



Правовые рамки защиты персональных данных в Беларуси 2016

ПРОЕКТ РЕКОМЕНДАЦИЙ

(презентован 9 декабря 2015, текст дополнен по сост. на май 2016)

Минск, 3 декабря 2015 г.

Документ **“Правовые рамки защиты персональных данных в Беларуси 2016: проект рекомендаций”** подготовлен в рамках программы “Доступ к информации” Просветительского учреждения “Центр правовой трансформации” (Lawtrend).

Программа включает три исследовательских компонента:

- 1) право на информацию, доступ к информации онлайн;
- 2) защита персональных данных;
- 3) свободный интернет.

Просветительское учреждение «ЦЕНТР ПРАВОВОЙ ТРАНСФОРМАЦИИ» (LAWTREND) — некоммерческая организация, целью которой является повышение правовой культуры, организация просветительской, аналитической и исследовательской деятельности в области права.

Задачи Lawtrend:

- содействие повышению роли права;
- содействие повышению правовой культуры;
- содействие имплементации международного права;
- пропаганда общепризнанных принципов международного права; содействие развитию правового сообщества и правовых технологий.

Методы деятельности:

консультирование; стратегические судебные тяжбы; аналитическая деятельность; мониторинговые исследования.

Экспертные направления Lawtrend:

1. Свобода ассоциаций;
2. Свобода информации; право на информацию;
3. Доступ к правосудию; право на справедливый суд; право на юридическую помощь.

Координатор Программы “Доступ к информации”: Елена ТОНКАЧЕВА, Председатель правления Центра правовой трансформации (Lawtrend)

Автор: Ольга ДЕМЬЯН, магистр права, юрист, краткосрочный консультант, Lawtrend

Консультант, редактор русскоязычной версии: Алексей КОЗЛЮК, юрист, эксперт Lawtrend

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	4
I. ОБЗОР ЕВРОПЕЙСКОГО ПРАВА В ОБЛАСТИ ЗАЩИТЫ ДАННЫХ	5
1.1. Определение ключевых понятий	7
1.2. Ключевые принципы европейского права в области защиты данных.....	10
1.3. Надзорные органы в области защиты данных	11
1.4. Права субъектов	12
1.5. Передача персональных данных третьим странам или международным организациям.....	12
1.6. Защита персональных данных в отдельных сферах	13
1.7. Уведомление о нанесении ущерба персональным данным	15
II. НОРМАТИВНАЯ БАЗА БЕЛАРУСИ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ	16
III. КРАТКОЕ ОПИСАНИЕ ПРЕДЛОЖЕНИЙ, КАСАЮЩИХСЯ БАЗОВОГО ЗАКОНА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ	17
3.1. Рекомендации по структуре базового закона о защите персональных данных:.....	17
ЗАКЛЮЧЕНИЕ	21

ВВЕДЕНИЕ

Интернет обеспечил беспрецедентный уровень возможностей взаимодействия и самовыражения. Персональные данные превратились в актив как для бизнеса, так и для государственного сектора. Сбор, агрегирование и анализ данных зачастую представляют собой значимый элемент их деятельности.

Чтобы гарантировать физическим лицам высокий уровень защиты персональных данных необходимо реформирование сферы защиты данных, а именно установление четких, технологически нейтральных правил, обеспечивающих юридическую определенность и снижающих административную нагрузку. Это ведет к росту доверия, стимулированию экономического роста, созданию новых рабочих мест и содействию инновациям.

В настоящем документе рассматриваются ключевые проблемы защиты персональных данных. В нем собраны примеры передовой практики в сфере европейского права в области защиты персональных данных (Европейский союз и Совет Европы). Документ предназначен для использования в качестве справочного пособия для участников процесса анализа и разработки нормативной базы в области защиты персональных данных. В первой главе дан общий обзор европейской нормативной базы в области защиты персональных данных. Вторая глава включает в себя некоторые комментарии действующего законодательства. В третьей главе содержится краткое описание предложений, касающихся базового закона о защите данных.

I. ОБЗОР ЕВРОПЕЙСКОГО ПРАВА В ОБЛАСТИ ЗАЩИТЫ ДАННЫХ

1. Данная глава посвящена европейскому законодательству о защите персональных данных. В качестве лучших практик приведен краткий обзор ключевых правовых актов, которые устанавливают и гарантируют право на уважение частной жизни и на защиту персональных данных.

2. Право на защиту персональных данных – составной элемент права на уважение личной и семейной жизни, жилища и корреспонденции, сформулированного в п. 1 статьи 8 Европейской конвенции по правам человека (ЕКПЧ)¹. Чтобы считаться не противоречащим ЕКПЧ, любое вмешательство в осуществление прав, охраняемых п. 1 статьи 8, должно отвечать критериям, перечисленным в п. 2 статьи 8².

3. Еще один юридически обязательный международный документ в области защиты данных – Конвенция о защите физических лиц при автоматизированной обработке персональных данных ("Конвенция № 108")³. Она открыта для присоединения со стороны государств, не являющихся членами Совета Европы.

4. С целью дальнейшего развития сформулированных в Конвенции № 108 общих принципов и правил Комитет министров Совета Европы принял ряд рекомендаций⁴. Они не носят юридически обязательного характера, однако задают определенное направление.

5. За период своей судебной практики⁵ Европейский суд по правам человека (ЕСПЧ) изучил множество ситуаций, в которых возникали проблемы с защитой данных, в том числе ситуаций, касающихся перехвата информации⁶, различных форм слежки⁷, а также предотвращения хранения персональных данных государственными органами⁸.

6. Хартия Европейского союза об основных правах, которая является юридически обязательным актом первичного права, гарантирует уважение частной и семейной жизни (статья 7) и устанавливает право на защиту данных (статья 8)⁹, недвусмысленно поднимая уровень такой защиты до уровня основополагающего права в рамках законодательства ЕС.

