*ҒТАХР 19.01.05*

*[1]Темірболат Ақылхан Серікұлы*
[1]Университета имени Сулеймана Демиреля, Каскелен, Казахстан

# «Совершенствование законодательства Республики Казахстан о персональных данных на основе общего регламента по защите персональных данных (GDPR)»

**Abstract:** Due to the fact that with the development of information technologies and automated systems, a person's personal data is becoming increasingly isolated from private life as a subject of legal relations, the practice of protecting them is just beginning to accumulate and acquire an integrated approach. And also, personal information is recognized as one of the priority objects of organizational and legal protection, since under certain conditions and circumstances it follows from the right to privacy. In human life, the provision of information about oneself to other members of society, as well as public relations for the provision and protection of information are regulated by the norms of law. Thus, effective management of an employee's behavior in the course of work is possible only if there is reliable information about his personality provided in sufficient volume. This fact is clearly fixed in the Labor Code of the Republic of Kazakhstan. In a special chapter of the codified labor legislation, the employer is allowed to receive, store, combine and use the personal data of the employee hired by him.

**Keywords:** Personal data, personal data law, personal information, confidentiality, GDPR, personal security.

***

**Аңдатпа:** Ақпараттық технологиялар мен автоматтандырылған жүйелердің дамуымен адамның жеке деректері құқықтық қатынастардың субъектісі ретінде жеке өмірден оқшауланғандықтан, оларды қорғау практикасы енді ғана жинақтала бастайды және кешенді тәсіл ала бастайды. Сондай-ақ, жеке ақпарат ұйымдық-құқықтық қорғаудың басым объектілерінің бірі ретінде танылады, өйткені белгілі бір жағдайлар мен жағдайларда ол жеке өмірге қол сұғылмаушылық құқығынан туындайды. Адам өмірінде қоғамның басқа мүшелеріне өзі туралы ақпарат беру, сондай-ақ ақпарат беру және қорғау жөніндегі қоғамдық қатынастар құқық нормаларымен реттеледі. Осылайша, жұмыс процесінде қызметкердің мінез-құлқын тиімді басқару оның жеке басы туралы жеткілікті мөлшерде ұсынылған сенімді ақпарат болған жағдайда ғана мүмкін болады. Бұл факт Қазақстан Республикасының Еңбек кодексінде нақты бекітілген. Кодификацияланған еңбек заңнамасының арнайы тарауында жұмыс берушіге өзі жалдаған қызметкердің дербес деректерін алуға, Сақтауға, біріктіруге және пайдалануға рұқсат етіледі.

**Түйінді сөздер:** дербес деректер, дербес деректер туралы заң, жеке ақпарат, құпиялылық, gdpr, жеке қауіпсіздік.

***

**Аннотация:** В связи с тем, что с развитием информационных технологий и автоматизированных систем персональные данные человека становятся все более изолированными от частной жизни как субъекта правоотношений, практика их защиты только начинает накапливаться и приобретать комплексный подход. А также, личная информация признана одним из приоритетных объектов организационно-правовой защиты, поскольку при определенных условиях и обстоятельствах она вытекает из права на неприкосновенность частной жизни. В жизнедеятельности человека предоставление информации о себе другим членам общества, а также общественные отношения по предоставлению и защите информации регулируются нормами права. Таким образом, эффективное управление поведением сотрудника в процессе работы возможно только при наличии достоверной информации о его личности, представленной в достаточном объеме. Этот факт четко закреплен в Трудовом кодексе Республики Казахстан. В специальной главе кодифицированного трудового законодательства работодателю разрешается получать, хранить, объединять и использовать персональные данные нанятого им работника; Законодатель установил общие требования к обработке персональных данных работников и определил гарантии их защиты.

**Ключевые слова:** персональные данные, закон о персональных данных, личная информация, конфиденциальность, GDPR, личная безопасность.

****

Казахстан, будучи страной, серьезно интегрированной в глобальное политическое и экономическое реальное пространство, демонстрирует впечатляющие темпы интеграции в глобальное информационное пространство, как на уровне государственных структур, так и на уровне общества. Недостаточное внимание к новым возможностям, а также рискам и угрозам может привести к тому, что страна выпадет из общей тенденции мирового развития и будет вытеснена на периферию международных процессов.

