до того, що був обраний Європейським Союзом, і свідчить про прагнення європейських країн встановити пан-європейські стандарти у галузі захисту персональних даних на основі Конвенції Ради Європи. Це пояснює і зацікавленість Європейських Співтовариств у приєднані до Конвенції № 108 [15]. Доповнення набудуть чинності після їх ратифікації всіма державами-учасниками Конвенції.

Організація Економічної Співпраці і Розвитку (ОЕСР)

Організація Економічної Співпраці і Розвитку почала дослідження питань пов'язаних із транскордонними потоками даних у 1969 році. Група з питань застосування комп'ютерів, а пізніше Комісія з питань баз даних проаналізувала та підготувала доповіді з різних аспектів, що стосуються питань приватності персональних даних, зокрема, цифрової інформації, транскордонних потоків даних, управління інформаційною діяльністю.

У 1977 році Комісія ОЕСР з питань баз даних спільно з Комітетом експертів Ради Європи у Відні провели міжнародний симпозіум, де відбувся обмін думками та досвідом людей, що представляли різні інтереси, включаючи представників політичних і бізнесових кіл, користувачів міжнародних мереж та зацікавлених міжнародних організацій. Під час його проведення було вироблено спільну позицію щодо необхідності встановлення на міжнародному рівні основоположних принципів для регулювання міжнародного обміну інформацією, що стосується осіб [16].

На початку 1978 року була сформована нова Група експертів з питань транскордонних потоків та захисту приватності на чолі з головою Австралійського Комітету з правової реформи паном *M.D. Kirby*. Група підготувала низку доповідей щодо ключових проблем обміну персональними даними і проаналізувала різні підходи, які обрали країни - члени ОЕСР у законодавчому регулюванні цих питань.

Серед членів ОЕСР на час ухвалення Керівних принципів деякі країни вже прийняли нормативні акти, які передбачали відповідне регулювання питань захисту інформаційної приватності. Так, Австрія, Канада, Данія, Франція, Люксембург, Норвегія, Швеція та Сполучені Штати вже мали відповідні закони. А Бельгія, Ісландія, Нідерланди, Іспанія та Швейцарія підготували законопроекти.

Наявні розбіжності між країнами торкалися питань сфери законодавчого регулювання, уваги до певних елементів захисту та контрольного механізму. Зокрема, не було узгодженості в питаннях запровадження ліцензування і функціонування контрольного механізму у формі спеціально уповноваженого наглядового органу, категорій "вразливих даних", розуміння принципу прозорості і індивідуальної участі суб'єкта даних в процесах обробки даних. До цього ж додавалися традиційні розбіжності між правовими системами, з яких випливали різні підходи до закріплення правил поводження з даними на законодавчому рівні.

Все це зумовило характер прийнятого документа. Керівні принципи, які були ухвалені у вигляді рекомендації, встановлюють узагальнені правила поводження з персональними даними. Вони є мінімальними стандартами, що створені в результаті пошуку консенсусу між країнами-членами ОЕСР в цьому питанні.

Керівні принципи про захист права на приватність та транскордонні потоки персональних даних вступили в дію 23 вересня 1980 року після ухвалення Рекомендації Радою ОЕСР на її 523-ому засіданні.

Документ складається з п'яти частин. Перша частина містить низку визначень та окреслює сферу застосування Керівних принципів. Друга частина вміщує вісім основних положень (пункти 7-14), які становлять стрижень Керівних принципів. Частина 3 подає принципи міжнародного застосування, що пов'язані з взаємовідносинами країн-членів ОЕСР в цьому питанні.

Питання імплементації основних принципів викладені у четвертій частині. Тут же конкретизується, що принципи повинні застосовуватися на недискримінаційній основі. П'ята частина присвячена питанням співпраці країн-членів, яке здійснюється через обмін інформацією, уникнення несумісних національних процедур для захисту персональних даних.

Рекомендація не покладає на країни-члени ОЕСР таких зобов'язань як Конвенція Ради Європи № 108 на її учасників. Разом з тим, Керівні принципи обмежують можливість застосування виключень з встановлених в них правил, що посилює цей документ.

До того ж Керівні принципи поширюють свою дію не лише на автоматизовані файли даних, як Конвенція Ради Європи, а і на дані, "обробка яких несе загрозу приватності та індивідуальним свободам незалежно від методів і засобів поводження з ними". Група експертів аргументувала такий підхід намаганням уникнути можливих прогалин у регулюванні, причиною яких є проблема розмежування на технічному рівні процесів автоматизованої і неавтоматизованої обробки даних, зокрема, у "змішаних" системах.

Крім того, Керівні принципи більш конкретно визначають права суб'єкта даних. Так, принцип 13 регламентує "індивідуальну участь" суб'єкта даних в процесі доступу, і містить право на отримання даних, що його стосуються. Суб'єкту даних надається право оскаржити будь-яку відмову в надані такої інформації, та отримати обґрунтування такої відмови.

Питання вільної передачі даних отримало свій подальший розвиток в Декларації про транскордонні потоки даних, яка була підготовлена Комітетом з інформації, комп'ютерам та комунікаціям у березні та затверджена Міністрами країн-членів у квітні 1985 року [17].

Приймаючи Декларацію, країни-члени ОЕСР підтвердили своє намагання забезпечити вільний обмін інформацією, та розробити спільні політичні підходи до питань транскордонної передачі даних, зокрема, щодо передачі інформації у торговельній сфері, внутрішньо-корпоративного обміну даними, комп'ютеризованих інформаційних послуг, наукового та технологічного обміну.

А у листопаді 1992 року, Рада ОЕСР ухвалила Рекомендацію про Керівні принципи щодо безпеки інформаційних систем [18]. Цей документ передбачає прийняття країнами національних положень для забезпечення захисту цілісності і конфіденційності

інформаційних систем та інформації, що в них обробляється, через вжиття комплексу організаційних і технічних захисних заходів.

Питанням гармонізації політики країн-членів ОЕСР у сфері застосування криптографічного захисту інформації присвячена Рекомендація про Керівні принципи щодо політики у галузі криптографії, ухвалена в березні 1997 року [19]. Документ встановлює принципи спрямовані на регламентування прав користувачів щодо вибору криптографічних методів, вільного проектування таких методів і засобів, можливість взаємодії інформаційних мереж, їх значення для захисту персональних даних та усунення бар'єрів в міжнародній торгівлі.

У жовтні 1998 року, в Отаві (Канада), на засіданні Міністрів 29 країн-членів ОЕСР присвяченому електронній комерції розглядалося питання захисту приватності в глобальних інформаційних мережах. Серед його результатів, зокрема, прийняття Декларації про захист приватності в глобальних мережах.

Декларація визнає за необхідне "захист приватності в глобальних інформаційних мережах для забезпечення поваги до основних прав, побудови довіри … і запобігання встановленню зайвих обмежень для транскордонної передачі даних [20]". В Декларації відзначається важливість прийняття на національному рівні комплексної програми заходів для забезпечення приватності, зокрема, попередження користувачів мереж щодо проблеми приватності в інформаційному просторі, їх навчання, сприяння розвитку технологій, що гарантують приватність інформаційного обміну.

Розвиток інформаційних технологій і глобалізація інформаційних потоків, вимагає перегляду раніше встановлених принципів з метою їх адаптації до вимог часу. Таку позицію, зокрема, розділяє керівник Групи експертів, що займалась їх розробкою, пан *M.D. Kirby*:

"Ця неочікувана дитина, зачата у союзі економіки і прав людини, народилася у 1980 році, а зараз їй вже 20 років. Її батьки вдячні та пишаються нею. Світ сучасності, особливо світ технологій змінився у порівняні із світом, до якої вона ввійшла майже двадцять років тому. Настав час врахувати зміни та їх вплив [21]".

Перед ОЕСР постає необхідність переосмислити раніше досягнутий між країнами-членами консенсус з цього питання. Це непросте завдання ускладнюється існуючими розбіжностями в стандартах між європейськими і неєвропейськими країнами-членами ОЕСР.

Європейські Співтовариства – Європейський Союз.

Європейське Економічне Співтовариство в перший раз згадує про захист даних у доповіді 1973 року, що була продовжена дебатами у Європейському Парламенті в 1974-75 роках. Про необхідність узгодження політики країн Європейських Співтовариств в цьому питанні ідеться у Резолюції, що була ухвалена Радою ЄС у липні 1974 року [22].

У червні 1979 року Парламент ухвалив підготовлену експертами Комітету з правових питань Резолюцію “Про захист прав індивідів стосовно технічного розвитку і обробки даних”, в якій робиться акцент на створені спільного ринку в обробці даних. У Резолюції, зокрема, зазначається, що національні положення в галузі захисту приватності мають безпосередній вплив на такий спільний ринок, а саме, здатні “деформувати умови конкуренції”.

У Рекомендації від 29 липня 1981 року № 81/679/EEC, яка присвячується затвердженню Радою Європи Конвенції № 108, вказується про її прийнятність для створення однакового рівня захисту інформаційної приватності в Європі [23].

Фактором, що активізував розробку документа, стала не вирішена повною мірою проблема транскордонної передачі даних як всередині Європи, так і при передачі даних за межі континенту.

Випадок, який отримав значний резонанс, стався у 1991 році, коли Французьке агентство з питань захисту персональних даних заборонило компанії *Фіат* електронну передачу інформації про французьких працівників компанії до її головного офісу в Італії, доки *Фіат* не погодиться бути пов’язаною вимогами законодавства Франції про захист даних.

Інший випадок стався у 1992 році. Німецький банк відмовився надати своєму підрозділу у Гон Конзі доступ до інформації про клієнтів банку, громадян Німеччини [24].

Європейська Комісія подала проект директиви у вересні 1990 році після низки запитів Європейського Парламенту щодо необхідності вжиття заходів у цій галузі. С численними зауваженнями Європейського Парламенту проект подали на друге читання у жовтні 1992 року.

У лютому 1994 року держави-члени дійшли політичної угоди стосовно основних положень директиви; і лише через рік Рада Міністрів ухвалила “спільну позицію”, що була підтверджена Парламентом у червні 1995 року. Директива набула чинності 24 жовтня 1995 року.

Процес проходження Директиви супроводжувався протидією з боку бізнесових кіл, як європейських, так і американських. Запропоновані Директивою правила вимагали, щоб індивіди надавали свою “повідомлену згоду” на вторинне, у тому числі при зміні цілі, використання персональних даних. Це положення було включено до тексту директиви з метою заборонити комерційним структурам продаж та обмін інформацією про осіб без сповіщення і згоди суб’єкта даних.

На практиці це означає, що суб’єкт даних має виявити бажання на будь-яке подальше використання, так звана формула ‘opt in’. В той час як для комерційних структур більш підходить пасивна форма, коли особа повідомляється про вторинне використання і їй надається можливість заперечувати проти такого використання чи обміну, що відповідає формулі ‘opt out’ [25].

Принципи інформаційної приватності, що їх містить друга частина документа, відповідають за свої духом принципам ОЕСР та Ради Європи і базуються на них. Разом з тим, певні положення Директиви розширюють коло прав суб'єктів даних, що дозволяє віднести Директиву ЄС до нового покоління міжнародних інструментів в галузі інформаційної приватності.

Так, стаття 11 встановлює, що у разі отримання персональних даних не від самої особи, а з інших джерел, суб'єкт даних має бути сповіщеним про цілі збору і обробки, її одержувачів, наявність права доступу та виправлення даних. Стаття 12 передбачає право суб'єкта даних вимагати сповіщення третім особам про зміну, знищення чи блокування інформації, що її було сповіщено раніше. А стаття 14 надає особі право заперечувати обробці персональних даних за певних обставин та заборонити використання даних у цілях рекламної діяльності чи ринкових досліджень.

Крім того, Директива встановлює нові правила, які до цього не містилися ні у Конвенції Ради Європи, ні у Керівних принципах ОЕСР. Ідеться про рішення, що їх приймають автоматизовані системи під час оцінки якостей людини на основі аналізу інформації, що стосується цієї людини. Директива надає особам право ознайомитися з логічною формулою, що її використовує така система (стаття 12), і право оскаржити таке рішення (стаття 15).

Встановлена також процедура попереднього контролю, за якою держави мають встановлювати, які обробки здатні становити специфічний ризик для прав осіб, та проводити їх перевірки до початку обробки даних (стаття 20).

Окремі вимоги встановлені щодо "вразливих даних". Стаття 8 містить загальну заборону на обробку даних, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання, членство у профспілках, а також даних стосовно стану здоров'я або статевого життя суб'єкта даних. Виключення з цього правила мають передбачатися на підставі закону у визначених випадках.

Іншим не менш принциповим є положення про заборону передачі даних до третіх країн, що не забезпечують *адекватного* рівня захисту. Цим, зокрема, встановлюється, що для транскордонних потоків даних з країн ЄС, від одержувача даних у третій країні вимагається надання достатніх гарантій щодо дотримання ним вимог Директиви ЄС.

Запропонований підхід піддався критиці Міжнародної Торгової Палати під час законодавчого проходження Директиви, яка відстоювала позицію, що гармонізація міжнародного права у галузі захисту приватності персональних даних повинна, швидше за все, відбуватися на основі моделі Керівних Принципів ОЕСР та Конвенції Ради Європи № 108, ніж на стандартах запропонованих Європейським Союзом.

Незважаючи на лобіювання, відповідне положення залишилося у тексті Директиви, що пояснюється намаганням країн ЄС встановити рівень захисту приватності вищий за стандарти Ради Європи і створити Європейську зону вільного руху інформації. Досягти такої

мети, передбачається завдяки зусиллям, спрямованим на зближення національних законів через імплементацію Директиви у внутрішнє право країн ЄС.

Така імплементація мала відбутися впродовж трирічного строку з дати набуття Директивою чинності, тобто до 24 жовтня 1998 року. Однак не всі країни ЄС впоралися із цим завданням у вказаний термін, що стало приводом для прийняття Робочою групою відповідної рекомендації у лютому 2000 року, в якій зазначається про необхідність негайного виправлення ситуації [26].

З метою галузевого застосування принципів, що їх проголосила Директива 1995 року, Європейський Парламент ухвалив 15 грудня 1997 року Директиву № 97/66/ЕС стосовно обробки персональних даних і захисту приватності у телекомунікаційному секторі [27].

Директива № 97/66/ЕС доповнює і конкретизує положення основної Директиви 1995 року. Положення цієї Директиви зобов'язують країни ЄС забезпечити через національне регулювання приватність інформаційних потоків у сфері публічних телекомунікаційних мереж та публічно доступних телекомунікаційних послуг.

Ці зобов'язання, зокрема, стосуються приватності операційних даних (transactional data), тобто інформації, яка збирається операторами під час надання телекомунікаційних послуг.

Забезпеченню приватності у телекомунікаційному секторі присвячені також рекомендації Робочої групи, ухвалені 23 лютого і 3 травня 1999 року [28], а питанню вдосконалення принципів основної Директиви 1995 року і приведення їх у відповідність до сучасного стану розвитку телекомунікаційних і мультимедійних технологій – висновок Робочої групи від 3 лютого 2000 року [29].

Увага, яку Європейські інституції приділяють цьому питанню, пояснюється важливістю захисту прав людини, і, права на приватність інформаційного обміну, зокрема, для повноцінного користування громадянами ЄС перевагами, що їх надають новітні інформаційні технології, і розвитку інформаційного суспільства в Європі [30].