¹ С текстом ЕКПЧ можно ознакомиться здесь: <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>

² Сборник "Прецедентное право на основании решений Европейского суда по правам человека в отношении защиты персональных данных" (2013) доступен по ссылке:

www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP_2013_Case_Law_Eng_FINAL.pdf

³ С более подробной информацией о процессе совершенствования положений Конвенции № 108 можно ознакомиться здесь: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

⁴ Перечень рекомендаций в области защиты персональных данных см. здесь:

http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp

⁵ Справочная публикация "Защита персональных данных" (2014) (http://www.echr.coe.int/Documents/FS_Data_ENG.pdf)

⁶ См., например: ЕСПЧ, иск Мэлоуна к Великобритании, № 8691/79, 2 августа 1984 г.; ЕСПЧ, иск Копланд к Великобритании, № 62617/00, 3 апреля 2007 г.

⁷ См., например: ЕСПЧ, иск Класса и др. к ФРГ, № 5029/71, 6 сентября 1978 г., иск Уцуна к ФРГ, № 35623/05, 2 сентября 2010 г.

⁸ См., например: ЕСПЧ, иск Леандера к Швеции, № 9248/81, 26 марта 1987 г.; иск С. и Марпера к Великобритании, №№ 30562/04 и 30566/04, 4 декабря 2008 г.

⁹ С текстом Хартии ЕС об основных правах можно ознакомиться по ссылке:

http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm

7. Была принята Директива 95/46/ЕС для раскрытия содержания принципов права на неприкосновенность частной жизни, к тому времени уже изложенных в Конвенции № 108 (статья 5), и их детализации¹⁰. Любые изъятия из данных принципов или ограничения их применения "могут приниматься на национальном уровне¹¹; они должны предусматриваться законодательством, преследовать законную цель и являться необходимой в демократическом обществе мерой".¹²

8. Как и ЕСПЧ, Суд Европейского союза (СЕС) указал, что при применении и трактовании положений статьи 8 ЕКПЧ и статьи 8 Хартии ЕС об основных правах необходимо руководствоваться принципом сбалансированного осуществления права, не препятствующего осуществлению иных прав.¹³

9. Нормативная база в области защиты персональных данных находится в процессе фундаментального реформирования в целях "более совершенного реагирования на вызовы, возникающие в результате стремительного развития новых технологий (в частности онлайн-технологий) и растущей глобализации, сохраняя при этом технологический нейтралитет нормативной базы".¹⁴

10. Согласно текущей редакции Общего регламента о защите данных новые юридические нормы должны применяться: (1) к обработке персональных данных в контексте деятельности контролера или обработчика данных в ЕС; (2) к обработке персональных данных проживающих в ЕС субъектов данных контролером данных, находящимся за пределами ЕС, если деятельность по обработке данных связана с (а) предложением товаров или услуг подобным находящимся в ЕС субъектам данных или (б) мониторингом их поведения; (3) к обработке персональных данных контролером данных, находящимся за пределами ЕС, однако в месте, на которое в силу публичного международного права распространяется национальное право государства-члена ЕС.

11. Следует отметить различие между защитой персональных данных и правом на приватность. Это иллюстрируется следующим образом: "согласно первому из них меры контроля *ex ante* применяются к обработке персональных данных вне зависимости от того, носит ли информация частный характер или нет, в то время как вопрос

¹⁰ Справочник по европейскому праву в области защиты данных, EU FRA (2014) (http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf)

¹¹ Статья 9(2), Конвенция № 108; статья 13(2), Директива 95/46/ЕС

¹² Справочник по европейскому праву в области защиты данных, EU FRA (2014) (http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf)

¹³ При рассмотрении объединенных дел C-92/09 и C-93/09, иск товарищества Фолькера и Маркуса Шеке и иск Хартмута Айферта к земле Гессен, 9.11.2010, СЕС указал, что данное право "не является, тем не менее, безусловным, а должно рассматриваться относительно его функции в обществе" (§ 48). См. также: ЕСПЧ, иск принца Ганноверского к ФРГ (№ 2) [GC], №№ 40660/08 и 60641/08, 7 февраля 2012 г.; СЕС, объединенные дела C-468/10 и C-469/10, иск Национальной ассоциации финансово-кредитных учреждений (ASNEF) и Федерации электронной коммерции и прямого маркетинга (FECOMD) к Правительству Испании, 24 ноября 2011 г., § 48; СЕС, C-275/06, иск Ассоциации производителей музыкальной продукции Испании (Promusicae) к компании Telefónica de España SAU, 29 января 2008 г.

¹⁴ Заключение № 168 от 1 декабря 2009 г. Рабочей Группы статьи 29 "Будущее неприкосновенности частной жизни. Объединенная реакция на консультации Европейской комиссии по нормативной базе в области осуществления основополагающего права на защиту персональных данных" (стр. 3) (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf)

неприкосновенности частной жизни как предмета неправомерного обращения возникает *ex post* – после возникновения злоупотребления или его ожидания".¹⁵

1.1. ОПРЕДЕЛЕНИЕ КЛЮЧЕВЫХ ПОНЯТИЙ

А. ОПРЕДЕЛЕНИЕ ПОНЯТИЯ "ПЕРСОНАЛЬНЫЕ ДАННЫЕ"

12. Согласно Директиве 95/46/ЕС "персональные данные означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу (субъекту данных)".¹⁶

13. Тщательный анализ понятия "персональные данные" с множеством примеров приведен в Заключении 4/2007¹⁷. Особое внимание уделено четырем главным элементам определения: "любая информация", "относящийся к", "идентифицированный или идентифицируемый", "физическое лицо". Согласно этому документу, чтобы определить, идет ли в той или иной конкретной ситуации речь о "персональных данных" или нет, необходимо оценить каждый из элементов. Они могут выступать в качестве ориентира при анализе понятия защиты персональных данных.

14. По мнению Рабочей Группы статьи 29 (далее РГ ст. 29)¹⁸, определение понятия "персональные данные" отражает стремление европейского законодателя к широкому пониманию "персональных данных", сохранявшееся на протяжении всего законодательного процесса; "как и в Конвенции № 108, принято широкое определение с целью охвата всей информации, которую можно связать с физическим лицом"¹⁹.

