PROUD ENGINEERS

Анализ изменений в нормативно правовые акты Казахстана по защите данных

Каспар Кала и Лаура Каск

Версия 1.1

1. Введение

Казахстанская экспертная группа по цифровым правам (Заказчик) обратилась с просьбой проанализировать предлагаемые изменения в казахстанское законодательство для улучшения защиты персональных данных Комитетом по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности (далее «КИБ МЦРИАП»). Клиент обратился к экспертам Proud Engineers со следующим запросом: действительно ли предлагаемые изменения гарантируют более высокий уровень защиты данных, или они повлекут за собой чрезмерное регулирование и контроль.

Эксперты Proud Engineers (PE) получилb от Клиента входные документы «Поправки для защиты персональных данных в законодательстве Казахстана» и «Реестр Согласия» и между PE и Клиентом прошла сессия для обсуждения предлагаемых изменений от 18 мая 2021 года и 1 июня 2021 года. Входные документы и встречи послужили входными данными для этого аналитического документа.

Целью этого аналитического документа является:

- Анализ предлагаемых изменений с точки зрения ЕС и Эстонии;
- Осветить имеющийся опыт ЕС и Эстонии;
- Предоставить Клиенту идеи, как участвовать в законодательной процедуре в качестве конструктивного заинтересованного лица.

Этот документ представляет собой обновленную версию чернового документа, отправленного Клиенту 28 мая 2021 года. В данную версию 1.1 внесены изменения в раздел 2.3, поскольку «реестр согласия» был отредактирован.

Содержание

2. Поправки

В этом разделе анализируются предлагаемые КИБ МЦРИАП поправки. В каждом подразделе рассказывается, что РЕ узнало о поправке, и представлены экспертные знания относительно данных поправок.

2.1. Сервис защиты персональных данных (СЗПД)

Что РЕ узнало о поправке:

• СЗПД - это служба осуществляющая контроль за доступом к данным граждан (субъектов данных). Задача СЗПД – создать реестр, в котором хранятся данные, и граждане могли бы предоставлять разрешения и доступ к данным, находящимся под их контролем.

• СЗПД включает реестр персональных данных, обрабатываемых частными и государственными организациями;

• Реестр операторов персональных данных (РОПД) будет интегрирован с СЗПД – сначала объекты должны быть зарегистрированы в РОПД;

• Портал электронного правительства будет интегрирован с СЗПД;

• Процедура согласия также является частью СЗПД;

• Архитектура СЗПД на данный момент к ознакомлению недоступна.

Изначальная цель поправок заключается в предоставлении гражданам большего контроля над своими личными данными и предоставлении им инструментов для управления доступом к личным данным на основе согласия - то, что обсуждалось в ЕС и Эстонии. В декларации 7 Общего регламента ЕС по защите персональных данных (ОРЗПД) говорится, что «физические лица должны иметь контроль над своими личными данными». Принцип прозрачности является одним из ключевых принципов ОРЗПД.

Хотя в законодательстве нет требования о том, что информационные системы должны создаваться децентрализованно, в Эстонии одним из основных принципов создания таких систем является децентрализация. Это означает, что данные не собираются в какой-либо единый реестр (что создает единую систему, которая может дать сбой и в результате увеличивает стоимость кибербезопасности), а хранятся в том месте, где они собираются и хранятся (например, в банке). Это не было описано, но у экспертов РЕ сложилось впечатление, что система СЗПД направлена на создание централизованной системы вместо децентрализованной.

К примеру, информационная система Эстонии основана на децентрализованной модели, и принцип единовременного использования (данные не дублируются в нескольких информационных системах, а запрашиваются у источника) означает, что потери могут быть

ограничены в случае утечки данных. Поскольку 100% -ная безопасность невозможна, утечки данных могут произойти в каждой информационной системе, поэтому принципы проектирования имеют решающее значение.

Поэтому мы настоятельно рекомендуем не создавать центральное хранилище личных данных, чтобы граждане могли контролировать свои личные данные, так как эту цель можно достичь другими способами.