Появление системы электронного правительства способствовало, с одной стороны, изменению отношений между обществами и их правительствами в пользу демократизации, а с другой стороны, значительно способствовало сокращению бюджетных расходов на администрирование.

21 мая 2013 года в Казахстане был принят Закон "О персональных данных и их защите". Как и в любом другом законе, в нем содержится терминология и основные направления работы по защите персональных данных [1].

Согласно закону, "персональные данные - информация, относящаяся к определенному или определяемому на основании субъекта персональных данных, записанная на электронных, бумажных и (или) иных материальных носителях". Основной целью этого закона является "обеспечение защиты прав и свобод человека и гражданина при сборе и обработке персональных данных" (статья 2), в то время как вопрос о их хранении пока не стоит.

Компетенция уполномоченного органа (Прокуратуры Республики Казахстан) в области защиты персональных данных представлена в статье 27-1 проекта Закона Республики Казахстан "О внесении изменений в законодательство Республики Казахстан о внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий".

Если сравнить этот документ с аналогичными законами в других странах мира, следует отметить, что, с одной стороны, он достаточно прямолинеен и всеобъемлющ, в то время как некоторые аспекты защиты персональных данных на практике провисают. Так, например, в статье 20 закону о персональных данных РК говорится, что персональные данные подлежат защите, которая гарантируется государством и осуществляется в порядке, определяемом Правительством Республики Казахстан.

Учитывая крупнейших утечек личных данных казахстанцев в 2019 году из баз данных ЦИК и Генеральную прокуратуру, встает вопрос, как государство может гарантировать защиту личной информации, если, по данным TSARK, утечка произошла из базы данных Генеральной прокуратуры Республики Казахстан, т. е. уполномоченный орган в сфере защиты персональных данных, и Министерства внутренних дел Республики Казахстан приостановлено в случае утечки данных из-за отсутствия состава преступления, потому что "указанной информации с данными граждан Республики Казахстан на сети не было обнаружено"? [2].

Очередная утечка персональных данных была зафиксирована Центром информационных технологий компании "ДАМУ", когда в июле 2019 года произошел инцидент передачи третьим лицам информации, содержащей конфиденциальные данные, от лица, имеющего законный авторизованный доступ пользователя к Медицинской информационной системе DamuMed23[3].

Предполагалось, что компания будет заниматься разбором полетов в соответствии с действующим законодательством, а именно Кодексом Республики Казахстан "Об административных правонарушениях" статья 79 "нарушение законодательства Республики Казахстан О персональных данных и их защите" и Уголовным кодексом Республики Казахстан Статья 205 "неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций", статья 208 "Неправомерное завладение информацией", но нет сведений о разрешении данного дела в публичном

пространстве. Еще предстоит выяснить, был ли кто-либо ответственен за этот инцидент.

Эти и другие примеры утечки персональных данных казахстанцев, по данным Министерства цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан, свидетельствуют о наличии ряда проблем.

Во-первых, "каждый государственный орган-владелец баз данных-самостоятельно несет ответственность за сохранность своих баз данных и соблюдение правил и положений об использовании и конфиденциальности хранящейся там информации".

Во-вторых, ни один государственный орган не обладает компетенцией и полномочиями по мониторингу Интернета с точки зрения нарушений законодательства в области персональных данных и их защиты.

В-третьих, в стране нет специализированного органа по защите персональных данных (по аналогии с Европейским агентством по защите данных).

Однако в дополнение к этим очевидным проблемам и анализу вышеуказанных случаев утечки личной информации, которые стали достоянием общественности, важно обратить внимание еще как минимум на три момента:

1. Преследование за нарушение закона. Здесь речь идет об увольнении

руководителя департамента, на примере дела Qazkom, и штрафе для должностных лиц, как и ожидалось в случае утечки данных 11 миллионов казахстанцев. Однако на самом деле правовой статистики по защите персональных данных нет, и правовой механизм должен разрабатываться открыто и прозрачно. Важно развивать культуру защиты персональных данных, в том числе путем информирования субъектов персональных данных об утечках информации, что позволит выстраивать доверительные отношения и серьезно относиться к ответственности за сбор, обработку и хранение персональных данных[4].