15. Персональные данные – понятие гораздо более широкое, чем информация, по которой можно непосредственно идентифицировать человека, такой как имя²⁰, национальный регистрационный номер или учетный номер налогоплательщика. По мнению СЕС, например, понятие персональных данных среди прочего включает в себя информацию, касающуюся вознаграждения²¹, биометрическую информацию²², адреса IP²³, данные о трафике и местонахождении²⁴, размер заработанного или незаработанного

¹⁵ Computer Law: The Law and Regulation of Information Technology, под ред. Криса Рида и Джона Эйнджела, Oxford University Press, 6-е издание, стр. 463

¹⁶ Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите физических лиц при обработке персональных данных и о свободном движении таких данных

¹⁷ Заключение Рабочей Группы статьи 29 4/2007 о понятии персональных данных от 20 июня 2007 г. (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf)

¹⁸ Рабочая группа статьи 29 сформирована согласно положениям Директивы 95/46/ЕС. Как предусмотрено статьей 29 данной директивы, "она имеет статус консультативного органа и действует в качестве независимой структуры".

¹⁹ См. итоговый документ СОМ (90) 314, 13.9.1990, стр. 19 (комментарий к статье 2)

²⁰ Об этом упоминается в тексте "контрольного перечня основополагающих прав", предложенного в рамках Стратегии Европейской комиссии по эффективной реализации Хартии Европейского союза об основных правах, СОМ(2010) 573

²¹ Пункты (а) и (б) статьи 2 как Директивы 95/46/ЕС, так и Регламента 45/2001

²² См., например, дело С-291/12, иск Шварца к г. Бохуму, решение суда от 17 октября 2013 г., § 27

²³ См., например, дело С-70/10, иск компании Scarlet Extended к Бельгийской ассоциации авторов, композиторов и издателей (SABAM), решение суда от 24 ноября 2011 г., § 51

²⁴ Digital Rights Ireland, § 26 и 29

дохода и активов физических лиц²⁵, периоды работы в течение дня, периоды отдыха и соответствующие перерывы и интервалы²⁶.

16. В текущей версии проекта Общего регламента о защите данных "персональные данные" определяются как "любая информация, относящаяся к субъекту данных"²⁷.

В. ОПРЕДЕЛЕНИЕ "ЧУВСТВИТЕЛЬНЫХ ДАННЫХ"

17. В рамках права в области защиты данных "особым категориям данных"²⁸ предоставляется более высокий уровень защиты. К ним относятся данные, "которые по своей природе способны привести к нарушению основополагающих свобод или неприкосновенности частной жизни".²⁹ Соответствующие механизмы защиты включают в себя требования к контролерам данных³⁰, обязывающие их получать явное, а не предполагаемое согласие, усилить предпринятые меры безопасности и (или) еще более ограничить перечень допустимых типов обработки данных³¹.

18. Как в Конвенции № 108 (статья 6), так и в Директиве 95/46/ЕС (статья 8) в определении чувствительных данных упоминаются следующие категории:

- персональные данные, дающие представление о расовом или этническом происхождении;
- персональные данные, дающие представление о политических взглядах, религиозных или иных убеждениях;
- персональные данные, касающиеся здоровья и половой жизни.

19. В Директиве 95/46/ЕС дополнительно указывается "членство в профессиональных союзах", и предоставляются полномочия государствам-членам ЕС "устанавливать условия, при которых может подвергаться обработке национальный идентификационный номер или любой иной идентификатор общего применения" (п. 7 статьи 8).

20. Согласно Конвенции № 108 чувствительными данными также считаются персональные данные, касающиеся уголовной судимости.

²⁵ См., например, дело C-73/07 по иску против компаний Satakunnan Markkinapörssi и Satamedia, решение суда от 16 декабря 2008 г., § 35 и § 37

²⁶ См., например, дело C-342/12 по иску компании Worten к Португальскому управлению по условиям труда (ACT), решение суда от 30 мая 2013 г., § 19

²⁷ См. текст проекта: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

²⁸ Чувствительными данными считаются следующие категории персональных данных: "персональные данные, дающие представление о расе или этническом происхождении, политических взглядах, религиозных или иных убеждениях, членстве в профессиональных союзах, генетические данные или данные, касающиеся здоровья или половой жизни"

²⁹ Директива 95/46/ЕС, п. 33 Преамбулы

³⁰ Как само понятие контролера данных (data controller), так и его взаимосвязь с понятием обработчика данных (data processor) играют решающую роль в применении Директивы 95/46/ЕС, поскольку ими определяется, кто обязан отвечать за соблюдение правил защиты данных, каким образом субъекты данных могут осуществлять свои права, какой применим национальный закон и насколько эффективно могут функционировать органы по защите данных (Data Protection Authorities). Заключение 1/2010 от 8.02.2010 РГ ст. 29 содержит подробный анализ понятий "контролер" и "обработчик" (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)

³¹ Директива 95/46/ЕС, статья 8

С. ОПРЕДЕЛЕНИЕ "КОНТРОЛЕРА" И "ОБРАБОТЧИКА"

21. Термин "контролер" определен п. (d) статьи 2 Директивы 95/46/ЕС и п. (d) статьи 2 Конвенции № 108. Правовая база ЕС включает в себя тщательный анализ данного понятия с приведением многочисленных примеров, например, в Заключении 1/2010 РГ ст. 29. В частности, в нем при анализе данного понятия оно поделено на "три главных составляющих", а именно: (1) "персональный аспект (*"физическое или юридическое лицо, государственный орган, организация или любой иной орган"*); (2) возможность плюралистического контроля (*"которое(ый) самостоятельно или совместно с другими"*); (3) существенные элементы, отличающие контролера от других действующих лиц (*"определяет цели и средства обработки персональных данных"*)³².

22. По сравнению с действующим регулированием в текущий проект Общего регламента о защите данных включены новые обязательства контролера, в том числе «вытекающие из принципов проектируемой защиты персональных данных и защиты по умолчанию (by design and by default)». Кроме того, проект "разъясняет обязанности объединенных контролеров в части их взаимоотношений как внутренних, так и с субъектом данных".