Государство, конечно, должно здесь подавать пример. В Эстонии есть служба Data Tracker, доступная на правительственном портале eesti.ee. На нем гражданин может узнать кто (какая организация) обращался за его данными в реестре населения:

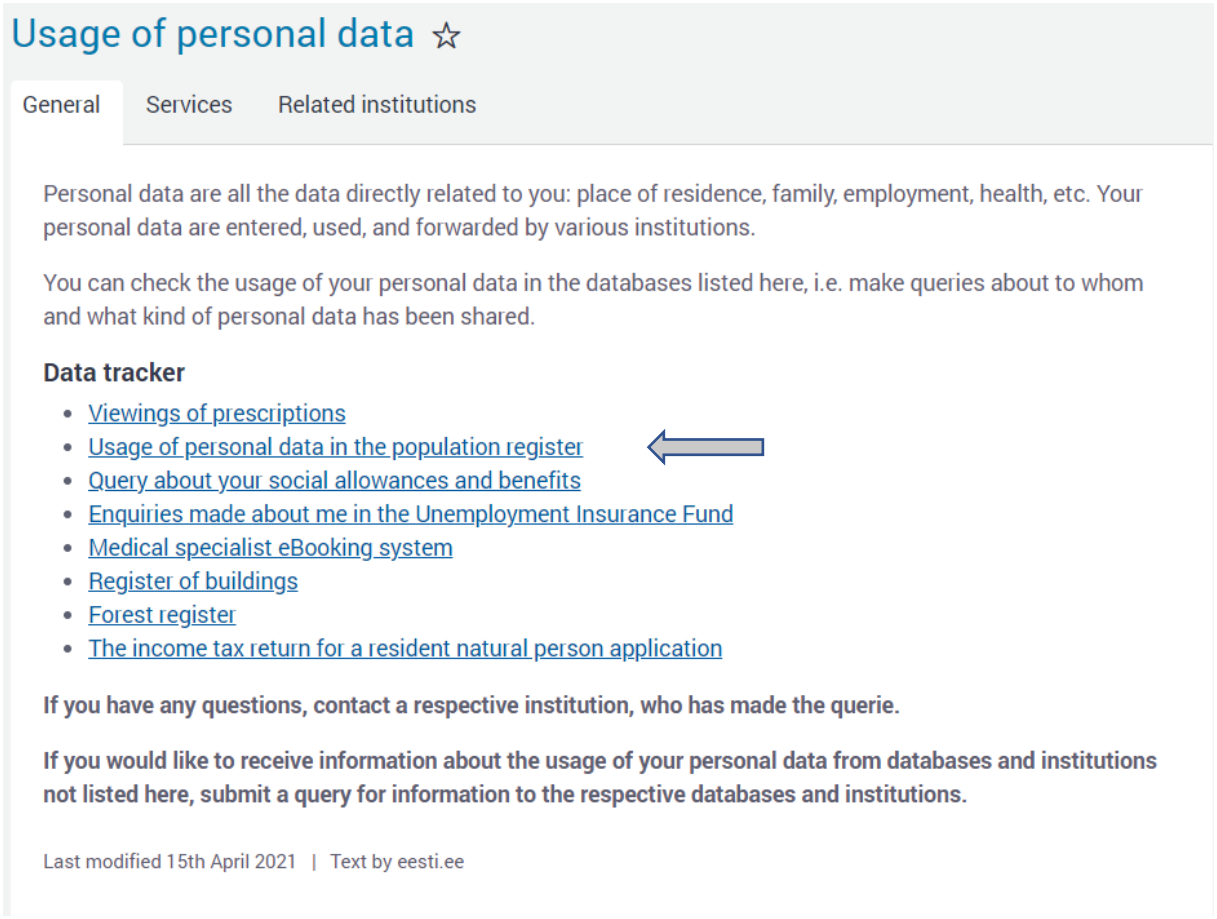
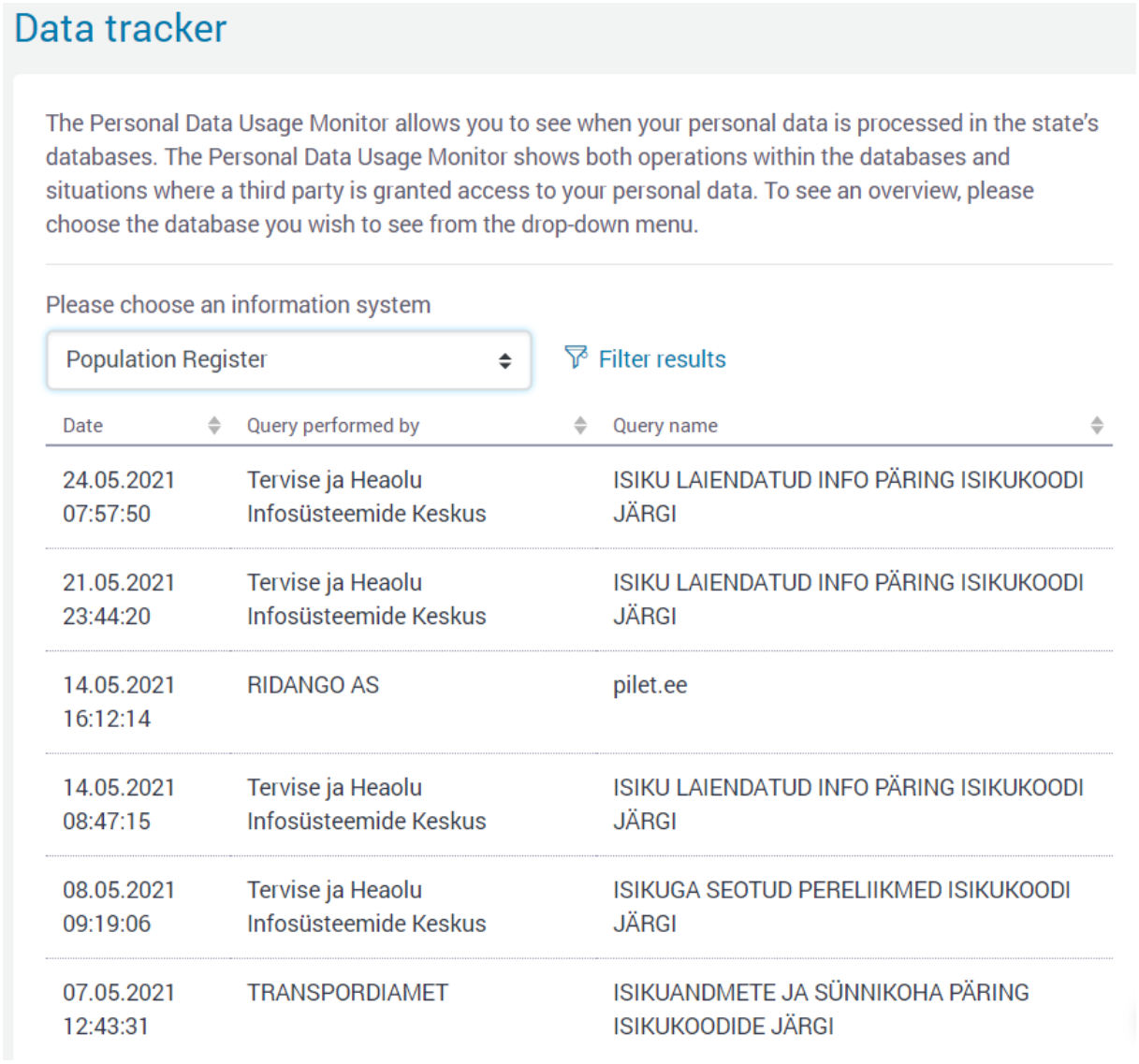