2. Защита данных и конфиденциальность данных. Если защита данных

это защита от несанкционированного доступа, то конфиденциальность данных — это авторизованный доступ - у кого он есть, и кто его определяет. Другими словами, защита данных, по сути, является технической проблемой, в то время как конфиденциальность данных является юридической (правовой) проблемой. Дело в том, что технологии сами по себе не смогут обеспечить конфиденциальность персональных данных. Большинство протоколов защиты конфиденциальности по-прежнему уязвимы для уполномоченных лиц, которые могут получить

доступ к данным. Бремя этих уполномоченных лиц в первую очередь связано с законом о конфиденциальности, а не с технологиями.

3. Технологические возможности и партнеры для сотрудничества. Прежде

всего, с точки зрения защиты персональных данных возникают вопросы о том, кто имеет доступ и контролирует безопасность сбора, обработки и хранения личной информации, полученной, например, с помощью камер Sergek. Этот вопрос особенно актуален в связи с тем, что два технических партнера, китайская компания Dahua Technology (партнер Korkem Telecom в Sergek) и Hikvision (которая работает в Казахстане с 2015 года), являются поставщиками продукции на казахстанский рынок.

Эта составляющая также усугубляется тем, в какой степени государственные органы будут уважать права граждан на защиту персональных данных, и здесь, в первую очередь, речь идет о функциях и возможностях правоохранительных органов Республики Казахстан, в частности Комитета национальной безопасности (КНБ). В контексте внедрения Национальной системы видеонаблюдения главный вопрос заключается в том, как достичь баланса между правом на неприкосновенность частной жизни и вмешательством в нее в интересах общественного порядка и национальной безопасности.

В целом, система заинтересованных сторон, участвующих в процессах, связанных с защитой персональных данных, очень велика. Несмотря на наличие специализированных учреждений, курирующих надзорные органы и других вовлеченных участников информационного процесса-сбора, обработки, хранения, уничтожения персональных данных, важно понимать, что, по сути, при составлении схемы должны быть отражены все существующие государственные органы и их комитеты, департаменты и ведомства, поскольку у каждого учреждения власти есть хотя бы одна база данных, с которой они работают. Это означает, что культура защиты персональных данных должна стать тем самым связующим звеном, которое позволит государственным органам гармонично взаимодействовать друг с другом и с обществом, повысить уровень доверия и коммуникации, что является неотъемлемой частью цифрового общества, создание которого предусмотрено Законом Республики Казахстан о персональных данных и их защите.

Законы о защите персональных данных необходимы для защиты личной жизни, обеспечения безопасности данных, содействия справедливости и прозрачности, защиты от дискриминации и облегчения трансграничных потоков данных. Однако есть несколько областей, в которых действующие законы о защите персональных данных могут быть усовершенствованы для более эффективного решения этих проблем. В этом разделе мы предложим несколько улучшений в законодательстве о защите персональных данных.

Ужесточение требований к уведомлению о нарушении данных: Одной из областей, где законы о защите персональных данных могут быть улучшены, является область требований к уведомлению о нарушении данных. В настоящее время многие законы о защите персональных данных требуют от организаций уведомлять физических лиц, если их персональные данные были скомпрометированы в результате утечки данных. Однако эти требования часто расплывчаты и не содержат четких указаний относительно того, когда и как организации должны уведомлять отдельных лиц. Для решения этой проблемы законы о защите персональных данных можно было бы усилить, установив более четкие и конкретные требования к уведомлению о нарушении данных, включая сроки уведомления и конкретную информацию, которая должна быть включена в уведомление.