23. Термин "обработчик" определен п. (e) статьи 2 Директивы 95/46/ЕС. По мнению РГ ст. 29, "два базовых условия квалификации в качестве обработчика – это, с одной стороны, представлять собой отдельное юридическое лицо по отношению к контролеру, а, с другой стороны, обрабатывать персональные данные от его имени"³³. См. также главу IV Общего регламента о защите данных. В рамках права Совета Европы суть данного понятия разъяснена в рекомендациях³⁴.

Д. ОПРЕДЕЛЕНИЕ "СОГЛАСИЯ"

24. Согласие является одним из законных оснований обработки персональных данных. Данный термин определен, например, в п. (h) статьи 2 Директивы 95/46/ЕС и "означает любое свободно данное конкретное и информированное выражение своих желаний, которым субъект данных обозначает свое согласие с выполняемой обработкой относящихся к нему персональных данных". В своих заключениях РГ ст. 29 пояснило данное понятие³⁵ и представила дальнейшие указания, касающиеся получения согласия

³² Заключение 1/2010 о понятиях "контролера" и "обработчика" от 16.02.2011 РГ ст. 29 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf)

³³ Заключение 1/2010 о понятиях "контролера" и "обработчика" от 16.02.2011 РГ ст. 29 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf)

³⁴ Например, Рекомендация по статистическим данным, стр. 6 (https://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompil_en.pdf)

³⁵ Заключение 15/2011 об определении понятия согласия от 13 июля 2011 г. РГ ст. 29 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf)

на использование файлов "cookies"³⁶. Кроме того, понятие согласия объясняется в нескольких рекомендациях Совета Европы³⁷.

Е. ИНЫЕ ПОНЯТИЯ, ОПРЕДЕЛЕННЫЕ В ПРОЕКТЕ РЕГЛАМЕНТА ЕС О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

25. В текущую версию проекта Общего регламента о защите данных включены определения из Директивы 95/46/ЕС, определения, измененные или дополненные новыми элементами, либо определения, вводимые впервые ("ущерб персональным данным" на основе п. (h) статьи 2 Директивы 2002/58/ЕС о неприкосновенности частной жизни в сфере электронной коммуникации³⁸ с изменениями, внесенными Директивой 2009/136/ЕС³⁹, "генетические данные", "биометрические данные", данные, касающиеся здоровья", "главное учреждение", "представитель", "предприятие", "группа предприятий", "юридически обязательные корпоративные правила", определение понятия "ребенок" на основе Конвенции ООН о правах ребенка⁴⁰, "надзорный орган")⁴¹.

26. См. Приложение 1 к данному документу, в которое включены определения соответствующих понятий, взятые из различных правовых документов.

1.2. КЛЮЧЕВЫЕ ПРИНЦИПЫ ЕВРОПЕЙСКОГО ПРАВА В ОБЛАСТИ ЗАЩИТЫ ДАННЫХ

27. По мнению РГ ст. 29⁴², главные принципы защиты данных "следует положить в основу всеобъемлющей нормативной базы", а нижеприведенные принципы следует провозгласить повторно:

- правомерность;
- справедливость;
- соразмерность;
- ограничение относительно цели;

³⁶ Рабочий документ 02/2013 с методическими указаниями по получению согласия на использование файлов "cookies" от 2.10.2013 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf)

³⁷ См., например, Рекомендацию Совета Европы по статистическим данным

³⁸ Директива 2002/58/ЕС Европейского парламента и Совета от 12 июля 2002 г. об обработке персональных данных и охране неприкосновенности частной жизни в сфере электронной связи (Директива о неприкосновенности частной жизни и электронной связи) OJ L 201, 31/07/2002, стр.37

³⁹ Директива 2009/136/ЕС Европейского парламента и Совета от 25 ноября 2009 г. о внесении изменений в Директиву 2002/22/ЕС о всеобщем обслуживании и правах пользователей, касающихся электронных коммуникационных сетей и сервисов; Директива 2002/58/ЕС об обработке персональных данных и охране неприкосновенности частной жизни в сфере электронной связи; Регламент (ЕС) № 2006/2004 о сотрудничестве между национальными органами власти, отвечающими за принудительное исполнение законов в области защиты потребителей; OJ L 337, 18.12.2009, стр. 11

⁴⁰ Принята Резолюцией 44/25 от 20.11.1989 Генеральной Ассамблеи ООН и открыта для подписания, ратификации и присоединения

⁴¹ Предложение о принятии Регламента Европейского парламента и Совета о защите физических лиц при обработке персональных данных и о свободном движении таких данных (Общий регламент о защите данных) (http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)

⁴² Данная рабочая группа сформирована согласно положениям статьи 29 Директивы 95/46/ЕС. Она представляет собой независимый европейский консультативный орган в области защиты данных и неприкосновенности частной жизни. Ее задачи описаны в статье 30 Директивы 95/46/ЕС и статье 15 Директивы 2002/58/ЕС

- прозрачность, права субъекта данных;
- а также независимый надзор со стороны государственных органов⁴³.

28. В новой нормативной базе в области защиты персональных данных эти принципы должны быть сохранены. Они в большей степени идентичны соответствующим принципам, изложенным в Резолюциях (73) 2244 и (74) 2945, повторены в Конвенции № 108⁴⁶ и далее включены в нормативную базу в области защиты данных⁴⁷ Европейского союза в целом и государств-членов ЕС в частности.

29. Согласно Конвенции № 108, допускаются лишь те изъятия из базовых принципов защиты данных, которые обусловлены необходимостью защиты фундаментальных ценностей того или иного демократического общества.⁴⁸

30. Текущая версия проекта Регламента о защите данных включает в себя следующие новые элементы:

- принцип прозрачности;
- разъяснение принципа минимизации данных;
- установление всесторонних обязанностей и юридической ответственности контролера (р.3.4.2)⁴⁹.

1.3. НАДЗОРНЫЕ ОРГАНЫ В ОБЛАСТИ ЗАЩИТЫ ДАННЫХ

31. Дополнительным протоколом Конвенции № 108 предусматривается учреждение национальных надзорных органов, отвечающих за обеспечение соблюдения законодательных и нормативных актов, принятых во исполнение Конвенции № 108.

