Сравнительный анализ законодательства стран СНГ и опыт стран Евросоюза (GDPR): Штрафы и санкции в отношении утечек персональных данных

Жылдыз Чынарбековна Тегизбекова

к.ю.н., доцент Международного университета Ала-Тоо, профессор университета КАЗГЮУ, Астана

27 января 2023 года

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА СТРАН СНГ И ОПЫТ ЕВРОСОЮЗА (GDPR): ШТРАФЫ И САНКЦИЙ В ОТНОШЕНИИ УТЕЧЕК ПЕРСОНАЛЬНЫХ ДАННЫХ

«Privacy Day – защита персональных данных в Кыргызской Республике»

Жылдыз Тегизбекова,
профессор КАЗГЮУ, Казахстан
Университет АлаТоо, Кыргызстан

Только **15%**

людей чувствуют, что у них есть полный контроль над информацией, которую они оставляют в сети Интернет *(прим. в ЕС)*

http://ec.europa.eu/justice/smedataprotect/index_en.htm

Утечка данных Mail.ru

- 13 января 2023 года в сети Интернет неизвестными были опубликованы данные **3 505 918 пользователей** почтового сервиса Mail.ru. Публикация содержала следующую информацию о пользователях: ID в системе; фамилия и имя пользователя; никнейм пользователя; номер телефона (1 647 711 уникальных номера); адрес электронной почты.
- Из которых 580 000 – данные жителей Казахстана

Утечка данных Mail.ru

Согласно п. 1 ч. 3.1 ст. 21 Федерального закона «О персональных данных» (ФЗ-152), оператор обязан в случае утечки данных уведомить уполномоченных орган в течении 24 часов с момента обнаружения факта утечки данных, уполномоченным органом постановлением правительства был определен Роскомнадзор.
Однако почтовый сервис Mail.ru не уведомил Роскомнадзор об утечке.

Роскомнадзор проведет проверку на предмет принятия оператором необходимых мер по обеспечению безопасности персональных данных при их обработке, в соответствии со ст.19 закона, и, более того, если кто-то из пользователей решит, что потерпел моральный вред, расследование будет и по факту этого заявления. От результатов расследования будет зависеть, понесет ли Mail.ru ответственность за свои действия, в том числе, возникнет ли обязательство возместить пользователям моральный ущерб.

Ст.13.11 КоАП РФ предусмотрен штраф не более 100 000 руб. Однако за нарушение требований о локализации данных штраф может составить до 6 000 000 руб., и до 18 000 000 руб. при повторном нарушении.

Что было бы, если такая утечка персональных данных произошла в ЕС?

Штрафы в ЕС

- 4% от годового оборота или 20 миллионов евро (выбирается большой показатель)

- Остальные нарушения:
  - 2% от годового оборота или 10 миллионов евро (выбирается больший показатель)

Примеры реальных штрафов по GDPR https://www.enforcementtracker.com/

ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure

Date **30 October 2020**

Type **News**

The ICO has fined Marriott International Inc £18.4million for failing to keep millions of customers' personal data secure.

Marriott estimates that 339 million guest records worldwide were affected following a cyber-attack in 2014 on Starwood Hotels and Resorts Worldwide Inc. The attack, from an unknown source, remained undetected until September 2018, by which time the company had been acquired by Marriott.

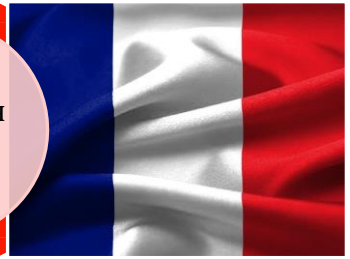
The personal data involved differed between individuals but may have included names, email addresses, phone numbers, unencrypted passport numbers, arrival/departure information, guests' VIP status and loyalty programme membership number.

The precise number of people affected is unclear as there may have been multiple records for an individual guest. Seven million guest records related to people in the UK.

The ICO's investigation found that there were failures by Marriott to put appropriate technical or organisational measures in place to protect the personal data being processed on its systems, as required by the General Data Protection Regulation (GDPR).