Той вибір, який зробили країни ЄС впровадив жорсткі вимоги щодо правил поводження з персональними даними, вимагає від інших країн переглядати власні підходи в пошуку компромісу. Однак цей процес ускладнюється тим, що будь-яка поступка з боку Європейських структур з метою досягнення домовленості принципово не можлива, оскільки неминуче призведе до послаблення проголошених стандартів.

Свідченням тому є переговори, які почали вести представники бізнесових кіл США з інституціями ЄС ще до прийняття Директиви, але які до цього часу не привели до вироблення спільної позиції, що задовольнила б обидві сторони [31].

Разом з тим, такий діалог закладає фундамент для подальшої співпраці між державами і організаціями всіх континентів з метою створення універсальних і загальновизнаних міжнародних стандартів.

1. Raymond W. Protection of Privacy. – London.: Sweet & Maxwell, 1980. – P. 1.
2. Brandeis Louis D., Warren Samuel D. The Right To Privacy // Harvard Law Review. – 1890. - P. 193-220.
3. Дженіс М., Кей Р., Бредлі Е. Європейське право у галузі прав людини: джерела і практика застосування: Пер. з англ.- К.: "АртЕк", 1997. - С. 250-251.
4. Prosser William L. Handbook of the Law of Torts. – 3rd ed. – St. Paul; West Publication Corp., 1964. - P. 810-811.
5. Privacy and Human Rights 1998: An International Survey of Privacy Laws and Developments. – EPIC. – 1998. – P. 3.
6. Иванский В.П. Теоретические проблемы правовой защиты частной жизни в связи с использованием информационных технологий: Дис. канд. юрид. наук: 12.00.01. - М., 1998. – С. 12.
7. Серед перших національних актів про захист даних: Закон Землі Гессе ФРГ (1970), Шведський Закон (1973), Закон Землі Райнланд-Фальц ФРГ (1974), Федеральний Акт ФРГ (1977) та деякі інші.
8. Michael J. Privacy and Human Rights. – Paris: UNESCO, 1994. – p. 35.
9. Explanatory Memorandum to the Convention # 108. Доступний на серверу Ради Європи за адресою: //www.coe.fr/dataprotection/edocs.htm
10. Це положення не було включено до Конвенції з прав людини з тих підстав, що будь-яка редакція такого доповнення не змогла б охопити всіх принципів поводження з персональними даними, що їх було закріплено у Конвенції Ради Європи № 108.
11. У секторах охорони здоров'я і статистичних досліджень питання забезпечення приватності під час роботи з даними розглядалося повторно через півтора десятка років. Рекомендації, що стосуються даних у сфері фінансових послуг і поліцейському секторі в цей час проходять ревізію на предмет їх відповідності сучасному рівню розвитку інформаційних технологій у цих секторах. Перелік рекомендацій доступний на серверу Ради Європи за адресою: //www.coe.fr/dataprotection/edocs.htm
12. The introduction and use of personal identification numbers: the data protection issues/ Study prepared by the Committee of experts on data protection (CJ-PD). - Council of Europe. – Strasbourg, 1991.
13. Model contract to ensure equivalent protection in the context of transborder data flows with explanatory report / Study made jointly by the Council of Europe, The Commission of the European Communities and the International Chamber of Commerce. – Council of Europe. – Strasbourg, 1992.

14. У більшості країн ці функції покладаються на уповноваженого з питань захисту даних.
15. 22 липня 1997 року Рада ЄС своїм рішенням уповноважила Комісію ЕС почати процес переговорів з метою приєднання Європейських Співтовариств приєднатися до Конвенції № 108. У листі датованому 22 жовтня 1997 року Генеральний Секретар Європейської Комісії повідомив Генерального Секретаря Ради Європи про таке прагнення Європейських Співтовариств.
16. Explanatory Memorandum to the Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. - OECD. - Paris, 1981. Документ доступний на серверу OECP за адресою: //www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM
17. Declaration on Transborder Data Flows - OECD. - Paris, 1985. Документ доступний на серверу OECP за адресою: //www.oecd.org//dsti/sti/it/secur/prod/e_dflow.htm
18. Recommendation of the Council concerning Guidelines for the Security of Information Systems - OECD. - Paris, 1992. Документ доступний на серверу OECP за адресою: //www.oecd.org//dsti/sti/it/secur/prod/e_secur.htm
19. Guidelines for Cryptography Policy - OECD. - Paris, 1997.
20. OECD Ministerial Declaration on Privacy on Global Networks // I-Ways. - 1998.- 4th Quarter. - P. 48.
21. Kirby M. D. Privacy Protection - A New Beginning // Доповідь на 21-ій Міжнародній конференції з питань приватності і захисту персональних даних. - Гон Конг. - 1999.
22. Council Resolution on a Community policy on data processing // Official Journal. - 1974. - C 086.
23. Commission Recommendation relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data // Official Journal. - 1981. - L 246.
24. Regan Priscilla M. American Business and the European Data Protection Directive: Lobbying Strategies and Tactics // Visions of Privacy: Policy Choices for the Digital Age; Ed. By Colin J. Bennett, Rebecca Grant. – Toronto. - P. 204
25. Див. зноску 24.
26. Recommendation 1/2000 on the Implementation of Directive 95/46/EC adopted on 3rd February 2000. - The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. - Brussels. - 2000.
27. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
28. Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware adopted on 23 February 1999. - The Working Party on the

Protection of Individuals with regard to the Processing of Personal Data. - Brussels. – 1999; Recommendation on the Respect of Privacy in the context of Interception of Telecommunications adopted on 3 May 1999. - The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. - Brussels. - 1999.

29. Opinion 1/2000 on certain data protection aspects of electronic commerce adopted on 3rd February 2000 - Article 29 Data Protection Working Party. - Brussels. – 2000.

30. Про це свідчать, зокрема, положення Резолюції про нові політичні пріоритети стосовно інформаційного суспільства від 21 листопада 1996 року // Official Journal. - 1996. - C 376. - P. 1 - 5; і пропозиція включити право на захист персональних даних до Хартії прав людини Європейського Союзу. Див. Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights adopted on 7 September 1999. - The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. - Brussels. - 1999.

31. Див. Opinions 1/99, 2/99, 4/99 і 3/2000 та інші документи щодо діалогу між Сполученими Штатами і Європейським Союзом стосовно принципів "Safe Harbor" (“Затишна Гавань”).

РОЗДІЛ 2. МІЖНАРОДНІ СТАНДАРТИ

А. Конвенція Ради Європи “Про захист осіб стосовно автоматизованої обробки персональних даних”; Поправки до Конвенції про захист осіб стосовно автоматизованої обробки персональних даних, що дозволяє приєднатися Європейським Співтовариствам.

КОНВЕНЦІЯ
ПРО ЗАХИСТ ОСІБ СТОСОВНО АВТОМАТИЗОВАНОЇ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Страсбург, 28 січня 1981 року
European Treaty Series/108

ПРЕАМБУЛА

Держави-члени Ради Європи, які підписали цю Конвенцію,
враховуючи, що метою Ради Європи є досягнення більшого єднання між її членами, зокрема на основі поважання верховенства права, а також прав і основних свобод людини,
зважаючи на доцільність поширення гарантій прав і основних свобод кожної людини, і зокрема права на повагу до приватності з огляду на зростання транскордонного потоку персональних даних, які піддаються автоматизованій обробці,
підтверджуючи в той же час свою відданість свободі інформації незалежно від кордонів,
визнаючи необхідність узгодження основоположних цінностей поваги до приватності та безперешкодного обміну інформацією між народами,
погодились про таке:

Глава I

Загальні положення

Стаття 1

Предмет і мета

Метою цієї Конвенції є забезпечення на території кожної Сторони для кожної особи незалежно від її національності або помешкання поважання її прав і основних свобод, і зокрема її права на приватність, стосовно автоматизованої обробки персональних даних, що її стосуються (”захист даних”).

Стаття 2

Визначення

Для цілей цієї Конвенції:

a) ”персональні дані” означають будь-яку інформацію, яка стосується ідентифікованої особи або особи, що може бути ідентифікована (”суб’єкт даних”);

b) ”файл даних для автоматизованої обробки” означає будь-який масив даних, що піддаються автоматизованій обробці;

c) ”автоматизована обробка” включає такі операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: зберігання даних, виконання логічних і/або арифметичних операцій з цими даними, зміни, знищення, пошук або поширення даних;

d) ”контролер файлу” означає фізичну чи юридичну особу, державний орган, установу або будь-який інший орган, що має повноваження відповідно до національного права вирішувати щодо цілі файлу даних для автоматизованої обробки, категорій персональних даних, що мають зберігатися, та операцій, які мають здійснюватися з ними.

Стаття 3

Сфера застосування

1. Сторони зобов’язуються застосовувати цю Конвенцію до файлів персональних даних для автоматизованої обробки та до автоматизованої обробки персональних даних у публічному та приватному секторах.

2. Будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або свого документа про прийняття, затвердження чи приєднання або в будь-який інший час після цього може повідомити заявою на ім’я Генерального секретаря Ради Європи про те, що вона:

a) не застосовуватиме цю Конвенцію до автоматизованої обробки певних категорій файлів персональних даних, перелік яких буде зданий на зберігання. Однак у цей перелік вона не включає категорії файлів даних для автоматизованої обробки, які згідно з її національним правом підпадають під дію положень про захист даних. Відповідним чином, вона вносить поправки до цього переліку новою заявою у випадках, коли згідно з її національним правом під дію положень про захист даних підпадають нові категорії автоматизованих файлів персональних даних;

b) застосовуватиме також цю Конвенцію до інформації, яка стосується груп осіб, асоціацій, фундацій, компаній, корпорацій та будь-яких інших установ, що безпосередньо чи опосередковано складаються з окремих осіб, незалежно від того, чи мають такі установи правосуб’єктність юридичної особи, чи ні;

c) застосовуватиме також цю Конвенцію до файлів персональних даних, які не піддаються автоматизованій обробці.

3. Будь-яка держава, що поширила сферу застосування цієї Конвенції будь-якою із заяв, передбачених у підпункті 2b або c вище, може повідомити у згаданій заяві, що таке поширення дії Конвенції стосується лише певних категорій файлів персональних даних, перелік яких буде зданий на зберігання.

4. Будь-яка Сторона, що заявою, передбаченою у підпункті 2a вище, виключила із сфери застосування цієї Конвенції певні категорії файлів персональних даних для автоматизованої обробки, не може вимагати застосування Конвенції до таких категорій Стороною, яка із сфери застосування цієї Конвенції їх не виключила.

5. Відповідним чином, Сторона, яка не поширила сферу застосування Конвенції, як це передбачено у підпунктах 2b і c вище, не може вимагати застосування цієї Конвенції по цих пунктах стосовно Сторони, яка поширила у такий спосіб сферу її застосування.

6. Заяви, передбачені у пункті 2 вище, набирають чинності з моменту набрання чинності Конвенцією стосовно держави, яка їх зробила, якщо такі заяви були зроблені під час підписання або здачі на зберігання її ратифікаційної грамоти або документа про прийняття, затвердження чи приєднання, або через три місяці після їхнього отримання Генеральним секретарем Ради Європи, якщо вони були зроблені в будь-який інший час після цього. Такі заяви можуть бути відкликані повністю або частково шляхом подання відповідного повідомлення на ім'я Генерального секретаря Ради Європи. Відкликання набирає чинності через три місяці від дати отримання такого повідомлення.

Глава II

Основоположні принципи захисту даних

Стаття 4

Обов'язки Сторін

1. Кожна Сторона в межах свого внутрішнього права вживає необхідних заходів з метою запровадження основоположних принципів захисту даних, викладених у цій главі.

2. Такі заходи вживаються не пізніше моменту набрання чинності цією Конвенцією стосовно відповідної Сторони.

Стаття 5

Якість даних

Персональні дані, що піддаються автоматизованій обробці:

a) отримуються та обробляються правомірно та законно;

b) зберігаються для визначених і законних цілей та не використовуються у спосіб несумісний з цими цілями;

c) мають бути адекватними, відповідними і не надмірними з точки зору цілей, заради яких вони зберігаються;

d) мають бути точними та у разі необхідності мають поновлюватися;

e) зберігаються у формі, який дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілі, заради якої такі дані зберігаються.

Стаття 6

Особливі категорії даних

Персональні дані, що свідчать про расову приналежність, політичні погляди або релігійні чи інші переконання, а також персональні дані, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє право не надає відповідних гарантій. Це правило застосовується також до персональних даних, що стосуються кримінальних вчинків.

Стаття 7

Захист даних

Для захисту персональних даних, що зберігаються у файлах даних для автоматизованої обробки, вживаються відповідні заходи захисту, спрямовані на запобігання випадковому чи несанкціонованому знищенню або випадковій втраті, а також на запобігання несанкціонованому доступу, зміні або поширенню.

Стаття 8

Додаткові гарантії для суб'єкта даних

Будь-якій особі має бути надана можливість:

a) встановлювати існування автоматизованих файлів персональних даних, його головні цілі, а також особистість та місце постійного розташування чи місце діяльності контролера файлу;

b) отримувати через розумні проміжки часу та без надмірної затримки або витрат підтвердження або спростування зберігання персональних даних, що її стосуються, в автоматизованому файлі даних, а також отримувати такі дані у зрозумілій формі;

c) вимагати у відповідних випадках виправлення або знищення таких даних, якщо вони оброблялися в порушення положень внутрішнього права, що запроваджують основоположні принципи, визначені у статтях 5 і 6 цієї Конвенції;

d) використовувати засоби правового захисту у разі незадоволення передбаченого у пунктах b і c цієї статті запиту про підтвердження або у відповідних випадках про надання, виправлення або знищення даних.

Стаття 9

Винятки та обмеження

1. Винятки з положень статей 5, 6 і 8 цієї Конвенції дозволяються тільки в межах, визначених цією статтею.

2. Відступ від положень статей 5, 6 і 8 цієї Конвенції дозволяється у випадках, коли такий відступ передбачається законодавством Сторони та є у демократичному суспільстві необхідним заходом, спрямованим на:

a) захист державної безпеки та громадського спокою, грошових інтересів держави або на боротьбу із кримінальними злочинами;

b) захист суб'єкта даних або прав і свобод інших осіб.

3. Обмеження на здійснення прав, визначених у пунктах b, c і d статті 8, можуть запроваджуватися законодавством стосовно файлів персональних даних для автоматизованої обробки, що використовуються для цілей статистики або наукових досліджень, у випадках явної відсутності небезпеки порушення приватності суб'єктів даних.

Стаття 10

Санкції та засоби правового захисту

Кожна Сторона зобов'язується передбачити відповідні санкції та засоби правового захисту від порушень положень внутрішнього права, що запроваджують основоположні принципи захисту даних, визначені у цій главі.

Стаття 11

Розширення захисту

Жодне з положень цієї глави не повинно тлумачитися як таке, що обмежує або іншим чином заважає можливості Сторони забезпечувати суб'єктам даних ступінь захисту більш високий, ніж той, що передбачається цією Конвенцією.

Глава III

Транскордонні потоки даних

Стаття 12

Транскордонні потоки персональних даних та внутрішнє право

1. Стосовно передачі через національні кордони за допомогою будь-яких засобів автоматизованих персональних даних або що зібрані з метою їхньої автоматизованої обробки, застосовуються такі положення.

2. Сторона не може лише з метою захисту приватності забороняти або зумовлювати спеціальними дозволами транскордонні потоки персональних даних, що передаються на територію іншої Сторони.