32. Подобные надзорные органы в области защиты данных обеспечивают надлежащие средства правовой защиты, при условии что они обладают эффективными полномочиями и пользуются подлинной независимостью при исполнении своих обязанностей. Они стали неотъемлемым компонентом действующей в демократическом обществе системы надзора в области защиты данных. В большинстве стран, в которых приняты законы о защите данных, учреждены надзорный орган⁵⁰, комиссар (например, в Венгрии⁵¹),

⁴³ "Будущее неприкосновенности частной жизни. Объединенная реакция на консультации Европейской комиссии по нормативной базе в области осуществления основополагающего права на защиту персональных данных" – заключение РГ ст. 29 от 1.12.2009 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf)

⁴⁴ <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=589402&SecMode=1&DocId=646994&Usage=2>

⁴⁵ <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2>

⁴⁶ <http://www.coe.int/ro/web/conventions/full-list/-/conventions/treaty/108>

⁴⁷ <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046>

⁴⁸ <http://www.coe.int/ro/web/conventions/full-list/-/conventions/treaty/108>

⁴⁹ http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

⁵⁰ См. перечень надзорных органов государств-членов ЕС: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm and data protection authorities in the CoE Member States http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/National_laws_en.asp

⁵¹ См. <http://www.naih.hu/>

комиссия (например, в Люксембурге⁵²), омбудсмен (например, в Финляндии⁵³) или инспекция (например, в Эстонии⁵⁴)(§5).⁵⁵

1.4. ПРАВА СУБЪЕКТОВ

33. В соответствии с европейской правовой базой в области защиты персональных данных физические лица в рамках национального законодательства имеют право запрашивать у любого контролера данных информацию о том, обрабатывает ли данный контролер его данные, а именно:

- получать доступ к своим собственным данным у любого контролера, которых обрабатывает такие данные;
- требовать от контролера, обрабатывающего их данные, исправления своих данных (и их блокировки по мере такой необходимости), если такие данные недостоверны.
- требовать от контролера удаления или блокировки своих данных по мере такой необходимости, если контролер обрабатывает их данные незаконно.

34. Кроме того, субъекты данных вправе отказывать контролерам в отношении:

- автоматических решений (принимаемых с использованием персональных данных, обрабатываемых исключительно автоматизированными средствами);
- обработки их данных, если это ведет к несоизмеримым результатам;
- использования их данных в целях прямого маркетинга.

35. Проект Общего регламента о защите данных вводит новые элементы (глава III)⁵⁶. Например, проектом вводится понятие "право быть забытым". Данный вопрос, в частности, рассматривался СЕС в рамках дела C-131/12 по иску компании Google Spain and Inc к Испанскому агентству по защите данных (AEPD) и Марио Костеха Гонсалесу. ПГ ст. 29 дает методические рекомендации по претворению в жизнь данного судебного решения в своем Заключении от 26.11.2014⁵⁷.

1.5. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ СТРАНАМ ИЛИ МЕЖДУНАРОДНЫМ ОРГАНИЗАЦИЯМ

36. Директива предусматривает возможность передачи персональных данных странам, не входящим в состав ЕС, только при условии гарантированного адекватного уровня защиты.

37. В решении СЕС от 6 октября 2015 г. по делу C-362/14 (*Шремз*)⁵⁸ еще раз провозглашается важность соблюдения основополагающего права на защиту

⁵² См. <http://www.cnpd.lu/>

⁵³ См. <http://www.tietosuoja.fi/en/>

⁵⁴ См. <http://www.aki.ee/en/inspectorate>

⁵⁵ Пояснительная записка – ETS 181 – Автоматическая обработка данных (Протокол) (<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce56>)

⁵⁶ http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

⁵⁷ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

⁵⁸ СЕС объявил, что "решение, основанное на оговорке, является недействительным. Из настоящего постановления вытекает обязательство ирландского надзорного органа со всей тщательностью изучить

персональных данных, закрепленного в Хартии Европейского союза об основных правах, в том числе при передаче таких данных за пределы ЕС.

38. Через месяц, 6.11.2015, Европейская комиссия издала указания⁵⁹ по трансатлантической передаче данных и призвала к скорейшему установлению новых правовых рамок вслед за решением по делу *Шремза*⁶⁰.

39. В своем заявлении⁶¹ РГ ст. 29 "настаивает на разделении обязанностей между органами по защите данных, учреждениями ЕС, государствами-членами ЕС и коммерческими организациями по поиску устойчивых решений по претворению в жизнь постановления Суда". В частности, в контексте постановления "коммерческим организациям следует задуматься о возможных рисках, которые они несут при передаче данных и рассмотреть вопрос своевременного внедрения тех или иных правовых и технических решений для смягчения данных рисков и уважения накопленного правового достояния ЕС в области защиты данных".

40. Представляется важным напомнить, что согласно действующим правовым нормам Европейская комиссия "может установить, что третья страна обеспечивает адекватный уровень защиты". В этом случае персональные данные могут передаваться из государств-членов ЕС без необходимости получения дополнительных гарантий.⁶²

41. Согласно Протоколу № 181 Конвенции № 108⁶³ цель соответствующих правовых положений – согласовать требования действующих норм в области защиты данных с принципом свободного движения информации невзирая на границы, закрепленного статьей 10 ЕКПЧ. Более того, тем же правовым документом предусматривается, что данные могут передаваться только в случае, если получатель – государство или международная организация – в состоянии обеспечить адекватный уровень защиты.⁶⁴

1.6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОТДЕЛЬНЫХ СФЕРАХ

42. Электронная связь:

жалобу г-на Шремза и принять решение, следует ли согласно положениям директивы приостановить передачу в США данных европейских подписчиков Facebook на основании того, что данная страна не может обеспечить адекватный уровень защиты персональных данных".