Рисунок 1: Сервисы отслеживания данных

Гражданин может увидеть список организаций государственного и частного секторов, которые запрашивали его личные данные из реестра населения:



Data tracker

The Personal Data Usage Monitor allows you to see when your personal data is processed in the state's databases. The Personal Data Usage Monitor shows both operations within the databases and situations where a third party is granted access to your personal data. To see an overview, please choose the database you wish to see from the drop-down menu.

Please choose an information system

Population Register

Filter results

Date	Query performed by	Query name
24.05.2021 07:57:50	Tervise ja Heaolu Infosüsteemide Keskus	ISIKU LAIENDATUD INFO PÄRING ISIKUKOODI JÄRGI
21.05.2021 23:44:20	Tervise ja Heaolu Infosüsteemide Keskus	ISIKU LAIENDATUD INFO PÄRING ISIKUKOODI JÄRGI
14.05.2021 16:12:14	RIDANGO AS	pilet.ee
14.05.2021 08:47:15	Tervise ja Heaolu Infosüsteemide Keskus	ISIKU LAIENDATUD INFO PÄRING ISIKUKOODI JÄRGI
08.05.2021 09:19:06	Tervise ja Heaolu Infosüsteemide Keskus	ISIKUGA SEOTUD PERELIIKMED ISIKUKOODI JÄRGI
07.05.2021 12:43:31	TRANSPORDIAMET	ISIKUANDMETE JA SÜNNIKOHA PÄRING ISIKUKOODIDE JÄRGI

Рисунок 2: Использование данных реестра населения

Эта информация позволяет человеку обратиться к лицу, инициировавшему запрос, чтобы узнать цель запроса, нет ли какой-либо ошибки, или, если запрос был сделан не на законном основании, подать жалобу в уполномоченный орган по защите персональных данных. Таким образом, гражданам предоставляется определенный уровень контроля над своими личными данными, но обратите внимание, что это можно сделать без сбора всех данных в центральном хранилище. Data Tracker - это программное обеспечение, созданное Государственной информационной системой, которое может использоваться любым владельцем общедоступного набора данных для повышения прозрачности для граждан.[1]

Как уже было сказано, в Эстонии существует децентрализованная информационная система, включающая более тысячи общедоступных баз данных[2], которые обмениваются данными на

[1] Код с открытым исходным кодом и доступен на GitHub: https://github.com/e-gov/AJ.
[2] По данным RIHA, в Эстонии зарегистрировано более 1300 информационных систем и реестров.