3. Однак кожна Сторона має право відступати від положень пункту 2:

a) якщо її законодавство містить спеціальні положення для деяких категорій персональних даних або автоматизованих файлів персональних даних, у зв'язку із характером цих даних або цих файлів, за винятком випадків, коли положення іншої Сторони забезпечують еквівалентний захист;

b) якщо передача даних здійснюється з її території на територію держави, що не є Договірною, через територію іншої Сторони, для запобігання порушенню такою передачею законодавства Сторони, згаданої на початку цього пункту.

Глава IV

Взаємна допомога

Стаття 13

Співробітництво між Сторонами

1. Сторони погоджуються надавати одна одній взаємну допомогу з метою імплементації цієї Конвенції.

2. Для цього:

a) кожна Сторона призначає один або більше органів, назву та адресу яких вона повідомляє Генеральному секретарю Ради Європи;

b) кожна Сторона, яка призначила більше одного органу зазначає у своєму повідомленні, згаданому в попередньому підпункті, сферу повноважень кожного з них.

3. Орган, призначений Стороною, на запит органу, призначеного іншою Стороною:

a) надає інформацію про свої законодавство та адміністративну практику у галузі захисту даних;

b) у відповідності до свого внутрішнього права та з метою виключно захисту приватності вживає всіх відповідних заходів для надання достовірної інформації, що стосується конкретної автоматизованої обробки, яка здійснюється на його території, за винятком однак персональних даних, що обробляються.

Стаття 14

Допомога суб'єктам даних, що мешкають за кордоном

1. Кожна Сторона надає допомогу будь-якій особі, що мешкає за кордоном, у здійсненні прав, наданих її внутрішнім законодавством, що запроваджує принципи, визначені у статті 8 цієї Конвенції.

2. Якщо така особа мешкає на території іншої Сторони, їй надається можливість подати свій запит через посередництво органу, призначеного цією Стороною.

3. Запит про надання допомоги має містити всі необхідні відомості, що стосуються, крім іншого:

a) прізвища, адреси та будь-яких інших відповідних відомостей, які ідентифікують особу, що звертається із запитом;

b) автоматизований файлу персональних даних, якого стосується запит, або його контролера;

c) цілі запиту.

Стаття 15

Гарантії стосовно допомоги, що надається призначеними органами

1. Орган, призначений Стороною, який отримав від органу, призначеного іншою Стороною, інформацію що супроводжує запит про надання допомоги або у відповідь на його власний запит про надання допомоги, використовує цю інформацію тільки для цілей, зазначених у запиті про надання допомоги.

2. Кожна Сторона забезпечує, щоб особи, які працюють у призначеному органі або діють від його імені, мали відповідні зобов'язання щодо збереження таємності або конфіденційності такої інформації.

3. Призначеному органу на свій власний розсуд і без ясно вираженої згоди суб'єкта даних, що проживає за кордоном, у жодному випадку не дозволяється звертатися згідно з пунктом 2 статті 14 із запитом про надання допомоги від імені заінтересованої особи.

Стаття 16

Відхилення запитів про надання допомоги

Призначений орган, якому адресується запит про надання допомоги згідно зі статтею 13 або 14 цієї Конвенції, може відмовитися задовольняти такий запит, якщо:

a) запит є несумісним із повноваженнями, якими наділені у галузі захисту даних органи, що відповідають за виконання прохання;

b) запит не відповідає положенням цієї Конвенції;

c) задоволення запиту може порушити суверенітет, безпеку або громадський порядок Сторони, якою він був призначений, або права та основні свободи осіб, що знаходяться під юрисдикцією цієї Сторони.

Стаття 17

Витрати на допомогу та порядок її надання

1. Взаємна допомога, яку Сторони надають одна одній згідно зі статтею 13, та допомога, яку вони надають згідно зі статтею 14 суб'єктам даних, що мешкають за кордоном, не може бути підставою для сплати жодних витрат або зборів, за винятком тих, що сплачуються на експертів і усних перекладачів. Витрати або збори на експертів і усних перекладачів сплачуються Стороною, яка призначила орган, що звертається із запитом про надання допомоги.

2. На суб'єкта даних не може покладатися сплата витрат або зборів, пов'язаних із заходами, що були вжиті від його імені на території іншої Сторони, крім витрат або зборів, які на законних підставах сплачуються резидентами цієї Сторони.

3. Інші подробиці надання допомоги, що стосуються, зокрема, форм і процедур, а також використання мов, визначаються безпосередньо відповідними Сторонами.

Глава V

Консультативний комітет

Стаття 18

Склад Комітету

1. Після набрання чинності цією Конвенцією створюється Консультативний комітет.

2. Кожна Сторона призначає в Комітет одного представника та заступника представника. Будь-яка держава-член Ради Європи, яка не є Стороною Конвенції, має право бути представленою в Комітеті спостерігачем.

3. Консультативний комітет одностайним рішенням може запропонувати будь-якій державі, що не є членом Ради Європи і не бере участі в Конвенції, бути представленою на тому чи іншому засіданні спостерігачем.

Стаття 19

Функції Комітету

Консультативний Комітет:

a) може вносити пропозиції з метою сприяння або поліпшення застосування Конвенції;

b) може вносити пропозиції про внесення поправок до цієї Конвенції у відповідності до статті 21;

c) надає свій висновок щодо будь-якої пропозиції про внесення поправок до цієї Конвенції, яка передається йому на розгляд у відповідності до пункту 3 статті 21;

d) може на прохання Сторони робити висновок з будь-якого питання, що стосується застосування цієї Конвенції.

Стаття 20

Процедура

1. Консультативний Комітет скликається Генеральним секретарем Ради Європи. Його перше засідання буде проведено упродовж дванадцяти місяців після набрання цією Конвенцією чинності. В подальшому він збирається якнайменш один раз на два роки і у будь-якому випадку, коли одна третина представників Сторін вимагає його скликання.

2. Більшість представників Сторін становитиме Кворум засідання Консультативного Комітету.

3. Після кожного свого засідання Консультативний Комітет подає Комітету Міністрів Ради Європи доповідь про свою роботу та про стан функціонування Конвенції.

4. З урахуванням положень цієї Конвенції Консультативний Комітет розробляє власні Правила Процедури.

Глава VI

Поправки

Стаття 21

Поправки

1. Поправки до цієї Конвенції можуть пропонуватися будь-якою Стороною, Комітетом Міністрів Ради Європи чи Консультативним Комітетом.

2. Будь-яка пропозиція про внесення поправки надсилається Генеральним секретарем Ради Європи державам-членам Ради Європи та кожній державі, що не є членом Ради, яка приєдналася до цієї Конвенції або якій було запропоновано приєднатися до неї у відповідності до положень статті 23.

3. Крім того, будь-яка поправка, запропонована Стороною або Комітетом Міністрів, надсилається Консультативному Комітету, який подає Комітету Міністрів свій висновок щодо цієї запропонованої поправки.

4. Комітет Міністрів розглядає запропоновану поправку та будь-який висновок, поданий Консультативним Комітетом, і може затвердити поправку.

5. Текст будь-якої поправки, затверджений Комітетом Міністрів у відповідності до пункту 4 цієї статті, надсилається Сторонам для прийняття.

6. Будь-яка поправка, затверджена у відповідності до пункту 4 цієї статті, набирає чинності на тридцятий день після того, як усі Сторони поінформували Генерального секретаря про її прийняття.

Глава VII

Кінцеві положення

Стаття 22

Набрання чинності

1. Цю Конвенцію відкрито для підписання державами-членами Ради Європи. Вона підлягає ратифікації, прийняттю або затвердженню. Ратифікаційні грамоти або документи про прийняття чи затвердження здаються на зберігання Генеральному секретарю Ради Європи.

2. Ця Конвенція набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати, на яку п’ять держав-членів Ради Європи висловили свою згоду на обов’язковість для них цієї Конвенції у відповідності до положень попереднього пункту.

3. Стосовно будь-якої держави-члена, яка висловлюватиме свою згоду на обов’язковість для неї цієї Конвенції після набрання нею чинності, Конвенція набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання ратифікаційної грамоти або документа про прийняття чи затвердження.

Стаття 23

Приєднання держав, що не є членами Ради

1. Після набрання цією Конвенцією чинності Комітет Міністрів Ради Європи може запропонувати будь-якій державі, яка не є членом Ради, приєднатися до цієї Конвенції у рішенні, що приймається більшістю голосів, передбаченою у статті 20d Статуту Ради Європи, і одностайним голосуванням представників Договірних Держав, які мають право засідати в Комітеті.

2. Стосовно будь-якої держави, що приєдналася до цієї Конвенції, Конвенція набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання документа про приєднання Генеральному секретарю Ради Європи.

Стаття 24

Територіальне застосування

1. Будь-яка держава під час підписання або здачі на зберігання своєї ратифікаційної грамоти або свого документа про прийняття, затвердження чи приєднання може визначити територію (території), до якої застосовуватиметься ця Конвенція.

2. Будь-яка Держава може в будь-який інший час після цього заявою на ім'я Генерального секретаря Ради Європи поширити дію цієї Конвенції на будь-яку іншу територію, визначену

в цій заяві. Щодо такої території Конвенція набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати отримання такої заяви Генеральним секретарем.

3. Будь-яка заява, зроблена відповідно до двох попередніх пунктів, може стосовно будь-якої території, визначеної в цій заяві, бути відкликана шляхом подання відповідного повідомлення на ім'я Генерального секретаря. Відкликання набирає чинності в перший день місяця, що настає після закінчення шестимісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 25

Застереження

Жодне застереження до положень цієї Конвенції не дозволяється.

Стаття 26

Денонсація

1. Будь-яка Сторона може в будь-який час денонсувати цю Конвенцію шляхом подання відповідного повідомлення на ім'я Генерального секретаря Ради Європи.

2. Така денонсація набирає чинності в перший день місяця, що настає після закінчення шестимісячного періоду від дати отримання такого повідомлення Генеральним секретарем.

Стаття 27

Повідомлення

Генеральний секретар Ради Європи повідомляє держави-члени Ради Європи та будь-яку державу, що приєдналася до цієї Конвенції, про:

a) будь-яке підписання;

b) здачу на зберігання будь-якої ратифікаційної грамоти або будь-якого документа про прийняття, затвердження чи приєднання;

c) будь-яку дату набрання чинності цією Конвенцією відповідно до статей 22, 23 та 24;

d) будь-яку іншу дію, будь-яке повідомлення або сповіщення, які стосуються цієї Конвенції.

На посвідчення чого нижчепідписані належним чином на те уповноважені представники підписали цю Конвенцію.

Вчинено у Страсбурзі двадцять восьмого дня січня місяця 1981 року англійською та французькою мовами, причому обидва тексти є однаково автентичними, в одному примірнику, який зберігатиметься в архіві Ради Європи. Генеральний секретар Ради Європи надсилає засвідчені копії цієї Конвенції кожній державі-члену Ради Європи та будь-якій державі, якій було запропоновано приєднатися до цієї Конвенції.

ПОПРАВКИ

до Конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру,

що дозволяє приєднатися Європейським Співтовариствам

(ухвалені Комітетом Міністрів у Стразбурзі 15 червня 1999)

Стаття 1

Пункти 2,3 та 6 Статті 3 цієї Конвенції читаємо так:

2. Будь-яка держава або Європейські Співтовариства під час підписання або здачі на зберігання своїх ратифікаційних грамот або своїх документів про прийняття, затвердження чи приєднання або в будь-який інший час після цього можуть повідомити заявою на ім'я Генерального секретаря Ради Європи про те, що вони:

a) не застосовуватимуть цю Конвенцію до певних категорій файлів даних особистого характеру для автоматизованої обробки, перелік яких буде зданий на зберігання. Однак у цей перелік вони не включають категорій автоматизованих файлів даних, які згідно з їх внутрішнім правом підпадають під дію положень про захист даних. Відповідним чином, вони вносять поправки до цього переліку новою заявою у випадках, коли згідно з їх внутрішнім правом під дію положень про захист даних підпадають нові категорії файлів даних особистого характеру для автоматизованої обробки;

b) застосовуватимуть також цю Конвенцію до інформації, яка стосується груп осіб, асоціацій, фундацій, компаній, корпорацій та будь-яких інших установ, що безпосередньо чи опосередковано складаються з окремих осіб, незалежно від того, чи мають такі установи правосуб'єктність юридичної особи, чи ні;

c) застосовуватимуть також цю Конвенцію до файлів персональних даних, які не піддаються автоматизованій обробці.

3. Будь-яка держава або Європейські співтовариства, що поширили сферу застосування цієї Конвенції будь-якою із заяв, передбачених у підпункті 2 в або e) вище, можуть повідомити у згаданій заяві, що таке поширення дії Конвенції стосується лише певних категорій файлів даних особистого характеру, перелік яких буде зданий на зберігання.

6. Заяви, передбачені у пункті 2 вище набирають чинності з моменту набрання чинності Конвенцією стосовно держави чи Європейських Співтовариств, які їх зробили, якщо такі заяви були зроблені під час підписання або здачі на зберігання їх ратифікаційних грамот або документа про прийняття, затвердження чи приєднання, або через три місяці після їхнього отримання Генеральним секретарем Ради Європи, якщо вони були зроблені в будь-який інший час після цього. Такі заяви можуть бути відкликані повністю або частково шляхом подання відповідного повідомлення на ім'я Генерального секретаря Ради Європи. Відкликання набирають чинності через три місяці від дати отримання такого повідомлення.

Стаття 2.

1. Новий пункт 3, у редакції наведеній нижче, вставляється в Статтю 20 цієї Конвенції: "Кожна Сторона має право голосувати. Кожна Держава, яка є Стороною для Конвенції, має один голос. Стосовно питань щодо повноважень, Європейські Співтовариства здійснюватимуть своє право голосувати і отримують кількість голосів, що дорівнює числу Держав-членів, які є Сторонами цієї Конвенції і передали свої повноваження Європейським Співтовариствам у цій сфері. В такому разі ці Держави-члени Співтовариства не голосують, а інші Держави-члени можуть це робити. Європейські Співтовариства не голосують, коли розглядаються питання, які не входять до сфери їх повноважень.

2. Пункти 3 та 4 Статті 20 цієї Конвенції перейменовуються на пункти 4 і 5 цієї ж статті відповідно.

Стаття 3

Статтю 21, пункт 2 цієї Конвенції читаємо так:

"Будь-яка пропозиція про внесення поправки надсилається Генеральним секретарем Ради Європи Державам-членам Ради Європи, Європейським Співтовариствам та кожній державі, що не є членом Ради, яка приєдналася до цієї Конвенції або якій було запропоновано приєднатися до неї у відповідності до положень Статті 23".

Стаття 4

Статтю 23 цієї Конвенції читаємо так:

"Стаття 23 - Приєднання держав, що не є членами, або Європейських Співавторств

1. Після набрання цією Конвенцією чинності Комітет міністрів Ради Європи може запропонувати будь-якій державі, яка не є членом Ради Європи, приєднатися до цієї Конвенції у рішенні, що приймається більшістю голосів, передбаченою у статті 20 d Статуту Ради Європи та одностайним голосуванням представників Договірних Держав, які мають право засідати в Комітеті.

2. Європейські Співтовариства можуть приєднатися до цієї Конвенції.

3. Стосовно будь-якої держави, що приєдналася до цієї Конвенції, чи Європейських Співтовариств, що можуть приєднатися, Конвенція набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі на зберігання документа про приєднання Генеральному секретарю Ради Європи".

Стаття 5

Статтю 24 цієї Конвенції читаємо так:

"Стаття 24 - Територіальне застосування

1. Будь-яка держава або Європейські Співтовариства під час підписання або здачі на зберігання своїх ратифікаційних грамот або своїх документів про прийняття, затвердження чи приєднання можуть визначити територію чи території, до яких застосовуватиметься ця Конвенція.