(<http://curia.europa.eu/juris/documents.jsf?num=C-362%2F>)

⁵⁹ COM(2015) 566 от 6.11.2015 "О передаче персональных данных из ЕС в Соединенные Штаты Америки согласно Директиве 95/46/ЕС вследствие принятия Судом ЕС постановления по делу C-362/14 (Шремз)(http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf)

⁶⁰ http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

⁶¹ http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

⁶² П.п. 2, 5 и 8 преамбулы к Решению 2000/520, принятому Европейской комиссией на основании п. 6 статьи 25 Директивы 95/46/ЕС

⁶³ <http://www.coe.int/ro/web/conventions/full-list/-/conventions/treaty/108>

⁶⁴ Пояснительная записка – ETS 181 – Автоматическая обработка данных (Протокол)

(<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce56>)

- Директива 2002/58/ЕС⁶⁵
- Конвенция № 108
- Рекомендация по услугам электросвязи⁶⁶

43. Трудовые отношения:

- Директива 95/46/ЕС, статья 8(2) (b)
- Конвенция № 108
- Рекомендация по трудовым отношениям⁶⁷

44. Медицинские данные:

- Директива 95/46/ЕС, статья 8(3)
- Конвенция № 108
- Рекомендация по медицинским данным⁶⁸

45. Статистика:

- Директива 95/46/ЕС, статья 6(1) (b) и (e), статья 13(2)
- Регламент № 223/2009 о европейской статистике
- Конвенция № 108
- Рекомендация по статистическим данным⁶⁹

46. Финансовые данные:

- Директива 2004/39/ЕС о рынках финансовых инструментов⁷⁰
- Регламент № 648/2012 о внебиржевых производных ценных бумагах, центральных контрагентах и торговых репозиториях⁷¹
- Регламент № 1060/2009 о кредитно-рейтинговых агентствах⁷²
- Директива 2007/64/ЕС о платежных услугах на внутренних рынках⁷³
- Заключение РГ ст. 29⁷⁴
- Конвенция № 108

⁶⁵ Директива 2002/58/ЕС Европейского парламента и Совета от 12 июля 2002 г. об обработке персональных данных и охране неприкосновенности частной жизни в сфере электронной связи (Директива о неприкосновенности частной жизни и электронной связи) OJ L 201, 31/07/2002

⁶⁶ Совет Европы, Комитет министров (1995 г.), Рекомендация Rec(95)4 государствам-членам о защите персональных данных в области услуг электросвязи с особым вниманием к услугам телефонной связи, 7 февраля 1995 г.

⁶⁷ <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=276592&SecMode=1&DocId=699842&Usage=2>

⁶⁸ Совет Европы, Комитет министров (1997 г.), Рекомендация Rec(97)5 государствам-членам о защите медицинских данных, 13 февраля 1997 г.

⁶⁹ Рекомендация Rec(97)18 Совета Европы государствам-членам о защите персональных данных, собираемых и обрабатываемых в статистических целях, 30 сентября 1997 г.

⁷⁰ <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0039&from=en>

⁷¹ <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0648&from=EN>

⁷² <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:302:0001:0031:EN:PDF>

⁷³ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:en:PDF>

⁷⁴ Заявление РГ ст. 29 от 4.02.2015 об автоматическом межгосударственном обмене персональными данными в целях налогообложения (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp230_en.pdf)

- Рекомендация 90/19 о защите персональных данных, используемых для осуществления оплаты и других связанных с оплатой операций⁷⁵

47. Защита данных в контексте правоохранительных органов и уголовного правосудия

- Рекомендация Совета Европы по правоохранительным органам⁷⁶
- Конвенция Совета Европы о киберпреступности⁷⁷
- Конвенция Совета Европы № 108
- РГ ст. 29⁷⁸
- Проект директивы⁷⁹

48. Важно также отметить Регламент (EU) № 910/2014 Европейского парламента и Совета от 23 июля 2014 г. об электронной идентификации и трастовых услугах при проведении электронных транзакций на внутреннем рынке. Данным правовым актом предусматривается, что его "следует применять в полном соответствии с принципами, касающимися защиты персональных данных, изложенными в Директиве 95/46/ЕС Европейского парламента и Совета. В этой связи, учитывая принцип взаимного признания, устанавливаемый настоящим Регламентом, аутентификация в рамках онлайн-услуги должна касаться обработки только тех идентификационных данных, которые носят адекватный, значимый и не избыточный характер для предоставления доступа к данной онлайн-услуге". Более того, "провайдером трастовых услуг и надзорным органам следует уважать" (п. 11 Преамбулы) требования Директивы 95/46/ЕС, касающиеся соблюдения конфиденциальности и безопасности при обработке данных. Надзорным органам, учреждаемым согласно данному правовому акту "следует сотрудничать с органами по защите данных, например, путем информирования их о результатах проверок прошедших квалификацию провайдеров трастовых услуг, свидетельствующих о нарушении правил защиты персональных данных. В предоставляемой информации "следует, в частности, отражать случаи нарушения безопасности и нанесения ущерба персональным данным" (п. 31 Преамбулы).

49. Нормативная база в области взаимодействия при коммуникации "должна отвечать следующим критериям ... (с) она способствует заложенному при проектировании соблюдению принципа неприкосновенности частной жизни (privacy by design); и (d) она обеспечивает обработку персональных данных в соответствии с Директивой 95/46/ЕС" (статья 12).

1.7. УВЕДОМЛЕНИЕ О НАНЕСЕНИИ УЩЕРБА ПЕРСОНАЛЬНЫМ ДАННЫМ

⁷⁵ <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=570709&SecMode=1&DocId=592684&Usage=2>

⁷⁶ Рекомендация Rec(87)15 государствам-членам, регулирующая использование персональных данных в сфере правоохранительных органов, 17.09.1987

⁷⁷ Конвенция о киберпреступности, CETS No. 185, Будапешт, 23 ноября 2001 г.; вступила в силу 1 июля 2004 г.

⁷⁸ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

⁷⁹ Проект Директивы Европейского парламента и Совета о защите физических лиц при обработке персональных данных компетентными органами в целях предотвращения, расследования, выявления уголовных преступлений, уголовного преследования или исполнения уголовных наказаний, а также о свободном движении подобных данных (<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012PC0010>)

50. В текущей версии проекта Общего регламента о защите данных⁸⁰ устанавливаются новые обязательства контролера данных, вытекающие, например, из принципов проектируемой защиты персональных данных и защиты по умолчанию (by design and by default). Более того, вводится обязательство уведомлять о нанесении ущерба персональным данным, взяв за основу п. 3 статьи 4 об уведомлении об ущербе персональным данным Директивы 2002/58/ЕС. Термин "ущерб персональным данным" определен в п. (i) статьи 2 Директивы 2002/58/ЕС⁸¹.