основании постановления правительства или министерства (как такового в соответствии с законодательством) через систему обмена данными X-Road. Однако существует центральный компонент, который можно описать как реестр метаданных для всех реестров. Он называется RIHA.[3] RIHA - это реестр всех реестров государственного сектора (местного и государственного уровня) - каждый публичный реестр должен быть описан в RIHA и для каждого реестра есть информация, какие данные они содержат, услуги, которые он предоставляет, критерии доступа. Похоже на то, что, создание СЗПД имеет такую же цель, но в более широком масштабе, включая базы данных и реестры частного сектора.

Тем не менее, чтобы добиться этого, государственный сектор может сначала стать лидером, открыто рассказав: i) какие государственные реестры он ведет; ii) какие данные обрабатываются в этих реестрах; и iii) какие API-интерфейсы используются реестром. Это дает правительству картину того, кто какие данные обрабатывает, и позволяет собирать данные только один раз (принцип однократного использования). Только когда это будет доказано и возникнет явная необходимость, частный сектор может последовать за государством.

Процесс и обязанности в отношении создания реестра (или любого общедоступного набора данных) изложены в Законе об общественной информации в Эстонии. Общедоступный набор данных должен быть одобрен пятью различными органами, которые проверяют документацию и соблюдение правил и положений (включая правила защиты данных). На рисунке ниже описаны организационные роли в создания общедоступных наборов данных.

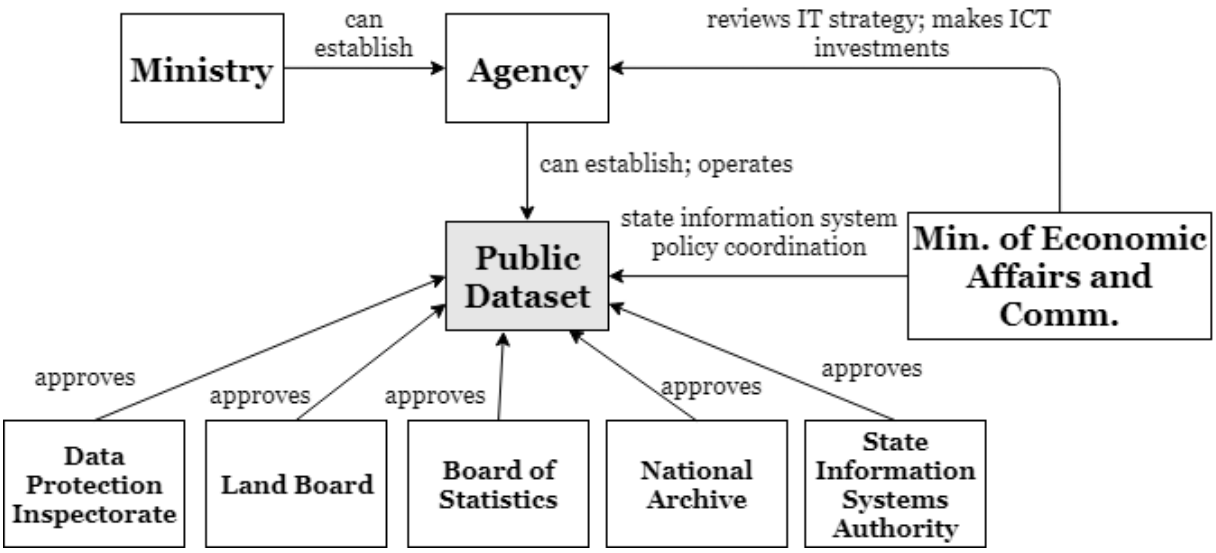


Рисунок 3: организационные роли в создании общедоступных наборов данных

[3] RIHA, https://www.riha.ee/Avaleht.