2. Будь-яка держава чи Європейські Співтовариства можуть в будь-який інший час після цього заявою на ім’я Генерального секретаря Ради Європи поширити дію цієї Конвенції на будь-яку іншу територію, визначену в цій заяві. Щодо такої території Конвенція набирає чинності в перший день місяця, що настає після закінчення тримісячного періоду від дати отримання такої заяви Генеральним секретарем."

Стаття 6

Статтю 27 цієї Конвенції читаємо так:

"Стаття 27 - Повідомлення

Генеральний секретар Ради Європи повідомляє Держави-члени Ради Європи, Європейські Співтовариства та будь-яку державу, що приєдналася до цієї Конвенції, про:

а) будь-яке підписання;

б) здачу на зберігання ратифікаційної грамоти або будь-якого документа про прийняття, затвердження чи приєднання;

в)будь-яку дату набрання чинності цією Конвенцією відповідно до статей 22, 23 та 24;

г) будь-яку іншу дію, будь-яке повідомлення або сповіщення, які стосуються цієї Конвенції"

В. Організація Економічної Співпраці і Розвитку: Рекомендація стосовно Керівних принципів, що регулюють захист приватності і транскордонні потоки персональних даних.

Рекомендація Ради стосовно Керівних принципів,
що регулюють захист приватності і транскордонні потоки персональних даних

Рада,

враховуючи статті 1(c), 3 (a) та 5(b) Конвенції про Організацію Економічного Співробітництва та Розвитку від 14 грудня 1960 р.,

визначаючи, що

незважаючи на відмінності у внутрішніх законодавствах і політиці, держави-члени мають спільний інтерес у захисті приватності та індивідуальних свобод особи, а також в узгодженні таких конкуруючих основоположних цінностей, як приватність та вільний потік інформації;

автоматизована обробка і транскордонні потоки персональних даних породжують нові форми відносин між країнами і вимагають вироблення відповідних правил і практики;

транскордонні потоки персональних даних сприяють економічному й соціальному розвитку;

внутрішнє законодавство з захисту приватності стосовно транскордонних потоків персональних даних може перешкоджати таким транскордонним потокам,

Визначивши за необхідне покращити вільні потоки інформації між державами-членами та уникнути створення невиправданих перешкод на шляху розвитку економічних і соціальних відносин між державами-членами;

Р е к о м е н д у є

1. Держави-члени враховують в їх внутрішніх законодавствах принципи захисту приватності та особистих свобод, які знайшли свій розвиток в "Керівних принципах" і містяться в Додатку до цих Рекомендацій, що становлять їх органічну частину.
2. Для захисту приватності держави-члени мають намір усунути або запобігати створенню несанкціонованих перешкод транскордонним потокам персональних даних.
3. Держави-члени співробітничають щодо втілення в життя "Керівних принципів", викладених у Додатку.
4. Держави-члени якомога швидше узгоджують процедури консультування та співробітництва стосовно застосування цих "Керівних принципів".

Додаток до рекомендації Ради від 23 вересня 1980 р.

Частина I. Загальні положення

Визначення

1. В "Керівних принципах" приймаються такі визначення:

а) "контролер даних" - сторона, яка згідно з внутрішнім законодавством має повноваження вирішувати питання щодо змісту та використання персональних даних безвідносно до того, чи такі дані збираються, зберігаються, обробляються чи повідомляються нею самою, чи агентом від її імені;

б) "дані особистого характеру" - будь-яка інформація, що стосується визначеної особи чи такої, що може бути встановлена (суб'єкта даних);

в) "транскордонні потоки персональних даних" - рух персональних даних через національні кордони.

Сфера застосування "Керівних принципів"

2. Ці "Керівні принципи" застосовуються до персональних даних як у публічному, так і приватному секторах, які через спосіб їх обробки, саму сутність чи контекст, в якому вони використовуються, містять загрозу приватності та індивідуальним свободам.

3. "Керівні принципи" не повинні тлумачитися у такий спосіб, що виключає:

а) застосування до різних категорій персональних даних, інших захисних заходів, обумовлених їх сутністю та умовами, в яких вони збираються, зберігаються, обробляються та поширюються;

б) вилучення із сфери застосування "Керівних принципів" персональних даних, які явно не містять загрози приватності чи індивідуальним свободам особи;

в) застосування "Керівних принципів" лише до автоматизованої обробки персональних даних.

4. Винятки до принципів, що містяться у частині 2, частині 3 "Керівних принципів", включаючи ті, що стосуються державного суверенітету, національної безпеки та громадського порядку, повинні бути:

а) мінімальні за числом, наскільки це є можливим;

б) доведені до відома громадськості.

5. У державах з федеративним устроєм нагляд за дотриманням "Керівних принципів" може здійснюватися відповідно до розподілу владних повноважень федерації.

6. Ці "Керівні принципи" мають розглядатися як мінімальні стандарти, що можуть доповнюватися додатковими заходами щодо захисту приватності та індивідуальних свобод особи.

Частина 2. Основні принципи національного застосування

Принцип обмеження збирання

7. Повинні існувати обмеження щодо збирання персональних даних; будь-які дані мають збиратися законно і чесно, а де вимагається, - з інформуванням про це суб'єкта даних чи за його згоди.

Принцип якості даних

8. Персональні дані повинні бути достатніми, але не надмірними з точки зору цілей, заради яких вони використовуватимуться, точними, повними та поновленими.

Принцип визначення цілі

9. Цілі, заради яких збираються дані, повинні визначатися не пізніше часу збирання даних; подальше використання повинне здійснюватися у межах цих цілей або інших, що не є несумісними з цими цілями і окреслені в кожному конкретному випадку зміни цілі.

Принцип обмеження використання

10. Дані особистого характеру не повинні розкриватися, бути доступними або використаними в інших цілях, окрім тих, що визначаються у відповідності до пункту 9, за винятком:

а) коли на це є згода суб'єкта даних або

б) коли це є правомірним за законом.

Принцип гарантій безпеки

11. Персональні дані повинні бути захищені розумними гарантіями безпеки від ризиків втрати чи несанкціонованого доступу, руйнування, використання, зміни чи відкриття.

Принцип гласності

12. Повинна бути поширеною практика відкритості щодо розвитку регулювання, практики та засад обробки персональних даних. Повинна забезпечуватись можливість з'ясування факту існування персональних даних, їх природи, основних цілей використання, а також особистості та звичайного місцезнаходження контролера даних.

Принцип індивідуальної участі

13. Особа повинна мати право:

а) отримати від контролера даних чи інших осіб підтвердження факту наявності чи відсутності у нього даних, що її стосуються;

б) отримати дані, що її стосуються:

- в межах розумного часу;
- без надмірних витрат;
- у розумний спосіб;
- у доступній для розуміння формі;

в) на отримання роз'яснень щодо причин відхилення запиту, зробленого згідно з підпунктами а), б), та можливості оскаржувати це відхилення; та

г) оскаржувати дані, що стосуються її; якщо оскарження задовольняється, знищувати, виправляти, доповнювати або поновлювати дані.

Принцип відповідальності

14. Контролер даних повинен нести відповідальність за дотримання заходів, що забезпечують втілення вищезазначених принципів.

Частина 3. Основні принципи міжнародного застосування: вільний потік і законні обмеження.

15. Держави-члени повинні враховувати застосування внутрішньої обробки та реекспорту персональних даних до інших держав-членів.

16. Держави-члени повинні вжити всіх розумних і відповідних заходів для забезпечення безперешкодності й безпечності транскордонних потоків персональних даних, включаючи транзит через територію держави-члена ОЕСР.

17. Держава-член має утримуватися від обмежень транскордонного обміну персональними даними з іншою державою-членом, окрім випадків, коли остання ще не достатньою мірою дотримується цих "Керівних принципів" або коли реекспорт таких даних порушує її внутрішнє законодавство з приватності. Держава-член може також наполягати на обмеженнях стосовно певних категорій персональних даних, для яких її внутрішнє законодавство з приватності має конкретні приписи з урахуванням характеру цих даних, але для яких інша держава-член не передбачає еквівалентного захисту.

18. Держави-члени мають уникати змін в законодавстві, політиці й практиці з метою захисту приватності та свобод особи, які можуть створювати перешкоди транскордонному потоку персональних даних, але такою мірою, що не виходить за потребу захисту.

Частина 4. Національне застосування

19. Під час імплементації принципів, викладених вище у Частині 2 та Частині 3, держави-члени встановлюють законодавчі, адміністративні або інші процедури або інституції для захисту права на приватність та індивідуальних свобод стосовно персональних даних. Держави-члени мають намагатися:

а) прийняти відповідне внутрішнє законодавство;

б) заохочувати й підтримувати саморегуляцію чи то у вигляді кодексів поведінки, чи в інший спосіб;

в) передбачати розумні заходи для забезпечення особам можливості реалізації їх прав;

г) передбачати адекватні санкції та засоби правового захисту у випадках недотримання заходів з втілення принципів, викладених у Частині 2 та Частині 3, і

д) передбачити недопущення дискримінації по відношенню до суб’єктів даних.

Частина П’ята. Міжнародне співробітництво

20. Держави-члени на запит повідомляють іншим державам-членам деталі щодо дотримання принципів, викладених вище у цих "Керівних принципах". Держави-члени повинні також забезпечувати, щоб процедури транскордонної передачі персональних даних і забезпечення приватності і особистих свобод були простими й узгоджувалися з процедурами іншої

держави-члена та відповідали цим "Керівним принципам".

21. Держави-члени встановлюють процедури для влаштування:

- обміну інформацією, що стосується цих "Керівних принципів" і
- взаємної допомоги у питаннях процедури та розслідування, що задіяні.

22. Держави-члени співпрацюють у напрямку розвитку принципів, внутрішніх та міжнародних, для вироблення прийнятного законодавства, що стосується транскордонних потоків персональних даних.

С. Директива 95/46 СЕ Європейського парламенту і Ради від 24 жовтня 1995 року

"Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних"

Директива 95/46 СЕ Європейського парламенту і Ради від 24 жовтня 1995 року.
"Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних"
Європейський парламент і Рада Європейського Союзу,
враховуючи Договір про заснування Європейського Співтовариства, зокрема його статтю 100a,
враховуючи пропозиції Комісії [1],
враховуючи висновки Економічного і Соціального Комітету [2],
діючи у відповідності з процедурою, передбаченою ст. 189 (в) Договору [3], вважають, що:
1) цілі Співтовариства, визначені в Договорі з урахуванням змін внаслідок Договору про Європейський Союз, полягають у досягненні більшої єдності між народами Європи, встановленні тісних взаємин між державами, що належать до Співтовариства, забезпеченні економічного і соціального прогресу спільними діями, скерованими на подолання перешкод, що розділяють Європу, сприянні постійному покращенню умов життя своїх народів, збереженню і зміцненню миру та свободи, розвитку демократії на основі дотримання не-від'ємних прав, визнаних конституціями та законодавствами Держав - членів та Європейською Конвенцією про захист прав людини та основних свобод;
2) системи обробки даних покликані служити людині незалежно від національності чи місця проживання фізичної особи, поважати основоположні права і свободи, зокрема право на приватність, і сприяти економічному та соціальному прогресу, розширенню торгівлі та піднесенню добробуту людей;
3) запровадження й функціонування спільного внутрішнього ринку, в якому згідно зі статтею 7a Договору забезпечується вільний рух товарів, людей, послуг і капіталу, вимагає не лише безперешкодного потоку персональних даних з однієї Держави-члена в іншу, але й гарантії захисту основних прав особи;
4) у Співтоваристві все більше використовується обробка персональних даних в різних сферах економічної та соціальної діяльності; прогрес інформативних технологій значно полегшує обробку та обмін такими даними;
5) економічна й соціальна інтеграція, яка є наслідком запровадження й функціонування спільного ринку відповідно до Статті 7(a) Договору, обов'язково приведе до зростання потоків персональних даних через кордони між всіма тими, хто задіяний у приватній чи публічній ролях в економічну і соціальну активність в Державах-членах; обмін

персональними даними між підприємцями в різних Країнах-членах має тенденцію до зростання; державні органи влади в різних Країнах - членах закликані через застосування законодавства Співтовариства до співпраці і взаємного обміну персональними даними для виконання своїх обов'язків та здійснення завдань за дорученням органів влади Держави-члена в межах простору без внутрішніх кордонів, встановленого спільним ринком;

6) зміцнення науково-технічного співробітництва, а також координоване впровадження нових телекомунікаційних мереж у Співтоваристві вимагають передачі персональних даних через кордони і полегшують їх;

7) відмінності у рівнях захисту прав і свобод людини, особливо права на приватність, зокрема, стосовно обробки персональних даних, гарантованих у Країнах-членах, можуть зашкодити переміщенню таких даних з території однієї Країни-члена до території іншої Держави-члена; ця відмінність може, таким чином, створювати перешкоди для здійснення низки видів економічної діяльності на рівні Співтовариства, порушити конкуренцію і завадити органам влади виконувати свої обов'язки, покладені на неї законодавством Співтовариства; різниця в рівнях захисту обумовлена наявністю розбіжностей в національних законодавствах, регулятивних та адміністративних положеннях;

8) для усунення перешкод в обігу персональних даних рівень захисту прав і свобод осіб стосовно обробки таких даних має бути еквівалентним в усіх Державах-членах; ця мета є нагальною для спільного ринку, але не може бути досягнута лише зусиллями Держав-членів з огляду на обсяг розбіжностей, які існують у чинних законодавствах Держав-членів і потребують координації законодавств Держав-членів, з тим щоб забезпечити регулювання потоку персональних даних через кордони в узгодженій формі, тобто, відповідно з цілями спільного ринку, що передбачено статтею 7(а) Договору; через це необхідне втручання Співтовариства з метою врегулювання законодавств;

9) забезпечивши еквівалентний захист, що стає можливим внаслідок зближення національних законодавств, Держави-члени вже не зможуть стримувати безперешкодний обмін персональними даними з причин, пов'язаних із захистом прав і свобод фізичних осіб, зокрема права на приватність; Держави-члени матимуть простір для маневру, яким зможуть відповідно до Директиви користуватися економічні й соціальні партнери; Держави-члени зможуть, таким чином, уточнити в своєму національному законодавстві загальні умови забезпечення законності у справі обробки даних; діючи так, Держави-члени намагатимуться поліпшити захист, що зараз надається їх законодавством; в межах зазначеного простору для маневру і згідно з законодавством Співтовариства, можуть виникати невідповідності в застосуванні цієї Директиви, що може позначитись на обміні даними всередині Держав-членів та в межах Співтовариства;

10) ціль національних законодавств стосовно обробки персональних даних полягає в захисті основоположних прав та свобод, зокрема права на приватність, що визнається як статтею 8

Європейської конвенції про захист прав людини та основних свобод, так і загальними принципами законодавства Співтовариства; з цієї причини зближення цих законодавств не повинно спричинятися до зниження захисту, який воно гарантує, а, навпаки, повинне мати на меті забезпечення високого рівня захисту в Співтоваристві;

11) принципи захисту прав і свобод осіб, зокрема права на приватність, що містяться в цій Директиві, уточнюють і розширюють принципи Конвенції Ради Європи від 28 січня 1981 року "Про захист осіб стосовно автоматичної обробки персональних даних";

12) принципи захисту повинні застосовуватися при всіх обробках персональних даних будь-якою особою, чия діяльність визначається законодавством Співтовариства; за виключенням обробки даних, виконуваної будь-якою фізичною особою при провадженні діяльності, що є виключно особистою чи сімейною, наприклад, листування чи ведення записів адрес;