51. В своем Заключении 03/2014 РГ ст. 29 предложила "неисчерпывающий перечень примеров ситуаций, когда следует уведомлять субъекта данных". Группа изучила понятие ущерба персональным данным с точки зрения трех критериев безопасности: "(i) "ущерб доступности", которому будут соответствовать случайная или неправомерная порча или утеря персональных данных, (ii) "ущерб целостности", которому будет соответствовать изменение персональных данных, и (iii) "ущерб конфиденциальности", которому будут соответствовать несанкционированное раскрытие персональных данных или доступ к ним".⁸² Далее обсуждаются случаи, не требующие уведомления, и подробно рассматриваются проблемы, с которыми могут столкнуться контролеры данных при принятии решения о наличии или отсутствии необходимости уведомлять субъектов данных.

II. НОРМАТИВНАЯ БАЗА БЕЛАРУСИ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

52. Беларусь приняла законодательный акт о защите физических лиц при обработке персональных данных и о свободном движении таких данных, который призван обеспечить защиту прав и основополагающих свобод физического лица, в частности, в отношении обработки персональных данных. В настоящее время действует ряд правовых актов, которые содержат положения, регулирующие защиту персональных данных в различном контексте, в частности:

1. Конституция (например, ст. 28, ч. 3 ст. 34);
2. Закон Республики Беларусь от 10.11.2008 № 455-3 "Об информации, информатизации и защите информации";
3. Закон Республики Беларусь от 21.07.2008 № 418-3 "О регистре населения";
4. Закон Республики Беларусь от 28.12.2008 № 113-3 "Об электронном документе и цифровой подписи";
5. Указ Президента Республики Беларусь от 08.11.2011 № 515 "О некоторых вопросах развития информационного общества в Республике Беларусь" и др.

53. Тем не менее, рекомендуется принять комплексное правовое регулирование в сфере защиты персональных данных. Следуя рекомендациям Доклада "Гармонизация

⁸⁰ http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

⁸¹ См. <http://www.enisa.europa.eu/act/it/data-breach-notification>

⁸² Заключение 03/2014 РГ ст. 29 от 25.03.2014 об уведомлении о нанесении ущерба персональным данным

цифровых рынков в Восточном Партнерстве” Беларуси необходим новый закон о защите персональных данных, чтобы лучше защищать персональные данные и приватность онлайн в соответствии с международной практикой, тем самым, обеспечив лучший баланс открытости Интернета и безопасности⁸³.

III. КРАТКОЕ ОПИСАНИЕ ПРЕДЛОЖЕНИЙ, КАСАЮЩИХСЯ БАЗОВОГО ЗАКОНА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

54. Базовый закон о защите персональных данных должен быть разработан в контексте национальной правовой системы, следуя детальному анализу потенциальных рисков и потребностей.

55. Содержание предложений для потенциального закона о защите персональных данных представлено с пояснениями в настоящей главе⁸⁴.

3.1. РЕКОМЕНДАЦИИ ПО СТРУКТУРЕ БАЗОВОГО ЗАКОНА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ:

- I. Общие положения
- II. Принципы защиты данных
- III. Права субъектов персональных данных
- IV. Контролер и обработчик
- V. Передача персональных данных третьим странам или международным организациям
- VI. Независимый орган по надзору за обработкой персональных данных
- VII. Средства правовой защиты, ответственность и санкции
- VIII. Положения, касающиеся отдельных ситуаций в области обработки данных
- IX. Заключительные положения

I. ОБЩИЕ ПОЛОЖЕНИЯ

56. Положениями данной главы следует определить цель данного законодательного акта. Следует дать определения используемым в нем терминам. Обычно к наиболее распространенным применяемым терминам относятся:

- персональные данные;
- субъект данных;
- чувствительные данные;
- обработка персональных данных;
- согласие субъекта персональных данных;
- контролер и обработчик;
- ущерб персональным данным;

⁸³ Study Report “Harmonisation of Digital Markets in the Eastern Partnership” (2015) <http://capacity4dev.ec.europa.eu/higstep/>

⁸⁴ Данный перечень не носит исчерпывающего характера, и необходимо рассматривать и другие аспекты, вытекающие из белорусского контекста. В настоящий документ включены дополнительные комментарии для разъяснения контекста.

- проектируемая неприкосновенность частной жизни (privacy by design) и неприкосновенность частной жизни по умолчанию (privacy by default);
- ребенок;
- данные, касающиеся здоровья, и другие термины, применяемые в данном законодательном акте.

57. Более того, необходимо указать применяемую нормативную базу и разъяснить территориальные рамки применения законодательного акта.

II. ПРИНЦИПЫ ЗАЩИТЫ ДАННЫХ

58. Регулированию подлежат ключевые принципы обработки персональных данных, которые предназначены служить передовой практикой, которой следует придерживаться контролерам данных в целях обеспечения защиты имеющихся у них данных. Принципы должны отражать как интересы контролеров, так и субъектов данных.

59. Можно включить ключевые европейские принципы защиты данных и детализировать их в национальной нормативной базе, а именно:

- а. принцип правомерной обработки данных;
- б. принцип указания и лимитирования цели обработки данных;
- с. принципы, касающиеся качества данных;
- д. принцип справедливой обработки данных;
- е. принцип подотчетности⁸⁵.

60. Можно рассмотреть вопрос о включении новых элементов, появившихся в результате подготовки проекта Общего регламента о защите данных⁸⁶. К этим элементам относятся: (i) принципы прозрачности, (ii) разъяснение принципа минимизации данных и (iii) установление всеобъемлющих обязанностей и юридической ответственности контролера данных.