2.2. Реестр согласия

Что эксперты РЕ выяснили о реестре:

- Реестр согласия предназначен для того, чтобы правительство знало обо всех случаях предоставления согласия, гражданами и компаниями;
- Реестр согласия также предназначен, для того чтобы правительство, а не компании собирало согласие и на основании этого предоставляло гражданам услуги по управлению согласием;
- В статью о реестре согласия внесены изменения. Изменения обсуждались во время телефонного разговора 21.01.21. В соответствии с документом «Реестр Согласия», направленным экспертам РЕ 21.03.21, статья 8 о реестре согласия отредактирована.

«Согласие как услуга» - это решение, которое на данный момент анализируется в Эстонии и по нему готовится первоначальное подтверждение концепции проекта.[4] Данный шаг рассматривается, как способ стимулировать экономику данных.[5] Однако решение, предложенное в Эстонии, никоим образом не будет препятствовать практике получения согласия гражданина (субъекта данных) и организации, собирающей согласие. Компании необходимо согласие на законную обработку информации. Правительство, конечно, может предложить дополнительные услуги и инструмент управления согласием может стать отличным способом повышения прозрачности в обществе. Однако это можно сделать таким образом, что не нужно будет собирать все артефакты согласия. Это означает, что служба согласия может быть создана таким образом, чтобы отправлять только метаданные согласия в назначенный государственный орган после того, как гражданин или пользователь дал согласие на обработку данных. Затем правительство может предоставить гражданам услугу управления согласием в качестве панели управления или инструмента прозрачности, не влияя на текущую деловую практику.

Если РЕ правильно понимает структуру реестра согласия, правительство будет действовать как сторона, которая собирает и хранит согласие. Тогда возникает вопрос, что означает согласие? Указывает ли правительство, что компания может собирать или нет? Если это так, то система сложна в исполнении и может ограничивать компании, а также мешает свободе ведения бизнеса. Еще одним недостатком этого механизма является то, что пользователя нужно будет направлять с веб-сайта компании на веб-сайт правительства и обратно, но сделать это безопасным способом сложнее, чем за один сеанс.

В результате **реестр согласия не будет пропорционален цели, которую он преследует, и будет слишком обременительным для всех вовлеченных сторон** - правительства (для этого

[4] Consent Service, https://github.com/e-gov/NT.
[5] 2020 Yearbook of the State Information System Authority, p 26-27, https://www.ria.ee/sites/default/files/content-editors/RIA/ria_aastaraamat_2020_eng.pdf.

потребуются значительные финансовые ресурсы), компаний (их деловые и договорные отношения существенно изменятся, а затраты на информационную безопасность увеличатся) и пользователей (пользовательский опыт значительно пострадает).

Также стоит упомянуть тот факт, что сценарий, когда правительство собирает согласие от имени компаний, будет подразумевать, что правительство должно рассматривать юридические жалобы и обрабатывать процессы отзыва согласия от имени компаний. Это может быть осуществлено, но у этого также должен быть экономический смысл.

Для субъектов данных, если правительство контролирует все их согласия, должны быть четкие критерии того, что правительство может и не может делать с такой информацией (принцип ограничения цели), поскольку это дает основания для профилирования того, что нравится пользователям, что они делают и если потенциально они могут рассматриваться как угроза обществу. Таким образом, решение можно использовать для контроля или, по крайней мере, для лучшего понимания того, какие услуги человек использует, смотрит и читает, и таким образом он станет инструментом контроля, а не прозрачности.

Согласие в Общем регламенте ЕС по защите персональных данных является одним из правовых оснований. Это не главное или самое важное основание, а одно из шести правовых оснований для обработки персональных данных, указанных в статье 6 (1) регламента. Условия согласия изложены в статье 7 регламента.[6]

В общем, согласие должно быть предоставлено свободно (это должен быть реальный выбор), конкретным (связано с конкретной целью), информированным (должна быть предоставлена соответствующая и достаточная информация), с однозначным указанием субъекта данных (например, без предварительно отмеченных полей разрешены), различимые (должны быть четко обозначены, если они являются частью условий), и субъект данных должен иметь возможность отозвать согласие без ущерба (отзыв не может быть сложнее, чем согласие было). Контроллер должен иметь возможность продемонстрировать, что субъект данных дал свое согласие (а не наоборот).[7]

Следовательно, использование согласия должно соответствовать определенным требованиям прозрачности и другим требованиям. Для государственного сектора Общий регламент ЕС по защите персональных данных имеет ограниченное применение, потому что изложение 43 регламента предусматривает, что в случаях, когда существует явный дисбаланс между

[6] См. Руководство Европейского надзорного органа по защите данных о согласии, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[7] См. Общем регламенте ЕС по защите персональных данных 43 GDPR.