13) види діяльності, передбачені в розділах V і VI Договору про Європейський Союз, що стосуються громадської безпеки, оборони або діяльності держави в сфері кримінального законодавства, не включаються до сфери застосування законодавства Співтовариства без впливу на зобов’язання, що накладаються на Держави-члени згідно з положенням 2 статті 56 і статтями 57 та 100 (A) Договору, що засновує Європейське Співтовариство; обробка персональних даних, необхідна в інтересах забезпечення економічного добробуту держави, не виключається із сфери застосування цієї Директиви, якщо така обробка не торкається справ державної безпеки;

14) враховуючи значення, яке для інформаційного суспільства має сучасний розвиток техніки для отримання, передачі, управління, реєстрації, збереження або повідомлення звукових чи зображуваних даних, що стосується фізичних осіб, ця Директива має застосовуватися до обробок, в яких задіяні ці дані;

15) обробка таких даних допускається цією Директивою, якщо вона автоматизована або якщо дані містяться або міститимуться у файловій системі, побудованої відповідно до критеріїв, що стосуються суб’єктів даних, з метою забезпечення зручного доступу до відповідних персональних даних;

16) обробка звукових та зображуваних даних, таких як під час стеження з допомогою відеокамери, не включається до сфери цієї Директиви, якщо вона виконується в цілях громадської безпеки, оборони, національної безпеки або пов’язана з діяльністю держави у сфері кримінального права чи належить до тих видів діяльності, на які не поширюється застосування права Співтовариства;

17) якщо обробка звукових та зображуваних даних виконується в журналістських цілях, а також в цілях літературного чи мистецького відображення, зокрема в аудіовізуальному секторі, принципи цієї Директиви повинні застосовуватися в обмеженому вигляді відповідно до положень, викладених у статті 9;

18) для забезпечення того, щоб особи не були позбавлені захисту, передбаченого цією

Директивою, будь-яка обробка персональних даних у Співтоваристві має виконуватись згідно з законодавством однієї з Держав членів; у зв'язку з цим обробка, що здійснюється під відповідальність контролера, що є заснований в Державі-члені, виконується згідно з правом цієї ж Держави;

19) заснування підприємства на території якої-небудь Держави-члена означає ефективне й реальне здійснення нею діяльності, якщо норми, що регулюють цю діяльність, будуть постійними; юридична форма цього закладу, будь то просто філія чи філія-підприємство з ознаками юридичної особи, не має значення в цьому відношенні; якщо єдиний контролер є заснований на території кількох Держав-членів, причому через підприємство-філію, він має забезпечити виконання кожним із своїх підрозділів зобов'язань, покладених на них національним законодавством, щоб уникнути порушень національних стандартів;

20) той факт, що обробка даних здійснюється особою заснованою у третій країні не повинен становити перешкоди для захисту осіб, що мають цей захист згідно з цією Директивою; у цих випадках обробка даних має здійснюватися згідно з законодавством Держави-члена, в якій зосереджені використовувані засоби, але тут мають бути гарантії для забезпечення дотримання прав і зобов'язань, що передбачені цією Директивою на практиці;

21) ця Директива не впливає на правила територіальної юрисдикції, що застосовуються в кримінальних справах;

22) Держави-члени мають точніше визначати в їх праві або при застосуванні розпоряджень згідно з цією Директивою загальні умови, за яких обробка даних є законною; зокрема, положення статті 5 у поєднані із статтями 7 і 8, дозволяють Державам-членам, незалежно від загальних правил, забезпечувати особливі умови обробки для специфічних сфер та різних категорій даних, передбачених статтею 8;

23) Держави-члени мають право забезпечувати захист осіб як засобами загального права про захист осіб стосовно обробки персональних даних, так і галузевим законодавством, що стосується, наприклад, питань статистики;

24) ця Директива не стосується законодавства про захист юридичних осіб стосовно обробки даних про них;

25) принципи захисту повинні відображатися, з одного боку, в різних зобов'язаннях, покладених на осіб, державні органи, підприємства, агенції або інші органи, відповідальних за обробку, зокрема за якість даних, технічний захист, повідомлення до контрольних органів, обставини, за яких можна здійснювати обробку даних; а з іншого боку, принципи захисту повинні відображатися в правах, наданих особам, чиї дані є об'єктом обробки, бути поінформованим про обробку, мати доступ до даних, вимагати їх виправлення або заборони обробки за певних обставин;

26) принципи захисту мають застосовуватися до будь-якої інформації, що торкається визначеної особи або яка може бути визначена; щоб встановити, що особа може бути

визначена, враховуються всі засоби, які можуть бути розумно застосовані контролером або будь-якою іншою особою для ідентифікації особи-суб'єкта даних; принципи захисту не застосовуватимуться до тих даних, які перетворені на анонімні, щоб унеможливити в подальшому ідентифікацію особи-суб'єкта даних; при обранні способів перетворення даних на анонімні та зберігання їх у формі, в якій визначення особи стає неможливим можуть використовуватися кодекси поведінки згідно зі статтею 27;

27) захист осіб має застосовуватися як до автоматизованої обробки даних, так і ручної; рівень цього захисту не повинен залежати від застосовуваної техніки, бо інакше виникатиме серйозний ризик недотримання захисту; щодо ручної обробки, то ця Директива поширюється лише на файлові системи і не застосовується до неструктурованих файлів; зміст файлової системи має структуруватися згідно з конкретними критеріями, що стосуються осіб, що забезпечить зручний доступ до персональних даних; згідно з положенням статті 2 (в) різні критерії для визначення елементів структурованої сукупності персональних даних і різні критерії, що регулюють доступ до цієї сукупності даних, можуть бути розроблені кожною Державою-членом; файли або системи файлів, як і їх обкладинки, що не структуровані згідно з конкретними критеріями, в жодному разі не підпадають під сферу застосування цієї Директиви;

28) будь-яка обробка персональних даних повинна бути законною і чесною по відношенню до осіб, яких вона торкається; зокрема, дані мають бути адекватними, справжніми і не надмірними щодо цілей, заради яких вони обробляються; такі цілі мають бути чітко сформульованими і законними, визначеними на момент збирання даних; цілі обробки після збору даних не можуть бути змінені і відрізнятися від тих, що були сформульовані спочатку;

29) подальша обробка персональних даних в історичних, статистичних чи наукових цілях не може вважатися несумісною з цілями, заради яких збиралися дані, якщо Держави-члени забезпечують відповідні гарантії; ці гарантії, зокрема, не повинні допускати використання цих даних для вжиття заходів або прийняття рішень проти будь-якої особи;

30) для того, щоб бути законною, обробка персональних даних має, окрім іншого, ґрунтуватися на згоді суб'єкта даних і бути необхідною з огляду на укладення або виконання договору, що накладає зобов'язання на суб'єкта даних, дотримання вимоги закону чи виконання завдань в громадських інтересах або для здійснення функції державної влади і навіть для задоволення законного інтересу фізичної чи юридичної особи за умови, що інтереси, права і свободи суб'єкта даних не будуть ігноруватись; зокрема, для підтримання балансу задіяних інтересів за одночасної гарантії дієвої конкуренції Держави-члени можуть уточнювати умови, за яких можуть використовуватися або повідомлятися Третій стороні персональні дані, під час правомірної поточної діяльності підприємств і інших установ; Держави-члени можуть подібним чином уточнювати умови, за яких персональні дані можуть повідомлятися Третій стороні в цілях вивчення ринку або реклами, що здійснюються

благодійною установою чи іншим об’єднанням, фундаціями, наприклад, політичного характеру, з одночасним урахуванням положень, що дозволяють суб’єктам даних відмовлятися без зазначення мотивів і без витрат від опрацювання персональних даних;
31) обробка персональних даних вважається правомірною, якщо здійснюється для захисту інтересу, що є важливим для життя суб’єкта даних;
32) національним законодавством має бути встановлено, чи є контролер даних, що виконує свої функції в інтересах суспільства або для здійснення державної влади, державним органом чи іншою фізичною або юридичною особою, визначеною публічним чи приватним правом, як наприклад, професійне об’єднання;
33) дані, які за своєю природою здатні завдати шкоди основним свободам або приватності, не повинні оброблятися, якщо суб’єкт даних не дасть на це однозначної згоди; винятки з цієї заборони мають формулюватися досить чітко для конкретних потреб, зокрема, якщо обробка цих даних здійснюється в цілях, пов’язаних зі здоров’ям осіб, що мають юридичне зобов’язання щодо професійної таємниці, або для законної діяльності з боку певних об’єднань або фундацій, метою яких є забезпечити втілення на практиці основних свобод;
34) Державам-членам необхідно також дозволити з міркувань важливості громадських інтересів робити винятки з заборони на обробку вразливих даних у таких сферах, як охорона здоров’я населення і соціальний захист, особливо для забезпечення якості і рентабельності під час процедур, що застосовуються при вирішенні питань про виплати і послуги в системі медичного страхування, науково-дослідної роботи та офіційної статистики; їм належить передбачити відповідні і конкретні гарантії з метою захисту основних прав і приватності фізичних осіб;
35) крім того, обробка персональних даних державними органами для досягнення цілей, встановлених у конституційному праві або міжнародному публічному праві, офіційно визнаних релігійних об’єднань здійснюється з причин важливості громадського інтересу;
36) якщо функціонування демократичної системи в деяких Державах-членах вимагає, аби під час проведення виборів політичні партії збирали дані про політичні погляди громадян, опрацювання цих даних з огляду на важливість громадського інтересу може дозволятись за умови, що будуть встановлені відповідні гарантії;
37) для обробки персональних даних в журналістських цілях, а також в цілях літературного чи мистецького відображення, зокрема в аудіовізуальному секторі, повинні передбачатися винятки або обмеження певних положень цієї Директиви за умови, що вони будуть необхідними для погодження основних прав людини із свободою слова і, зокрема, свободою отримувати і передавати інформацію, як це гарантовано в статті 10 Європейської Конвенції про захист прав людини і основних свобод; у зв’язку з цим Державам-членам для посилення цих основних прав слід передбачити необхідні винятки і обмеження з метою балансування між основними правами, в тому, що стосується основних засад законності обробки даних,

засад про передачу даних у треті країни і компетенцію органів нагляду, але це не повинно призводити до впровадження Державами-членами винятків із заходів, що гарантують безпеку обробки; відповідальному наглядовому органу з цього питання мають надаватися повноваження *a posteriori*, наприклад, періодична публікація доповіді чи передача справи на розгляд до судових органів;

38) правомірність опрацювання даних передбачає, що суб'єкти даних повинні сповіщатись про вчинення операцій з обробки, а коли дані отримуються від них самих, суб'єкти повинні мати точну і повну інформацію про обставини збору;

39) певні операції з обробки даних, які контролер отримав не безпосередньо від суб'єкта даних; більше того, ці дані на законних підставах можуть розкриватися третій стороні, навіть якщо це розкриття не передбачалося в момент отримання даних від самого суб'єкта даних; за всіх цих умов треба повідомляти суб'єкта даних у момент реєстрації даних або щонайпізніше - при розкритті даних в перший раз третій стороні;

40) проте немає потреби вимагати цього, якщо суб'єкт даних уже поінформований; більше того, потреби в такому зобов'язанні немає, якщо реєстр чи повідомлення недвозначно передбачені законом або якщо поінформувати суб'єкта неможливо, або якщо це вимагає надзвичайних зусиль, як це може бути з обробкою в історичних, статистичних чи наукових цілях; в такому разі враховується кількість суб'єктів даних, давність даних та можливі компенсаційні заходи;

41) будь-яка особа повинна користуватися правом доступу до даних, що стосуються її і є предметом обробки, аби впевнитися у точності даних та правомірності їх обробки; з цих же причин кожен суб'єкт даних повинен мати право знати логіку, покладену в основу автоматизованої обробки даних, що стосуються її, принаймні у випадку автоматичних рішень згідно зі Статтею 15 (1), де йдеться про те, що це право не повинно завдавати шкоди комерційній таємниці або інтелектуальній власності, зокрема праву автора, що захищає програмне забезпечення; проте це не повинно призводити до відмови в наданні будь-якої інформації суб'єкту даних;

42) Держави-члени можуть в інтересах суб'єкта даних або з метою захисту прав і свобод інших осіб обмежувати права доступу та інформацію; вони, наприклад, можуть зробити уточнення, згідно з яким доступ до даних медичного характеру може здійснюватися лише через працівників охорони здоров'я;

43) обмеження прав доступу, інформації та на певні повноваження контролера можуть також накладатися Державами-членами, якщо вони потрібні для гарантій, скажімо, національної безпеки, захисту, громадського спокою або важливих економічних чи фінансових інтересів Держави-члена або Союзу, а також кримінальних розслідувань, звинувачень та дій, пов'язаних з порушенням правил етики регламентованих професій; перелік винятків та обмежень повинен включати також завдання для моніторингу, перевірки або врегулювань,

необхідних у трьох останніх зазначених сферах, які стосуються громадського порядку, економічних та фінансових інтересів та запобігання злочинності; перерахування завдань у цих трьох сферах не впливає на законність винятків чи обмежень, встановлених з причин безпеки й захисту держави;

44) Держави-члени можуть бути змушені з огляду на положення законодавства Співтовариства встановити винятки з положень цієї Директиви, що стосуються права доступу, обов'язку інформувати осіб та якості даних, для гарантії деяких з вищезазначених положень;

45) якщо можна правомірно виконати обробку даних у державних інтересах або для здійснення державної влади чи для задоволення законного інтересу фізичної чи юридичної особи, суб'єкт даних має, однак, право заперечувати проти обробки даних, що його стосуються, на підставі обґрунтованих причин, пов'язаних з його конкретною ситуацією; проте Держави-члени можуть встановлювати протилежні національні положення;

46) захист прав і свобод суб'єктів даних стосовно обробок персональних даних вимагає вжиття відповідних технічних і організаційних заходів як у момент створення системи обробки, так і під час самих обробок, передусім з метою гарантування безпеки і запобігання будь-якій несанкціонованій обробці; Державам-членам належить дбати про те, аби контролери дотримувалися цих засад; ці засади мають гарантувати адекватний ступінь безпеки з урахуванням стану розвитку техніки і витрат щодо її застосування у зв'язку з появою ризику, пов'язаного з опрацюванням, характером даних, що мають захищатись;

47) коли персональні дані передаються телекомунікаційними засобам або електронною поштою, єдиною метою яких і є передача таких повідомлень, зазвичай контролером персональних даних, наявних у повідомленні, вважається та особа, що є відправником повідомлення, а не та, яка надає послуги з передачі; разом з тим, особи, які надають ці послуги, також вважатимуться контролерами додаткових, необхідних для надання послуги з передачі персональних даних;

48) процедури повідомлення наглядовому органові мають на меті забезпечення гласності цілей обробок і їх основних характеристик з метою встановлення їх відповідності положенням національного права, прийнятим на виконання цієї Директиви;

49) для запобігання недоречним адміністративним процедурам Держави - члени можуть встановлювати винятки або спрощення повідомлення обробок, якщо при цьому вони зможуть уникнути порушенням прав і свобод суб'єктів даних і відповідають актові, прийнятому Державою - членом, в якому визначаються правові рамки для цього; Держави - члени можуть також запроваджувати винятки або спрощення, якщо особа призначена контролером переконується в тому, що виконувані обробки не можуть порушити прав і свобод суб'єкта даних; такий уповноважений із захисту даних, незалежно від того, чи є він посадовою особою контролера, повинен виконувати свої функції цілком незалежно;