61. Как предусмотрено Конвенцией № 108, могут допускаются лишь те изъятия из базовых принципов защиты данных, которые обусловлены необходимостью защиты фундаментальных ценностей демократического общества.⁸⁷

III. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

62. Регулированию подлежат права субъектов данных и механизмы принудительного обеспечения их соблюдения. Можно предусмотреть следующие права: (i) право доступа, которое также охватывает вопрос предоставления запрашиваемой информации, включающей в себя персональные данные другого физического лица (персональные данные третьей стороны); (ii) право на предотвращение и ограничение обработки данных;

⁸⁵ Проект Регламента о защите персональных данных (http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf)

⁸⁶ http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

⁸⁷ <http://www.coe.int/ro/web/conventions/full-list/-/conventions/treaty/108>

(iii) компенсация; (iv) исправление, удаление, уничтожение, блокировка; а также (v) следует отразить исключения (например, специальные цели, исследовательские цели, внутренние цели, коммерческие цели).

IV. КОНТРОЛЕР И ОБРАБОТЧИК

63. Положениями данной главы следует регулировать юридические обязательства как контролера, так и обработчика данных с учетом "принципа подотчетности"⁸⁸. Можно предусмотреть следующие обязательства: (i) обязательство принимать надлежащие меры по обеспечению безопасности обработки данных, (ii) уведомлять о нанесении ущерба персональным данным, (iii) проводить оценку воздействия защиты данных (если это будет сочтено подходящим решением для Беларуси), (iv) уведомлять надзорный орган перед выполнением обработки персональных данных, (v) ввести должность специалиста по защите данных и определить его ключевые обязанности и др.

64. В части исключений, касающихся обязательства контролера данных уведомлять надзорный орган перед выполнением обработки персональных данных, законодатель должен решить, включать ли безусловное обязательство уведомления, как, например, в Директиве 95/46/ЕС или указать обстоятельства, в которых контролер обязан уведомлять, как, например, в проекте Общего регламента о защите персональных данных.

65. Должность специалиста по защите данных может быть обязательной для всех контролеров данных либо обязательной только в конкретных случаях, как это, например, предусмотрено в текущем проекте Общего регламента о защите персональных данных ЕС. Следует определить ключевые задачи такого специалиста.

66. Можно определить обязательства контролера данных, вытекающие из принципов проектируемой защиты данных и защиты данных по умолчанию.

V. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕТЬИМ СТРАНАМ ИЛИ МЕЖДУНАРОДНЫМ ОРГАНИЗАЦИЯМ

67. Необходимо регламентировать вопросы передачи персональных данных третьим странам или международным организациям. В частности, следует определить общие принципы передачи данных, касающиеся как стран, обеспечивающих адекватный уровень защиты данных, так и стран, не обеспечивающих адекватного уровня защиты.

VI. НЕЗАВИСИМЫЙ ОРГАН ПО НАДЗОРУ ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

68. В данной главе предлагается учредить надзорный орган, обладающий независимым статусом, с учетом того, что он не сможет эффективно обеспечивать защиту прав и свобод физического лица, если не будет осуществлять свои функции в режиме полной независимости⁸⁹. Кроме того, в ней предлагается регламентировать обязанности и компетенцию надзорного органа.

⁸⁸ Заключение 3/2010 РГ ст. 29 от 13 июля 2010 г. о принципе подотчетности (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf)

⁸⁹ Пояснительная записка – ETS 181 – Автоматическая обработка данных (Протокол) (<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce56>)

69. Обязанности и компетенцию следует регламентировать с учетом национальной нормативной базы. Следует включить условие о независимости надзорных органов. Следует установить правила учреждения надзорного органа. Следует оговорить обязанности, в том числе обязанности рассматривать жалобы и проводить по ним расследования, а также повышать уровень информированности населения о рисках, правилах, способах защиты и правах. Может быть рассмотрен вопрос о наделении надзорного органа полномочиями по принятию постановлений об административных нарушениях.

70. Следует отразить права субъекта данных, такие как, например, право на подачу жалобы в надзорный орган, право судебной защиты против действий надзорного органа, право судебной защиты против действий контролера или обработчика данных, право на получение компенсации и привлечение к ответственности.

VII. СРЕДСТВА ПРАВОВОЙ ЗАЩИТЫ, ОТВЕТСТВЕННОСТЬ И САНКЦИИ

71. Следует установить правила, регламентирующие средства правовой защиты, ответственность и санкции с учетом соответствующей национальной нормативной базы.

VIII. ПОЛОЖЕНИЯ, КАСАЮЩИЕСЯ ОТДЕЛЬНЫХ СИТУАЦИЙ В ОБЛАСТИ ОБРАБОТКИ ДАННЫХ

72. В данной главе следует регламентировать конкретные ситуации, касающиеся обработки данных. В частности, могут быть рассмотрены следующие вопросы:

- a) обработка персональных данных и свобода слова;
- b) обработка персональных данных, касающихся здоровья;
- c) обработка данных в контексте трудовых отношений;
- d) обработка данных в целях исторических, статистических и научных исследований;
- e) обязательства сохранения секретности;
- f) правила защиты данных для церквей и религиозных объединений;
- g) обработка государственного идентификационного номера физического лица (личный номер), отпечатков пальцев или иного идентификатора общего применения;
- h) обработка персональных данных, касающихся судимости, принудительных мер или административных санкций и др.

IX. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

73. Положениями данной главы могут регламентироваться вопросы, касающиеся вступления в силу, оценки, взаимосвязи с другими актами и внесения в них изменений, а также иные вопросы, вытекающие из национального законодательства, в том числе регулирующего подготовку законопроектов.

ЗАКЛЮЧЕНИЕ

Планируемые к осуществлению в Беларуси инновации требуют действенных механизмов соблюдения безопасности и конфиденциальности персональных данных, которые не могут быть обеспечены без предоставления законодательных гарантий защиты физических лиц при обработке персональных данных и свободного движения таких данных.

В настоящем документе освещены ключевые аспекты, вытекающие из европейской системы регулирования защиты персональных данных. Базовый закон о защите персональных данных должен быть разработан с учетом действующей в Беларуси нормативной базы, потенциальных рисков, позиций различных заинтересованных субъектов и других факторов.