сторонами, в частности, когда контролер является государственным органом, согласие не может быть дано свободно.[8]

Основным основанием для государственного сектора должна быть обработка на основе закона или постановления (статья (6) (1) (e)) - обработка, необходимая для задачи, выполняемой в общественных интересах или при выполнении официальных полномочий контролера.[9]

В статье 8 (1), касающейся процедуры согласия, говорится, что «субъект или его законный представитель дает (отзывает) согласие на сбор, обработку персональных данных в письменной форме, через Службу контроля доступа к персональным данным или другим способом, который подтверждает получения согласия». Ни этот, ни другие подразделы статьи 8 не содержат каких-либо требований к согласию, аналогичных тем, которые есть в Регламенте (добровольно, конкретное, информированное и т.д.). Статья 8 (4) действительно устанавливает определенные требования к информации, которым должен следовать контролер, но это не обязательно делает согласие конкретным, предоставленным свободно, ясным и понятным для субъекта данных.

Что касается отзыва согласия, Регламент устанавливает, что субъект данных должен иметь возможность отозвать согласие в любое время. Субъект данных должен быть проинформирован до предоставления согласия о возможности отзыва согласия всякий раз, когда согласие используется на законном основании. Также указано, что «отозвать согласие будет так же легко, как и дать согласие» (см. Статью 6 (3) Общего регламента ЕС по защите персональных данных). Таким образом, поскольку отзыв влияет на законность обработки с момента отзыва, он может иметь отдельный подраздел, в котором будут выделены все соответствующие компоненты.[10] На данный момент, отзыв согласия в казахстанских поправках упоминается, но нет четких требований к тому, как он должен быть обработан контролером и как быстро.

В ходе обсуждения 01.06.2021 возник вопрос, решен ли обмен личными данными на основании согласия, если личные данные находятся в «открытом источнике».[11]

---

[8] См. Изложение 43 регламента: «Чтобы согласие было дано свободно, согласие не должно служить законным основанием для обработки персональных данных в конкретном случае, когда существует явный дисбаланс между субъектом данных и контролером, в частности, когда контролером является государственный орган, и поэтому маловероятно, что согласие было дано свободно

[9] Согласно статье 6 (3) Регламента, это правовое основание может содержать конкретные положения для адаптации применения правил Регламента, в том числе: общие условия, регулирующие законность обработки контролером; типы данных, которые подлежат обработке; заинтересованные субъекты данных; лица и цели, для которых личные данные могут быть раскрыты; ограничение цели; сроки хранения; а также операции обработки и процедуры обработки, включая меры по обеспечению законной и справедливой обработки, например, для других конкретных ситуаций обработки, предусмотренных в главе IX Регламента. Закон Союза или государства-члена должен соответствовать цели, представляющей общественный интерес, и быть соразмерным преследуемой законной цели».

[10] Руководство Европейского надзорного органа о согласии, стр.23-25.

[11] Поправка гласит: «Распространение персональных данных, опубликованных в открытых источниках, допускается с согласия субъекта данных или его законного представителя. Разрешается распространение опубликованных в открытых источниках персональных данных со ссылкой на источник информации ».

Это рассматривалось как потенциальный риск ограничения свободы выражения мнения на основании защиты личных данных. Это очень важный аспект и этот вопрос также регулируется Общим регламентом ЕС по защите персональных данных. В положении 153 Регламента говорится, что «законодательство государств-членов должно согласовывать правила, регулирующие свободу выражения мнений и информации, включая журналистское, академическое, художественное и / или литературное выражение, с правом на защиту личных данных в соответствии с настоящим Регламентом». Закон о регулировании был предоставлен государствам-членам в соответствии со статьей 85 (2) Регламента. Таким образом, то, как каждое государство-член регулирует этот баланс, зависит от национального законодательства, а не от законодательства ЕС, такого как Регламент. В примере с Эстонией статья 4 Закона о защите личных данных гласит[12]:

§ 4. Обработка персональных данных в журналистских целях

Персональные данные могут обрабатываться и раскрываться в средствах массовой информации в журналистских целях ***без согласия субъекта данных****, в частности, освещаться в средствах массовой информации, если к этому есть общественный интерес и это соответствует принципам журналистской этики.* ***Раскрытие персональных данных не должно наносить чрезмерный ущерб правам любых субъектов данных****.*

Глядя на изменения в регулировании персональных данных в Казахстане, следует параллельно рассматривать положения о свободе выражения мнения, поскольку они оба являются основными правами и одно нельзя назвать более важным, чем другое - они должны быть сбалансированы.