50) винятки або спрощення можуть встановлюватися для процесуальних операцій, єдиною метою яких є утримання реєстрів, призначених згідно з національним правом забезпечувати інформацією громадськість, доступних для ознайомлення громадськості або будь-якої особи, що доведе правомірність свого інтересу;
51) проте спрощення або запровадження винятків у процедурі повідомлення не звільняє контролера від інших зобов'язань, передбачених цією Директивою;
52) в цьому зв'язку наступна перевірка з боку компетентних органів повинна вважатися достатнім заходом;
53) проте певні операції обробки можуть становити особливий ризик правам і свободам суб'єкта даних через свою природу, їх сукупність або цілі, як, наприклад, позбавлення осіб права, вигоди чи контракту або через специфічне використання нових технологій; Держави - члени за бажанням можуть окреслити такі ризики в своїх законодавствах;
54) з усіх обробок, виконуваних в суспільстві, число тих, що становлять ризик, повинно бути дуже обмеженим; Держави - члени повинні передбачити для таких обробок до їх реалізації попередню перевірку з боку наглядового органу або уповноваженого із захисту даних спільно з цим органом; після попередньої перевірки наглядовий орган згідно з положеннями національного законодавства може зробити висновок або дати спеціальний дозвіл стосовно обробки; така попередня перевірка може здійснюватися також у ході розробки законодавчих засад, схвалених національним парламентом, або правового акту, що ґрунтується на таких законодавчих засадах, який визначає характер обробки і уточнює відповідні гарантії;
55) національне законодавство повинне передбачити засоби правового захисту для випадків, коли контролер даних не забезпечує прав суб'єктів даних; будь-яка шкода, яку може бути завдано особам внаслідок неправомірної обробки, повинна компенсуватися контролером даних; останній може бути звільнений від такої відповідальності, якщо доведе, що шкідлива дія не може бути поставлена йому в провину або якщо доведе відповідальність суб'єкта даних чи пошлеться на обставини непоборної сили; до будь-якої особи, яка не дотримується положень національного права, прийнятих на виконання цієї Директиви, мають застосовуватися санкції як за приватним правом, так і за публічним;
56) потоки персональних даних через кордони потрібні для розвитку міжнародної торгівлі; захист осіб, гарантований у Співтоваристві цією Директивою, не суперечить передачі персональних даних до третіх країн, які гарантують адекватний рівень захисту; адекватність ступеня захисту, який забезпечується третьою країною, має оцінюватися з урахуванням усіх обставин, пов'язаних з передачею чи низкою процедур передачі;
57) інакше передача персональних даних до третьої країни, яка не забезпечує адекватного рівня захисту, повинна бути заборонена;
58) з такої заборони мають бути винятки, сформульовані окремими положеннями, що стосуються таких обставин, коли суб'єкт даних дав свою згоду, коли передача необхідна у

зв’язку з контрактом або юридичною вимогою, коли цього вимагає захист важливого громадського інтересу, наприклад, у випадках міжнародного обміну даними між податковими чи митними відомствами або між службами, компетентними в питаннях соціального страхування, або коли передача відбувається з реєстру, передбаченого в законодавстві з метою ознайомлення громадськості або осіб, що мають законний інтерес; в такому разі ця передача не повинна впливати на сукупність даних або категорії даних, що містяться в зазначеному реєстрі; оскільки призначення реєстру полягає в ознайомленні з ним особами, що мають законний інтерес, передача може відбуватися лише на прохання цих осіб або коли вони є її одержувачами;

59) для поліпшення рівня захисту в третій країні, можуть прийматися конкретні заходи, якщо контролер пропонує відповідні гарантії; більше того, повинні передбачатися процедури переговорів між Співтовариством і, відповідно, третьою країною;

60) в будь-якому разі передачі в треті країни можуть відбуватися тільки за умови повного дотримання положень, прийнятих Державами - членами на виконання цієї Директиви, зокрема статті 8;

61) Держави - члени і Комісія у межах своїх компетенцій повинні стимулювати професійні сектори та інші зацікавлені представницькі організації для розробки кодексів поведінки з метою сприяння застосування цієї Директиви, враховуючи специфіку обробок, виконуваних у різних сферах, і виявляючи повагу до національних положень, прийнятих на її втілення;

62) створення наглядового органу в Державах-членах, який здійснює свої функції цілком незалежно, є важливим чинником захисту осіб стосовно обробки персональних даних;

63) цей орган повинен мати в своєму розпорядженні необхідні для виконання функцій засоби, будь то повноваження на розслідування або втручання, зокрема у випадках оскарження, та повноваження вступати в судовий процес; такі органи мають сприяти прозорості обробки даних, здійснюваної в Державі - члені, під юрисдикцією якої він перебуває;

64) органи різних держав - членів мають надавати один одному взаємну допомогу при виконанні своїх функцій, аби гарантувати повне дотримання правил захисту в усьому Європейському Союзі;

65) у Співтоваристві має бути створена Робоча група із захисту осіб стосовно опрацювання персональних даних, яка має бути сформована цілком незалежно; з урахуванням своєї специфічності група має допомагати Комісії й сприяти, зокрема, неухильному дотриманню національних норм, прийнятих на виконання цієї Директиви;

66) стосовно передачі даних у треті країни застосування цієї Директиви вимагає надання Комісії повноважень з імплементації і створення процедури згідно з видами, встановленими в рішенні Ради 87/373/CEE [4];

67) 20 грудня 1994 року досягнуто угоду про *modus vivendi* між Європейським парламентом,

Радою і Комісією щодо заходів із застосування актів, прийнятих згідно з процедурою, встановленою в статті 189(в) Договору про ЄС;
68) принципи захисту прав і свобод осіб, зокрема їх права на приватність, стосовно обробки персональних даних, викладені в цій Директиві, можуть доповнюватись або уточнюватися в окремих галузях спеціальними правилами, що ґрунтуються на цих принципах;
69) Державам - членам доцільно надати термін, не більший, ніж три роки з моменту набрання чинності національних засобів на впровадження цієї Директиви, для прогресивного застосування нових національних положень до вже наявних обробок даних; з метою полегшення застосування з прийнятним співвідношенням витрат і ефективності Державам - членам надається додатковий період, що закінчиться через 12 років від дати прийняття цієї Директиви, аби гарантувати пристосування існуючих ручних файлових систем на цю дату до положень Директиви; якщо дані, які містяться в цих файлових системах, ефективно обробляються в ручний спосіб, то упродовж цього перехідного періоду вони мають бути пристосовані до цих положень при здійсненні ручного опрацювання;
70) недоцільно змушувати суб'єкта даних ще раз давати свою згоду на те, щоб відповідальний міг продовжувати після набрання чинності національних положень, прийнятих у відповідь на цю Директиву, здійснювати обробку вразливих даних, необхідних для виконання укладених контрактів за попередньої вільної та поінформованої згоди до набрання чинності зазначених вище положень;
71) ця Директива не суперечить тому, щоб Держава - член регулювала діяльність із комерційної реклами, спрямовану на споживачів, що мешкають на її території, тією мірою, якою це регулювання не стосується захисту осіб стосовно обробки персональних даних;
72) ця Директива дозволяє враховувати принцип громадського доступу до офіційних документів під час застосування принципів, викладених у цій Директиві.

Зважаючи на все викладене, Європейський парламент і Рада Європейського Союзу прийняли таку директиву:

Розділ 1
Загальні положення
Стаття 1
Предмет Директиви
1. Держави - члени гарантують згідно з положеннями цієї Директиви захист основних свобод і прав фізичних осіб, зокрема, права на приватність стосовно обробки персональних даних.
2. Держави - члени не можуть ні обмежувати, ні забороняти вільний потік даних на своїх територіях з причин, пов'язаних із захистом, гарантованим згідно з викладеним у положенні 1.

Стаття 2

Визначення

Для цілей цієї Директиви:

a) "персональні дані" - це будь-яка інформація про фізичну особу, ідентифіковану чи таку, що може бути ідентифікована ("суб'єкт даних"); такою, що може бути ідентифікована, вважається будь-яка особа, чия особистість може бути встановлена безпосередньо чи опосередковано, наприклад, через ідентифікаційний номер або один чи кілька специфічних елементів фізичної, фізіологічної, психічної, економічної, культурної або соціальної тотожності;

b) "обробка персональних даних" ("обробка") означає будь-яку операцію або сукупність операцій, здійснених через автоматизовані або неавтоматизовані процеси і застосовані до персональних даних, таких як збирання, реєстрація, організація, збереження, розробка або модифікація, вибірка, консультування, використання, розкриття передачею, поширенням або через будь-яку іншу дію, що робить їх доступними, комбінування і взаємо пов'язування, а також їх блокування, стирання або знищення;

c) "файлова система персональних даних" ("файлова система") означає будь-який структурований масив персональних даних, до якого є доступ згідно з визначеними критеріями, централізований чи децентралізований або розподілений за функціональним чи географічним принципом;

d) "контролер" означає фізичну чи юридичну особу, державний орган, агенцію або будь-який інший заклад, який самостійно або разом з іншими визначає цілі і засоби обробки персональних даних; в разі, коли цілі й засоби обробки визначені правом або регулятивними положеннями Держави - члена чи Співтовариства, контролер або специфічні для його функціонального призначення критерії можуть бути визначені національним законодавством чи правом Співтовариства;

e) "обробник" означає фізичну або юридичну особу, державний орган, агентство або будь-який інший орган, який сам або спільно з іншими опрацьовує персональні дані за завданням контролера;

f) "третя сторона" означає фізичну чи юридичну особу, державний орган, агенцію чи будь-який інший орган, що не є ні суб'єктом даних, ні контролером, ні обробником, або особами, яким згідно з безпосереднім розпорядженням контролера чи обробника надається повноваження обробляти ці дані;

g) "одержувач" означає фізичну чи юридичну особу, державний орган, агенцію чи будь-який інший орган, якому розкриваються дані, будь то третя сторона чи ні; проте органи, які можуть отримати дані за особливим запитом, не повинні розглядатися як "одержувачі";

h) "згода суб'єкта даних" означає будь-яке добровільне, конкретне та повідомлене волевиявлення, через які суб'єкт даних згоджується на опрацювання персональних даних, що

його стосуються.

Стаття 3.

Сфера застосування

1. Положення цієї Директиви застосовуються повністю або частково до автоматизованої обробки персональних даних, а також до неавтоматизованої обробки персональних даних, що складають частину файлової системи або призначені складати частину файлової системи.

2. Положення цієї Директиви не застосовуються до обробки персональних даних:

- якщо така обробка виконується для провадження діяльності, що не входить до сфери застосування права Співтовариства, передбаченої положеннями розділів У і У1 Договору про Європейський Союз, і в жодному разі для виконання операцій з обробки даних, що стосуються громадського порядку, оборони, державної безпеки (включаючи економічний добробут держави, якщо обробка стосується справ державної безпеки), а також діяльності держави у сфері кримінального права;
- якщо обробку збирається виконувати фізична особа для здійснення виключно особистої або домашньої діяльності.

Стаття 4.

Застосування національного законодавства

1. Держави - члени застосовують внутрішні положення, прийняті для впровадження цієї Директиви, до будь-якої обробки персональних даних, якщо:

a) обробка здійснюється в межах діяльності закладу контролера на території Держави - члена; якщо один і той же контролер призначений на території кількох Держав - членів, він повинен вживати необхідних заходів для забезпечення того, аби кожна з цих закладів виконував зобов'язання, передбачені національним законодавством;

b) контролер не розміщується на території Держави - члена, а на території, де застосовується його внутрішнє право згідно з міжнародним громадянським правом;

c) контролер не заснований на території Співтовариства і для обробки персональних даних використовує автоматизовані чи неавтоматизовані засоби, розташовані на території згаданої Держави-члена, якщо такі засоби використовується не лише в цілях транзиту через територію Співтовариства.

2. За обставин, викладених у положеннях 1 (c), контролер повинен призначити представника, заснованого на території цієї Держави-члена, не створюючи упередженого ставлення до законних дій, яке могло б бути використаним проти самого контролера.

Розділ П

Загальні положення щодо правомірності обробки персональних даних.

Стаття 5.

Держави-члени уточнюють в межах положень цього Розділу умови, за яких обробка персональних даних є правомірною.

Підрозділ 1.

Положення, що стосуються якості даних

Стаття 6.

1. Держави-члени приймають рішення, згідно з якими персональні дані повинні:

a) оброблятися на справедливих і законних підставах;

b) збиратися для визначених і законних цілей та не використовуватися в подальшому у спосіб, несумісний з цими цілями; не вважається несумісною обробка в історичних, статистичних чи наукових цілях за умови, що Держави-члени встановлюють відповідні гарантії;

c) бути адекватними, відповідними і не надмірними з точки зору цілей, заради яких вони збираються і/або в подальшому обробляються;

d) бути точними і в разі необхідності поновлюватися; повинні вживатися всі розумні заходи, щоб неточні або неповні з точки зору цілей дані знищувались або виправлялися;

e) зберігатися у формі, яка дозволяє ідентифікувати суб'єктів даних не довше, ніж це необхідно для цілі, заради якої такі дані зберігаються або в подальшому обробляються. Держави - члени встановлюють відповідні гарантії для персональних даних, що зберігаються протягом довшого періоду для історичної, статистичної чи наукової цілі.

2.Відповідальність за виконання положень, викладених у пункті 1, покладається на контролера.

Підрозділ П

Принципи щодо узаконення обробки даних

Стаття 7.

Держави - члени встановлюють, що обробка персональних даних здійснюється лише за умови, якщо:

a) суб'єкт даних дав на це однозначну згоду; або

b) обробка необхідна для виконання контракту, в якому суб'єкт даних є однією з сторін, або заходів, що передують підписанню такого контракту; або

c) обробка необхідна для виконання юридичного зобов'язання, покладеного на контролера; або

d) обробка необхідна для забезпечення життєво важливих інтересів суб'єкта даних; або

e) обробка необхідна для виконання завдання в громадських інтересах або пов'язана з реалізацією владних повноважень, покладених на контролера або на третю сторону, якій розкриваються дані; або

f) є необхідною для задоволення законного інтересу, що його виявляє контролер або третя сторона чи сторони, яким розкриваються дані, за умови, що він не переважає інтересів суб'єктів даних в його правах і свободах, які вимагають захисту згідно зі Статтею 1 (1) цієї Директиви.

Підрозділ Ш

Спеціальні категорії обробки

Стаття 8.

Обробка спеціальних категорій даних

1.Держави - члени забороняють обробку персональних даних, які розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання, членство у профспілках та обробку даних, що стосуються здоров'я чи статевого життя.

2.Положення пункту 1 не застосовуються, якщо:

a) суб'єкт даних дав свою однозначну згоду на опрацювання таких даних, окрім випадків, коли Держава - член положеннями закону встановила, що заборона викладена в положенні 1, не може зніматися за згодою суб'єкта даних; або

b) обробка є необхідною з огляду на конкретні зобов'язання і спеціальні права контролера в питаннях трудового законодавства, тією мірою, якою це регламентовано національним законом, який передбачає відповідні гарантії; або

c) обробка необхідна для захисту життєвих інтересів суб'єкта даних або іншої особи, а суб'єкт даних фізично чи юридично нездатний дати свою згоду; або

d) обробка здійснюється фундацією, асоціацією або будь-яким іншим неприбутковим органом політичної, філософської, релігійної або профспілкової спрямованості під час своєї законної діяльності і з належними гарантіями за умови, що обробка стосується виключно членів закладу або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, і здійснюється таким чином, що дані не передаються третій стороні без згоди суб'єктів даних; або

e) обробка стосується даних, які суб'єкт даних зробив гласними, або є необхідною для обґрунтування, виконання або захисту правової вимоги.