Внедрение оценки воздействия на защиту данных: ещё одной областью, в которой законы о защите персональных данных могут быть усовершенствованы, является область оценки воздействия на защиту данных (DPIAS). DPIA — это оценка потенциальных рисков и воздействия деятельности по обработке данных на частную жизнь отдельных лиц и их права на защиту данных. Они являются важным инструментом для выявления и снижения рисков, связанных с деятельностью по обработке данных. Однако действующие законы о защите персональных данных не требуют от организаций проводить DPIA во всех случаях. Для решения этой проблемы законы о защите персональных данных можно было бы усовершенствовать, обязав организации проводить DPIA во всех случаях, когда существует высокий риск для частной жизни физических лиц и их прав на защиту данных.

Усиление требований к согласию: Согласие является важным принципом законов о защите персональных данных, поскольку оно дает отдельным лицам контроль над своими персональными данными. Однако действующие требования к согласию часто расплывчаты и не содержат четких указаний относительно того, что представляет собой действительное согласие. Для решения этой проблемы законы о защите персональных данных можно было бы усилить, установив более четкие и конкретные требования к действительному согласию. Например, может потребоваться, чтобы согласие было дано свободно, конкретно, информировано и недвусмысленно.

Минимизация данных: Минимизация данных — это принцип сбора и обработки только минимального объема персональных данных, необходимого для определенной цели. Действующее законодательство во многих юрисдикциях прямо не требует минимизации данных, что может привести к ненужному сбору и обработке персональных данных. Сведение к минимуму данных может помочь снизить риск утечки данных и обеспечить защиту частной жизни отдельных лиц.

Внесение таких изменений в законодательство, безусловно, будет способствовать, во-первых, эффективному применению положений закона, а во-вторых, усилению контроля субъектов персональных данных над их данными, а также эффективной защите персональных данных в целом. Только установив положения о принципах и правилах обработки персональных данных, правовой природе контроллера и обработчика, деятельности уполномоченного органа по защите персональных данных, ответственности за нарушения и другие аналогичные положения, как они закреплены в GDPR , можно действительно претендовать на звание “Цифровой Казахстан в эпоху глобализации”, поскольку именно GDPR является одним из самых высоких стандартов безопасности для защиты персональных данных на сегодняшний день.

Что касается независимого органа по защите данных, то комитет должен руководствоваться следующими принципами: независимость, беспристрастность, компетентность, открытость и эффективность. Комитет является надзорным органом, который может взаимодействовать с различными субъектами персональных данных для выполнения своих обязанностей. Современный опыт показывает, что благодаря таким органам достигается высочайший уровень защиты персональных данных, к которому могут обратиться физические и юридические лица для восстановления своих нарушенных прав. Для этого, в первую очередь, необходимо внести изменения в действующее законодательство о защите персональных данных с целью создания национального независимого органа по защите персональных данных. Во-вторых, необходимо утвердить устав такого органа, который будет регулировать его миссию, цели, задачи, принципы деятельности и т.д. Учитывая важность и ценность защиты персональных данных, положения и нормы настоящей хартии должны применяться ко всем субъектам персональных данных в Республике Казахстан. Конечно, предстоит еще проделать большую работу и изучить вопросы определения правовой структуры такого органа, но только с помощью такого правового инструмента мы сможем добиться защиты основного права субъектов персональных данных – защиты личной информации.

**Список использованной литературы:**

1 Закон Республики Казахстан // "О персональных данных и их защите", 21 мая 2013 г. № 94-V

2 "Утечка данных из базы данных Генеральной прокуратуры Республики Казахстан: законопроект идет месяцами", Ратель, 14 февраля 2020 года, https://ratel.kz/raw/utechka_dannyh_iz_bazy_genprokuratury_rk_schet_idet_na_mesjatsy

3 "Насколько казахстанцы защищены от утечки персональных данных", Прибыль, 11 июля 2019 года, https://profit.kz/news/53478/Naskolko-kazahstanci-zaschischeni-ot-utechki-personalnih-dannih/.
4 "Должностные лица, ответственные за утечку данных 11 миллионов казахстанцев, будут оштрафованы", Информбюро, 9 июля 2019 года, https://informburo.kz/novosti/dolzhnostnyh-lic-vinovnyh-v-utechke-dannyh-11-mln-kazahstancev-nakazhut-shtrafom-92602.html