Кроме того, публикация данных из открытых источников также может регулироваться конкретным законодательством, а распространение данных на основе согласия может использоваться только при отсутствии других юридических оснований, позволяющих использовать эти личные данные. Смысл этого заключается в следующем: если есть закон, который гласит, например, что информация о доходах государственных служащих в Эстонии является публичной информацией, то эту информацию можно свободно использовать.[13] Однако, если бы для этого не было конкретного правового основания, необходимо было бы получить согласие (отвечающее всем требованиям, упомянутым выше) каждого государственного должностного лица, поскольку в противном случае для этого не было бы никаких юридических оснований.

[12] Закон о защите персональных данных, https://www.riigiteataja.ee/en/eli/523012019001/consolide.

[13] Заработная плата публикуется на основании подпунктов 65 (1) и 65 (2) Закона о государственной службе:
§ 65. Раскрытие информации о вознаграждении
(1) Базовая заработная плата должностного лица на текущий календарный год публикуется на центральной веб-странице государственной службы не позднее 1 мая.
(2) Базовая заработная плата, переменная заработная плата и другие доходы, возникающие в результате его или ее функций, публикуются в общей сумме за предыдущий календарный год на центральной веб-странице государственной службы не позднее 1 мая.

Здесь также вступают в игру исключения (например, в журналистских целях) - в некоторых случаях общественность имеет право знать и тогда это также может подпадать под исключение для журналистских целей, когда никакого согласия не требуется. Другой вопрос, имеет ли общественность право знать, сколько зарабатывает каждый государственный служащий, но знание того, использовались ли государственные средства в соответствии с применимыми законами, безусловно, является аспектом, входящим в общественные интересы. Таким образом, на этот вопрос нет конкретного ответа, но рекомендуется сбалансировать фундаментальное право на защиту данных с правом на свободу выражения мнений, поскольку в противном случае право на защиту данных действительно может быть использовано для ограничения свободы выражения мнения.

2.3. Реестр операторов персональных данных (РОПД)[14]

Что было выявлено касательно РОПД:

- РОПД больше не включен в пакет поправок КИБ МЦРИАП;
- Планировалось, что РОПД будет списком всех операторов персональных данных;
- РОПД был нацелен на охват всего жизненного цикла обработки данных - от начала до завершения обработки;
- Если организация не являлась частью РОПД, она не может выполнять действия по обработке данных.

РОПД стал бы большим препятствием для компаний и мог бы стать средством блокировки выхода компаний на рынок, поскольку значительная часть деятельности таких компаний, если не вся, связана с обработкой персональных данных. Кроме того, введение единообразного требования для регистрации в РОПД будет означать, что правительству потребуется значительный объем ресурсов для подключения всех правомочных операторов.

Как обсуждалось на заседании 18 мая 2021 года, реестр может быть сделан для небольшого сегмента компаний, которые занимаются обработкой особых категорий персональных данных[15] (например, данных о здоровье), и, следовательно, с операторами, которые обрабатывают данные, и имеют большее влияние на вовлеченных людей.

[14] В последней из опубликованных версия поправок идея создания реестра операторов персональных данных была удалена по рекомендациям экспертной группы (прим. Заказчика)

[15] В статье 9 (1) Общего регламента ЕС по защите персональных данных (2016/679 / EU) особые категории персональных данных определяются как персональные данные, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения или членство в профсоюзах, а также обработка генетических данных, биометрических данных с целью однозначной идентификации физического лица, данных, касающихся здоровья, или данных, касающихся половой жизни или сексуальной ориентации физического лица.

В Эстонии такой реестр существовал для компаний, обрабатывающих особые категории данных (например, медицинские карты) до 2018 года. Регистрация медицинской компании в реестре была предварительным условием для получения лицензии на деятельность в медицинском секторе. В 2018 году вступил в силу Общий регламент ЕС по защите персональных данных, и реестр был помещен в архив. Теперь компании, обрабатывающие особые категории персональных данных, должны нанять сотрудника по защите данных и вести журнал обработки данных.[16]

В результате, отказ от идеи унифицированного РОПД, вероятно, будет приветствоваться, но в связи с этим стоит изучить конкретные правила для объектов, которые выполняют более рискованные операции обработки. Чем более конфиденциальные, чувствительные данные они обрабатывают, тем выше риски и тем шире обязанности по проявлению добросовестности.