3. Положення 1 не застосовується, якщо обробка даних виявляється необхідною для цілей превентивної медицини, медичної діагностики, для забезпечення піклування чи лікування або успішного функціонування служб охорони здоров'я за умови, що такі дані обробляються медичним персоналом згідно з національним законодавством або відповідно до правил, встановлених уповноваженими державними органами, з дотриманням професійної таємниці або іншою особою, на яку покладено подібні зобов'язання по збереженню таємниці.

4. За умови наявності положень про відповідні гарантії Держави - члени можуть з важливих причин публічного інтересу встановлювати інші винятки на додаток викладеним у пункті 2 в положеннях національного законодавства або за рішенням наглядового органу.

5. Обробка даних, що стосується звинувачень у злочині, карних вироків або заходів з безпеки, може здійснюватись лише під контролем державної влади або якщо в національному законодавстві передбачено відповідні спеціальні гарантії; це не стосується винятків, які може встановлювати Держава-член, спираючись на внутрішні розпорядження, що передбачають відповідні спеціальні гарантії. Проте повний реєстр кримінальних

покарань може вестися лише під контролем державної влади.

Держави-члени можуть встановлювати, що обробка даних, пов'язаних з адміністративними санкціями або цивільними судочинством здійснюється також під контролем державних органів влади.

6. Винятки з положень пункту 1, визначені в пунктах 4 і 5, повідомляються Комісії.

7. Держави-члени визначають умови, за яких національний ідентифікаційний номер або будь-який інший засіб ідентифікації загального характеру може бути предметом обробки.

Стаття 9.

Обробка персональних даних і свобода виявлення поглядів.

Якщо обробка персональних даних здійснюється виключно в журналістських цілях, а також в цілях літературного чи мистецького відображення, Держави-члени встановлюють в межах положень цього Розділу, Розділу IV і Розділу VI винятки, але в тому обсязі, в якому вони необхідні для узгодження права на приватність з положеннями, що регулюють свободу виявлення поглядів.

Підрозділ IV

Інформація, яка повинна надаватися суб'єктові даних

Стаття 10

В разі отримання даних від самого суб'єкта даних

Держави-члени встановлюють, що контролер чи його представник повинен надавати суб'єкту даних, від якого отримуються дані, що стосуються його, принаймні інформацію, характер якої подано нижче, якщо особі її ще не повідомили:

a) про особу контролера та його представника, за наявністю;

b) про цілі, заради яких здійснюється обробка;

c) будь-яка інша інформація, зокрема:

- про одержувача або категорії одержувачів даних;

- про обов'язковість чи необов'язковість відповіді і наслідки, які спричинить відмова відповідати для суб'єкта даних;

- про наявність права доступу і права на виправлення даних, що стосуються суб'єкта даних, в тому обсязі, який з урахуванням конкретних обставин отримання даних є необхідним для гарантування правомірності обробки даних стосовно суб'єкта даних.

Стаття 11

Інформація у разі отримання даних не від суб'єкта даних

1. Якщо дані не були отримані від самого суб'єкта даних, Держави-члени встановлюють, що контролер або його представник повинні в момент реєстрації даних або в разі, коли є намір розкриття даних третій стороні, не пізніше дати першого розкриття даних довести до відома суб'єкта даних принаймні інформацію, подану нижче, якщо він не був поінформований раніше:

a) про особу контролера та його представника, за наявністю;

b) про цілі обробки, предметом яких будуть дані;

c) будь-яку іншу інформацію, що стосується:

- категорії даних, про які йдеться,

- одержувача або категорії одержувачів даних,

- наявність права доступу та права на виправлення відповідних даних, що стосуються його,

тією мірою, якою з урахуванням конкретних обставин за яких отримуються дані, буде необхідна додаткова інформація для гарантування правомірності обробки даних стосовно суб'єкта даних.

2. Положення пункту 1 не застосовуються зокрема до обробок даних у статистичних цілях або для історичного чи наукового дослідження, коли інформування суб'єкта даних виявляється неможливим або вимагає непропорційних зусиль, або якщо реєстрація або розкриття однозначно сформульовані в законодавстві. У цих випадках Держави-члени забезпечують відповідні гарантії.

Підрозділ V.

Права суб'єкта даних на доступ до даних.

Стаття 12

Право доступу

Держави-члени гарантують всім суб'єктам даних право на отримання від контролера:

a) вільно, без обмежень, із розумною періодичністю та без запізнень чи надмірних витрат:

- підтвердження наявності або відсутності обробки даних, що стосуються суб'єкта даних, а також інформування принаймні про цілі цих обробок, категорії цих даних, а також одержувачів або категорії одержувачів, яким розкриваються ці дані,

- повідомлення у доступній для розуміння формі даних, що є предметом обробки, а також усієї інформації щодо походження даних,

- ознайомлення з логікою, використаною в автоматизованих обробках даних, що стосується їх суб'єкта, зокрема в автоматизованих рішеннях, про що йдеться в Статті 15 (1);

b) якщо доцільно виправлення, усунення або блокування даних, опрацювання яких не відповідає положенням цієї Директиви, зокрема через їх неповноту або неточність;

c) повідомлення третій стороні, якій були розкриті дані, про виправлення, усунення або блокування, здійснені відповідно до пункту b), якщо це не є неможливим або не потребує непропорційних зусиль.

Підрозділ VI

Винятки і обмеження

Стаття 13

1. Держави-члени можуть передбачати у законодавстві обмеження сфери дії зобов'язань і прав, передбачених у пункті 1 статті 6, у статті 10, у пункті 1 статті 11 та статтях 12 і 21,

якщо таке обмеження є необхідним заходом для забезпечення:

a) державної безпеки;

b) оборони;

c) громадської безпеки;

d) запобігання, розслідування, затримання і припинення кримінальних порушень або недотримання етичних норм для регламентованих професій, або

e) важливого економічного або фінансового інтересу Держави-члена або Європейського Союзу, включаючи грошово-кредитні, бюджетні і податкові питання;

f) функції моніторингу, інспекції або регламентування, пов'язаної навіть принагідно з повноваженнями державної влади у випадках, передбачених пунктами c), d) та e);

g) захисту суб'єкта даних або прав і свобод інших осіб.

2. Не торкаючись адекватних законних гарантій, які, зокрема, виключають дані, що можуть використовуватись для вжиття заходів або прийняття рішень стосовно конкретної особи, Держави-члени можуть за умови відсутності явного ризику посягань на право приватності суб'єкта даних обмежувати через законодавче положення передбачені в Статті 12 права, якщо дані обробляються виключно для наукового дослідження або утримуються в персоніфікованій формі протягом періоду, що не перевищує термін, необхідний виключно для статистичних цілей.

Підрозділ VII

Право суб'єкта даних на заперечення

Стаття 14

Право суб'єкта даних заперечувати

Держави-члени надають суб'єкту даних право:

a) заперечувати, принаймні у випадках, передбачених у пунктах e) та f) статті 7, у будь-який час на законних підставах у кожній конкретній ситуації проти обробки даних, що його стосують, якщо це не суперечить національному законодавству. У разі правомірного заперечення проти обробки даних контролер не може здійснювати опрацювання таких даних;

b) безкоштовно заперечувати на запит проти обробки персональних даних, що його стосується, які контролер збирається обробляти у цілях дослідження ринку або бути поінформованим перед тим, як дані будуть розкриті вперше третім сторонам або будуть використані від їх імені в цілях дослідження ринку; мати реально запропоноване право безкоштовно заперечувати проти такого розкриття або використання.

Держави-члени мають вжити всіх необхідних заходів для забезпечення того, щоб суб'єкти даних усвідомлювали існування права, про яке йдеться у першій частині положення b).

Стаття 15

Автоматизовані індивідуальні рішення

1. Держави-члени визнають за кожною особою право не підлягати рішенню з юридичними наслідками для неї або рішенню, що має на неї значний вплив і яке ґрунтується виключно на автоматизованій обробці даних, призначеній для оцінки певних характеристик особистості, таких як професійні якості, кредитоспроможність, надійність, особливості поведінки тощо.

2. З урахуванням інших статей цієї Директиви Держави-члени передбачають, що особа може підпадати під одне з рішень, розглянутих у пункті 1, якщо це рішення:

a) прийняте в межах укладення або виконання контракту за умови, що прохання про укладення або виконання контракту, представлене суб'єктом даних, було задоволено; або існують відповідні заходи, наприклад, можливість захищати свою точку зору з метою забезпечення свого законного інтересу, або

b) дозволене законом, що встановлює заходи для гарантування законного інтересу суб'єкта даних.

Підрозділ VIII

Конфіденційність і захист обробки

Стаття 16

Конфіденційність обробки

Будь-яка особа, що діє від імені контролера або обробника, включаючи самого обробника, яка має доступ до персональних даних, не може обробляти дані за виключенням, коли це буде дозволено контролером або якщо зробити це вимагається від особи за законом.

Стаття 17

Захист обробки

1. Держави-члени зобов'язують контролера застосовувати адекватні технічні й організаційні заходи для захисту персональних даних від випадкового чи незаконного знищення або від випадкової втрати, зміни, розкриття або недозволеного доступу, зокрема у випадках, коли обробка включає передачу даних мережею, і від будь-якої іншої незаконної форми обробки.

Рівень захисту даних має забезпечуватися відповідно до стану розвитку технічних знань і вартості їх застосування і повинен відповідати ризикам, які несе обробка і характер даних, що мають захищатися.

2. Держави-члени зобов'язують контролера, у випадках коли обробка здійснюється вів його імені, обирати обробника, який надає достатні гарантії стосовно вжиття технічних і організаційних заходів із захисту під час процесу обробки і забезпечує дотримання цих заходів.

3. Здійснення обробок за дорученням повинно регулюватися контрактом або іншим правовим актом, який пов'язує обробника даних з контролером і передбачає, зокрема, що:

- обробник діятиме лише згідно з інструкціями контролера;
- зобов'язання пункту 1, визначені законодавством Держави-члена, де заснований обробник, поширюється також і на нього.

4. З метою забезпечення доказовості частина контракту або правового акту, що стосується захисту персональних даних і вимоги щодо заходів, про які йдеться в пункті 1, оформляються письмово або в іншій рівноцінній формі.

Підрозділ IX

Повідомлення

Стаття 18

Обов'язок повідомлення наглядовому органові

1. Держави-члени забезпечують, щоб контролер або, його представник, за наявністю, повідомляли наглядовому органові, про який ідеться в статті 28, до проведення повної чи часткової автоматизованої обробки чи сукупності таких обробок, призначених для досягнення однієї чи кількох взаємопов'язаних цілей.

2. Держави-члени можуть прийняти рішення про спрощення або скасування обов'язкового повідомлення лише у таких випадках і за таких умов:

- якщо для категорій обробок, які не можуть зачіпати прав і свобод суб'єктів даних, зважаючи на дані, що будуть оброблятися, Держави-члени уточнюють цілі обробок, дані або категорії даних, що обробляються, категорію або категорії суб'єктів даних, одержувачів або категорії одержувачів, яким повідомляються дані, і термін зберігання даних і/або
- якщо контролер призначає згідно з національним законодавством, у сфері якого він працює, уповноваженого з питань захисту персональних даних, в обов'язки якого входить:
- забезпечувати незалежним чином застосування національних положень, прийнятих згідно з цією Директивою;
- вести реєстр операцій з обробки, здійснюваних контролером, що містить інформацію, перелічену в пункті 2 статті 21;
- забезпечити при цьому, щоб операції з обробки даних не змогли завдати шкоди правам і свободам суб'єктів даних.

3. Держави-члени можуть передбачати, що пункт 1 не застосовуватиметься до тих обробок, єдиною метою яких є ведення реєстру, який згідно із законодавчими або підзаконними актами призначений інформувати громадськість, який є відкритим для ознайомлення громадськості в цілому або будь-якої особи, що може підтвердити свій законний інтерес.

4. Держави-члени можуть звільнити від обов'язку повідомлення або передбачити його спрощення стосовно обробок, про які йдеться в положенні d) пункту 2 статті 8.

5. Держави-члени можуть передбачити, що про неавтоматизовані обробки персональних даних в цілому або лише деякі з них повідомлятимуться у спрощеній формі.

Стаття 19.

Зміст повідомлення

1. Держави-члени визначають характер інформації, яка має міститися в повідомленні; інформація має включати:

a) прізвище та адресу контролера та його представника, за наявністю;

b) ціль або цілі обробки;

c) опис категорії або категорій суб'єктів даних і самих даних чи категорій даних, яких вона стосуються;

d) відомості про одержувачів або категорії одержувачів, яким дані можуть бути розкриті;

e) запропоновані передачі даних до третіх країн;

f) загальний опис, який дозволяє попередньо оцінювати адекватність заходів, прийнятих на виконання статті 17, для забезпечення захисту обробки.

2. Держави-члени визначають процедури, за якими наглядовий орган повідомляється про будь-які зміни , що впливають на інформацію, про яку йдеться в пункті 1.

Стаття 20

Попередній контроль

1. Держави-члени визначають обробки, які можуть становити особливі ризики для прав, свобод суб'єктів даних, і контролюють проходження випробування до початку обробки.

2. Цей попередній контроль здійснюються їх наглядовим органом після отримання повідомлення від контролера або уповноваженого з питань захисту даних, який у разі сумніву повинен проконсультував контрольний орган.

3. Держави-члени можуть також здійснювати цей контроль під час підготовки законодавчого акту національного парламенту або акті, що ґрунтується на такому законодавчому акті, який визначає характер опрацювання даних і встановлює відповідні гарантії.

Стаття 21

Гласність обробок

1. Держави-члени вживають необхідних заходів для забезпечення гласності операцій з обробок.

2. Держави-члени встановлюють, що наглядовий орган веде реєстр операцій з обробок, про який повідомляється у відповідності із положеннями статті 18.

У реєстрі як мінімум зазначається інформація перелічена в підпунктах від a) до e) пункту 1 статті 19;

Реєстр може бути перевіреним будь-якою особою.

3. Держави-члени передбачають, що контролер або інший орган, призначений Державами-членами, повідомляє про обробки, щодо яких повідомлення не є обов'язковим, у відповідній формі будь-якій особі, яка цього вимагатиме, принаймні ту інформацію, про яку йдеться в підпунктах від a) до e) пункту 1 статті 19.

Держави-члени можуть встановити, що це положення не застосовується до обробок, єдиною метою яких є ведення реєстру, який згідно з законодавчими або підзаконними нормативними актами призначений інформувати громадськість і є відкритим для ознайомлення громадськості в цілому або для будь-якої особи, яка може довести свій законний інтерес.

Розділ III.

Засоби правового захисту, відповідальність і санкції

Стаття 22.

Засоби правового захисту

Незалежно від адміністративного оскарження, яке може подаватись зокрема до наглядового органу, про який ідеться у статті 28, що передує зверненню до судового органу, Держави-члени надають будь-якій особі право оскарження в суді в разі порушення прав, гарантованих положеннями національного законодавства, що застосовується до зазначених обробок.

Стаття 23.

Відповідальність

1. Держави-члени передбачають, що будь-яка особа, якій завдано шкоди внаслідок незаконної обробки або будь-якої дії, несумісної з національними положеннями, прийнятими на виконання цієї Директиви, має право на отримання від контролера компенсації за заподіяну шкоду.