Еще одно требование, которое можно здесь принять во внимание, - это требование Общего регламента ЕС по защите персональных данных о проведении оценки воздействия на защиту данных в тех случаях, когда характер, объем, контекст и цели обработки могут привести к высокому риску для прав и свобод физических лиц.[17]

Это требование должно применяться как к организациям государственного, так и частного секторов, и потребует от организаций подумать о связанных с этим рисках до начала обработки данных. Согласно регламенту ЕС, не существует обязательств показывать оценку воздействия какому-либо надзорному органу до начала деятельности по обработке, но если есть жалоба со стороны субъекта данных или нарушение данных, надзорный орган всегда может запросить документ об оценке воздействия во время официальной процедуры. Если такая оценка не была проведена, компания будет оштрафована за несоблюдение.

Поскольку РОПД также является системой, которая должна быть интегрирована с СЗПД, экспертам РЕ неясно, как это влияет на СЗПД.

2.4. Прием и рассмотрение жалоб, мониторинг и инспекции

Что эксперты РЕ выяснили в данной связи:

- Поправки не относятся к ресурсам, связанным с рассмотрением жалоб и инспекциями.

Очень важно, чтобы изменения были не только отражены в нормативных документах, но и должны быть выделены ресурсы для проведения необходимых проверок, инспекций, жалоб и мониторинга. В данном ключе важное значение будет иметь лучшее знание планируемых ресурсов.

[16] См. Статью 30 Общего регламента ЕС по защите персональных данных
[17] См. Статью 35 Общего регламента ЕС по защите персональных данных

Еще один элемент, котором следует учесть, - это тот факт, что необходимы разъяснения и предоставление рекомендаций в отношении новой системы. Эстония предлагает несколько хороших примеров - Налогово-таможенный департамент и Управление по защите данных, - где правительство не только контролирует и обеспечивает соблюдение, но также отвечает на вопросы соответствующих сторон и действует в качестве советника для соответствующих заинтересованных сторон. Это означало бы изменение культуры, но, было бы намного лучше, если бы заинтересованные стороны были самодисциплинированными участниками процесса и действовали не только из страха перед проверкой. Это не столько вопрос регулирования, сколько культуры лидерства. Некоторые ресурсы следует выделить на консультационные услуги.

Орган, осуществляющий надзор, должен быть независимым. В ЕС органы по защите данных (надзорные органы по вопросам защиты данных) должны быть независимыми органами.[18] Это означает, что на такой орган нельзя влиять или он не контролируется каким-либо министерством или агентством через ресурсы. Должностные лица должны быть независимыми.

3. Выводы

Предлагаемые изменения по сути нейтральны и могут быть использованы как для пользы (усиление прозрачности и контроль граждан над личными данными), так и для вреда (контроль над гражданами и блокирование выхода нежелательных компаний на рынок). Таким образом, у Клиента больше возможностей оценить наиболее вероятный исход. Однако, чтобы смягчить или избежать негативных последствий, в предложениях КИБ МЦРИАП должны быть четко указаны ограничения для СЗПД и регистра согласия – какова их *определенная* цель, как долго хранятся данные, с кем они делятся и так далее.

Независимый надзорный орган (или, если он еще не существует, какая-то другая специальная группа, уполномоченная на это), должен иметь возможность изучить вопрос и вынести решение, существует ли риск для основных прав на неприкосновенность частной жизни и защиту данных, и как эти риски уменьшаются. Предлагаемые изменения во многом зависят от того, как они будут реализованы. Пример Эстонии и движение блокчейнов во всем мире явно продвигают децентрализованные модели над централизованными. Однако поддержание децентрализованной системы означает, что между сторонами должна быть хорошая координация, а согласование общей цели требует больше времени. Но снизить риски, связанные с конфиденциальностью, целостностью и доступностью личных данных, проще в децентрализованной системе, потому что, если часть системы будет взломана, другие части могут продолжить работу. Изменения в

[18] Статья 51 (1) Общего регламента ЕС по защите персональных данных: Каждое государство-член должно предусмотреть, чтобы один или несколько независимых государственных органов несли ответственность за мониторинг применения настоящего Регламента с целью защиты основных прав и свобод физических лиц в отношении обработки данных и должны способствовать свободному обмену личными данными внутри Союза («надзорный орган»).

законодательстве о защите данных могут повлиять на ситуацию со свободой выражения мнения. Следовательно, важно сбалансировать два основных права, чтобы в результате не ущемлялась свобода выражения мнений.

Участникам рынка нужно время, чтобы отреагировать на изменения. Поэтому, когда это возможно, изменения следует внедрять поэтапно, и в правовом акте может быть указано, когда определенные изменения вступят в силу (*vacatio legis*).