2. Контролер може бути звільнений частково або повністю від цієї відповідальності, якщо доведе, що обставина, через яку заподіяно шкоду, не може бути поставлена йому в провину.

Стаття 24.

Санкції

Держави-члени вживають відповідних заходів для забезпечення імплементації положень цієї Директиви і вживають зокрема санкції, які мають застосовуватися в разі невиконання положень, прийнятих на виконання цієї Директиви.

Розділ IV. Передача персональних даних до третіх країн

Стаття 25

Принципи

1. Держави-члени передбачають, що передача до третіх країн персональних даних, що є предметом обробки або призначені для обробки згодом після передачі, може здійснюватися тільки тоді, коли третя країна гарантує адекватний рівень захисту незалежно від виконання положень національного законодавства, прийнятих відповідно до решти положень цієї Директиви.

2. Адекватність рівня захисту, що його надає третя країна, оцінюється з урахуванням усіх обставин, що пов’язані із передачею або низкою операцій з передачі даних; зокрема, враховується характер даних, ціль, тривалість обробки або запропонованих обробок, країна походження і країна кінцевого призначення, стан законності і дотримання норм права – як загальних, так і галузевих, - що діють у цій третій країні, а також професійні норми і заходи безпеки, що застосовуються у цій країні.

3. Держави-члени і Комісія інформують одна одну про ті випадки, коли, на їх думку, третя країна не забезпечує адекватного рівня захисту згідно з пунктом 2.

4. Коли Комісія підтвердить згідно з процедурою, передбаченою в пункті 2 статті 31, що третя країна не забезпечує адекватного рівня захисту згідно з пунктом 2 цієї Статті, Держави-члени вживають заходів, необхідних для запобігання будь-якій передачі персональних даних цього типу до такої третьої країни.

5. У відповідний момент Комісія починає процес досягнення домовленості з метою виправлення ситуації, що склалася, коли підтвердиться факт, передбачений пунктом 4.

6. Комісія може стверджувати за процедурою, передбаченою в пункті 2 Статті 31, що третя країна забезпечує адекватний рівень захисту згідно з пунктом 2 цієї статті з огляду на її внутрішнє законодавство або її міжнародні зобов'язання, підписані, зокрема, після досягнення домовленості, про які ідеться у пункті 5, для захисту приватного життя та основних прав і свобод осіб.

Держави-члени вживають необхідних заходів для дотримання рішень Комісії.

Стаття 26.

Винятки

1. Зважаючи на викладене в статті 25, Держави-члени передбачають можливість передачі або низки передач персональних даних до третьої країни, яка не гарантує адекватного рівня захисту, як це визначається у пункті 2 статті 25, якщо національне законодавство не пропонує іншого на ці випадки, за умови, що:

a) суб'єкт даних дав свою чітку згоду на запропоновану передачу; або

b) передача є необхідною для виконання контракту між суб'єктом даних і контролером або для виконання підготовчих щодо контракту заходів, здійснюваних на прохання суб'єкта даних; або

c) передача є необхідною для укладення або виконання контракту, укладеного в інтересах суб'єкта даних між контролером та Третьою стороною, або

d) передача є необхідною або вимагається за законом для забезпечення важливого державного інтересу або для обґрунтування або реалізації чи захисту права в судовій процедурі; або

e) передача є необхідною для захисту життєвих інтересів суб'єкта даних або

f) передача здійснюється з реєстру, який згідно з законодавчими та підзаконними нормативними актами призначений для надання громадськості інформації і відкритий для ознайомлення громадськості в цілому або для будь-якої особи зокрема, якщо вона зможе довести правомірність свого інтересу за дотримання в кожному конкретному випадку умов, передбачених законом для ознайомлення.

2. Незалежно від встановленого в пункті 1, Держави-члени можуть дати дозвіл на передачу або низку передач персональних даних до третьої країни, яка не гарантує адекватний рівень захисту, як це розуміється у пункті 2 статті 25, якщо контролер доведе адекватність гарантій щодо захисту права на приватність, основних прав і свобод осіб, а також стосовно реалізації

відповідних прав; ці гарантії можуть випливати, зокрема, з відповідних договірних положень.

3. Держави-члени інформують Комісію та інші Держави-члени про дозволи, які надаються згідно з пунктом 2.

Якщо будь-яка Держава-член або Комісія заперечують на правомірних підставах, посилаючись на право на приватність, основні права і свободи особи, Комісія вживає відповідних заходів згідно з процедурою, визначеною пунктом 2 статті 31.

Держави-члени вживають необхідних заходів для дотримання рішення Комісії.

4. Якщо Комісія вирішила згідно з процедурою, встановленою в пункті 2 статті 31, що певні типові договірні положення надають достатні гарантії, встановлені в пункті 2, Держави-члени вживають необхідних заходів для дотримання рішення Комісії.

Розділ V

Кодекси поведінки

Стаття 27

1. Держави-члени і Комісія сприяють розробці кодексів поведінки, покликаних сприяти правильному застосуванню національних положень, прийнятих Державами-членами на виконання цієї Директиви, враховуючи галузеві особливості.

2. Держави-члени передбачають, що профспілки та інші організації, що представляють інші категорії контролерів, які розробляли або мають намір змінити чи розширити існуючі національні кодекси, можуть представити їх на розгляд національному органові.

Держави-члени встановлюють, що цей орган повинен встановити, серед іншого, чи відповідають представлені йому на розгляд проекти національними положеннями, прийнятими на виконання цієї Директиви. У разі потреби, цей орган вивчає думки суб’єктів даних або їх представників.

3. Проекти кодексів Співтовариства, а також зміни або доповнення до існуючих кодексів Співтовариства можуть подаватися для ознайомлення Робочій групі, зазначеній у статті 29. Ця Робоча група робить висновок про відповідність проектів, представлених на її розгляд, національним положенням, прийнятим на виконання цієї Директиви. У разі потреби, вивчає думки суб’єктів даних або їх представників.

Розділ VI.

Наглядовий орган і Робоча група з питань захисту осіб стосовно обробки персональних даних

Стаття 28.

Наглядовий орган

1. Держави-члени передбачають, що один або більше державних органів займаються наглядом за застосуванням на їх територіях положень, прийнятих на виконання цієї

Директиви.

Ці органи діють на виконання покладених на них функції цілком незалежно.

2. Держави-члени передбачають, що думка наглядових органів враховується при розробці підзаконних нормативних актів стосовно захисту прав і свобод осіб стосовно обробки персональних даних.

3. Кожний наглядовий орган наділяється, зокрема:

- повноваженнями для проведення розслідування, зокрема правом доступу до даних, які становлять предмет обробки, а також правом на збір будь-якої інформації, необхідної для виконання своєї наглядової діяльності;

- дієвими повноваженнями втручання, зокрема, як наприклад, надсилання висновків перед тим, як операції з обробки відбудуться, згідно зі статтею 20, та забезпечення публікації таких висновків, розпоряджатися стосовно блокування, стирання або знищення даних, тимчасового чи на невизначений час забороняти обробку, попереджати або нагадувати контролеру чи виносити питання на обговорення в парламенті або інших державних політичних інституціях;

- правом оскарження в разі порушень національних положень, прийнятих на виконання цієї Директиви, або передачі на розгляд судовій владі цих порушень.

Рішення контрольного органу, які порушують права, можуть бути об’єктом правового оскарження.

4. Кожний наглядовий орган повинен розглядати заяву від будь-якої особи або будь-якого об’єднання, яке її представляє, з питань її прав і свобод стосовно опрацювання персональних даних.

Особа повинна бути поінформована про результати розгляду заяви.

Кожний наглядовий орган повинен, зокрема, розглядати заяви на перевірку правомірності обробки, подані будь-якою особою, якщо застосовуються національні положення, прийняті для застосування Статті 13 цієї Директиви. Ця особа також повинна бути поінформована про факт проведення перевірки.

5. Кожний наглядовий орган періодично подає доповідь про свою діяльність. Доповідь доводиться до відома громадськості.

6. Кожний наглядовий орган є повноважним, які б національні положення не застосовувалися до цієї обробки даних, виконувати на території своєї держави функції, покладені на нього згідно з положенням 3 цієї статті. Цей орган може бути запитаний іншою Державою-членом для виконання своїх функцій на території за його юрисдикцією. Наглядові органи співпрацюють між собою тією мірою, якою це потрібно для виконання своїх функцій, зокрема, обмінюючись інформацією, яку вони вважають корисною.

7. Держави-члени передбачають, що члени і службовці наглядових органів підпадають навіть після звільнення від виконання своїх обов’язків під зобов’язання зберігати професійну

таємницю щодо конфіденційної інформації, до якої вони мали доступ.

Стаття 29.

Робоча група з питань захисту осіб стосовно обробки персональних даних.

1. Створюється Робоча група з питань захисту осіб стосовно обробки персональних даних, далі - "Робоча група".

Вона має консультативний статус і діє незалежно.

2. Робоча група складається з представника наглядового органу або органів, призначених кожною з Держав-членів, представника органу чи органів, створених установами та органами Співтовариства, і представника Комісії. Кожен член Групи призначається установою, органом або органами, який він представляє. Якщо Держава-член призначає більше одного наглядового органу, то вони призначають спільного представника. Таким же чином діють органи, створені установами і органами Співтовариства.

3. Робоча група приймає свої рішення простою більшістю представників контрольних органів.

4. Робоча група обирає свого голову. Мандат голови має тривалість два роки. Мандат може отримуватися вдруге.

5. Комісія забезпечує роботу секретаріату Робочої групи.

6. Робоча група приймає свій внутрішній регламент.

7. Робоча група вивчає справи, включені до порядку денного головою як з його власної ініціативи, так і на прохання представника наглядових органів або Комісії.

Стаття 30

1. Робоча група має такі обов’язки:

a) вивчати всі питання, що стосуються правильного застосування національних положень, прийнятих на виконання цієї Директиви з метою їх однакового застосування;

b) давати Комісії висновок про рівень захисту у межах Співтовариства і в третіх країнах;

c) надавати консультації Комісії щодо подальших змін цієї Директиви, будь-яких додаткових чи спеціальних заходів, які повинні прийматися з метою забезпечення прав і свобод фізичних осіб стосовно обробки персональних даних, а також щодо проектів інших заходів Співтовариства, що торкаються цих прав і свобод;

d) давати висновок про кодекси поведінки, розроблені на рівні Співтовариства.

2. Якщо Робоча група виявляє наявність розбіжностей між законодавством і практикою Держав-членів, які можуть вплинути на рівноцінність захисту осіб стосовно обробки персональних даних у Співтоваристві, вона повідомляє про це Комісію.

3. Робоча група може за власною ініціативою готувати рекомендації щодо будь-якої справи, яка стосується захисту осіб стосовно обробки персональних даних у Співтоваристві.

4. Висновки і рекомендації Робочої групи передаються Комісії і Комітету, про який ідеться в статті 31.

5. Комісія інформує Робочу групу про дії, які були вчинені для реагування на висновки та рекомендації. З цією метою готується доповідь, яка передається також у Європейський парламент і Раду. Доповідь доводиться до відома громадськості.

6. Робоча група готує щорічну доповідь про стан захисту фізичних осіб стосовно обробки персональних даних у Співтоваристві та третіх країнах і передає його Комісії, Європейському парламенту і Раді.. Доповідь доводиться до відома громадськості.

Розділ VII Заходи Співтовариства на виконання

Стаття 31.

Комітет

1. Комісії надається допомога Комітетом, який складається з представників Держав-членів і в якому головує представник Комісії.

2. Представник Комісії подає на розгляд Комітету проекти нормативних актів, які треба прийняти. Комітет надсилає висновок про цей проект у строк, який може бути визначений головою залежно від терміновості питання, що розглядатиметься.

Висновок затверджується більшістю, про яку ідеться у пункті 2 Статті 148 Договору. Голоси представників Держав-членів у Комітеті враховуватимуться в порядку, встановленому в статті, яка щойно зазначалась. Голова не бере участі в голосуванні.

Комісія вживає заходів, які мають втілюватися негайно. Проте, якщо ці заходи не відповідають висновку Комітету, про них без зволікання Комісія повідомляє Раді. У цьому випадку:

- Комісія відкладає застосування заходів, які передбачено прийняттям рішення, на три місяці з дати такого повідомлення;

- Рада, яка діє за принципом кваліфікованої більшості, може прийняти відмінне рішення протягом періоду, зазначеного в першому пункті.

Кінцеві положення

Стаття 32

1. Держави-члени приймають законодавчі, регулятивні й адміністративні положення, необхідні для виконання положень цієї Директиви, не пізніше, як в кінці третього року з дати її прийняття.

При прийнятті цих положень Держави-члени посилаються на цю Директиву або супроводжують їх офіційну публікацію таким посиланнями. Держави-члени самі встановлюють форми таких посилань.

2. Держави-члени стежать за тим, аби будь-яка обробка, вже розпочата на дату набуття чинності положеннями національного права, прийнятими на виконання цієї Директиви, була приведена у відповідність з цими положеннями впродовж трирічного терміну від цієї дати.

Як виняток з викладеного в першому абзаці, Держави-члени можуть встановити, що обробка даних, які знаходяться в ручних файлових системах на дату набрання чинності

національними положеннями, прийнятими на виконання цієї Директиви, були приведені у відповідність з положеннями статей 6, 7 і 8 протягом дванадцятирічного періоду з моменту її прийняття. Проте Держави-члени надають суб'єктові даних за його запитом під час реалізації права доступу, виправлення, знищення або блокування даних, які є неповними, неточними або зберігаються у формі, несумісній з законними цілями, яким слідує контролер.

3. Як виняток з викладеного в пункті 2, Держави-члени можуть передбачити, що за наявності адекватних гарантій дані, що зберігаються виключно для історичних досліджень, не потребують узгодження зі статтями 6, 7 і 8 цієї Директиви.

4. Держави-члени повідомляють Комісії текст положень внутрішнього законодавства, які будуть прийняті у сфері, що регулюється цією Директивою.

Стаття 33

Комісія представляє Раді і Європейському парламенту періодично, а вперше - в трирічний термін від дати, зазначеної в пункті 1 статті 32, доповідь про застосування цієї Директиви, додаючи в разі потреби пропозиції щодо змін. Доповідь доводиться до відома громадськості.

Комісія вивчає зокрема застосування цієї Директиви до обробки даних, які складаються зі звуків і зображень, що стосуються фізичних осіб, представляє для розгляду відповідні пропозиції, які можуть бути необхідними у зв'язку з прогресом у розвитку інформаційних технологій та станом розвитку інформаційного суспільства.

Стаття 34

Одержувачами цієї Директиви є Держави-члени. Зроблено в Люксембурзі 24 жовтня 1995 року

За Європейський парламент	За Раду
Пан Президент	Пан Президент
K. HÄNSCH	L. ATIENZA SERNA

1. Official Journal. - 1990. - # C 277. - P. 3; Official Journal. - 1992. - # C 3. - P. 30
2. Official Journal. – 1991. - # C 159. - P. 38.
3. Висновок Європейського Парламенту від 11 березня 1992 року // Official Journal. - 1992. - # C 94. - P. 198; підтверджений 2 грудня 1993 року // Official Journal. - 1993. - # C 342. - P. 30; Спільна позиція Ради від 20 лютого 1995 року // Official Journal. - 1995. - # C 93. – P. 1; і Рішення Європейського Парламенту від 15 червня 1995 року // Official Journal. - 1995. - # C 166.
4. Official Journal. - 1987. - # L 197. - P. 33.