Утечка персональных данных в ЕС

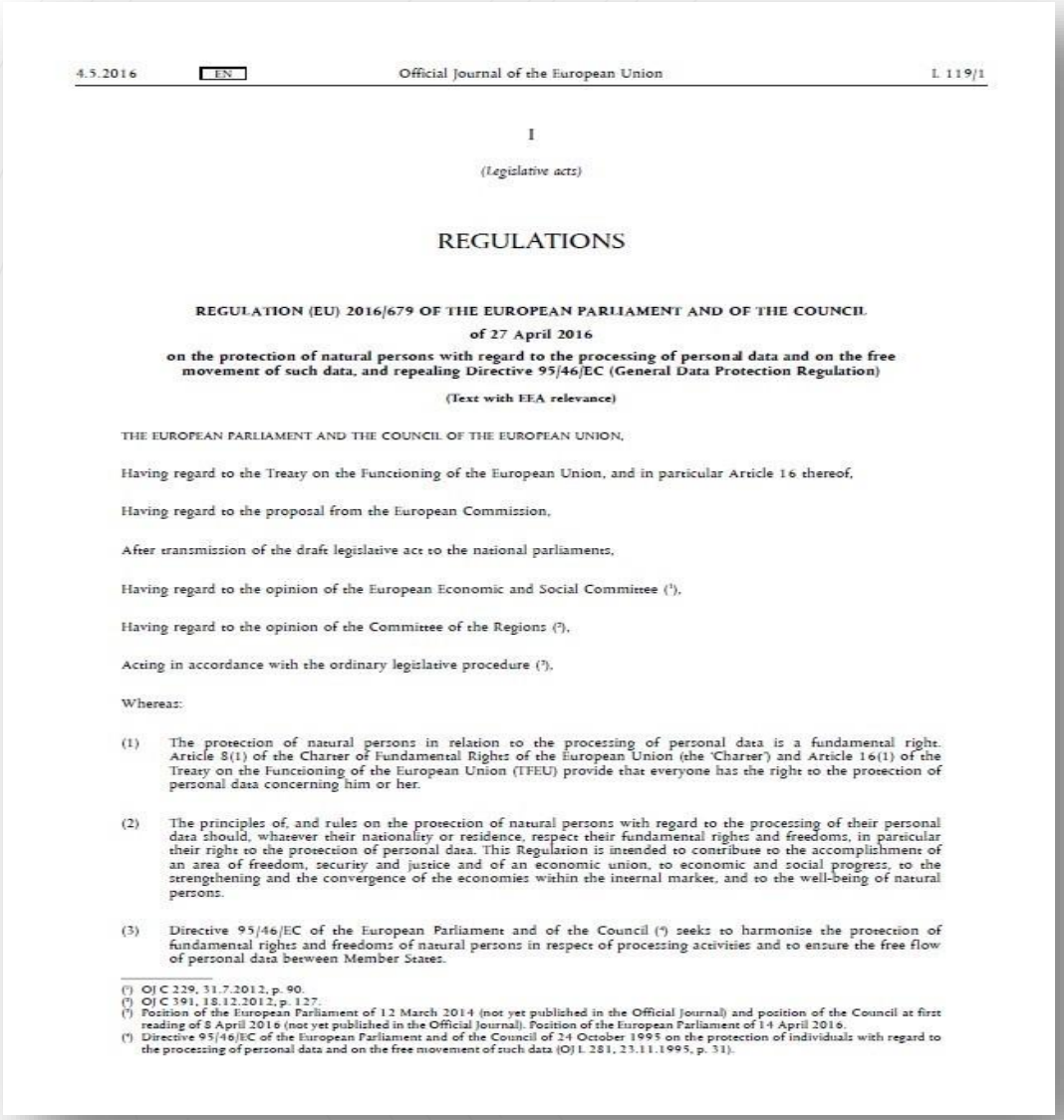
Ирландия
Твиттер



Франция
Google

Германия
H&M

Что такое GDPR?



4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council (4) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(1) OJ C 229, 31.7.2012, p. 90.
(2) OJ C 391, 18.12.2012, p. 127.
(3) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
(4) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

- General Data Protection Regulation (GDPR) – это новый европейский регламент по защите персональных данных, единый для 28 стран ЕС
- Заменяет собой Directive 95/46/EC (1995)
- Принят 27 April 2016
- Вступает в силу 25 May 2018
- Регулятор: European Parliament, Council of the European Union
- Очень много положений про «цифровые технологии» (IoT, профилирование, BigData, cookies и пр.)

GDPR EU

- ***персональные данные - это любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (субъект данных), по которой прямо или косвенно можно его определить.*** К такой информации относится в том числе имя, данные о местоположении, онлайн идентификатор или один или несколько факторов характерных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица (п. 1 ст. 4). Определение широкое и достаточно четко дает понять, что даже IP адреса также могут быть персональными данными.

Понятие утечки персональных данных

- Утечка данных (data leak) — «**Утечка персональных данных**» – означает нарушение безопасности, приводящее к случайному или противозаконному **уничтожению**, **потере**, **изменению**, **несанкционированному раскрытию** или **доступу** к персональным данным, переданных, хранящихся или обработанных иным образом.

СТ.4 (12) GDPR

- *Примечание: В законодательстве стран СНГ нет понятия утечки персональных данных*

Почему важно контролировать утечки?

GDPR: *“(85) **Утечка персональных данных**, если она надлежащим образом и своевременно не была устранена, **может привести к физическому, материальному или нематериальному ущербу** для физических лиц, таким как **утрата контроля** над персональными данными или ограничение их прав, дискриминация, кража идентификационных данных или мошенничество с персональными данными, финансовые потери, несанкционированный отказ от псевдонимизации, ущерб репутации, нарушение конфиденциальности персональных данных, защищённых профессиональной тайной, или любые иные существенные экономические или социальные потери для соответствующих физических лиц…”*

Уведомление об утечках по GDPR

Процедура обращения при утечке ПД в ЕС

Supervisory authority (Надзорный орган) **Art.33**

Data subjects (Субъекты данных) **Art.34**

	Уведомление надзорного органа	Уведомление субъектов
Когда можно НЕ уведомлять	• Если риск минимальный	• Если риск НЕ большой • Если приняты надлежащие меры (например, криптографическая защита) • Если приняты адекватные последующие меры • Если требуются несоразмерные усилия
Состав уведомления	• Реквизиты DPO • Возможные последствия • Принятые меры • Характер утечки (категории и количество пострадавших субъектов и записей)	• Реквизиты DPO • Возможные последствия • Принятые меры
Срок уведомления	• Без неоправданной задержки и, не позднее чем через **72 часа** после выявления	• Без неоправданной задержки

Базовая идея про штрафы GDPR

Статья 83 GDPR

Общие условия наложения административных штрафов

1. Каждый надзорный орган должен обеспечить, чтобы наложение административных штрафов, в порядке настоящей Статьи в отношении нарушений положений настоящего Регламента, предусмотренных в параграфах 4, 5 и 6, в каждом отдельном случае, было **эффективным**, **соразмерным** и имело **сдерживающее воздействие**.

Полномочия Надзорного органа

по ст.58.1 и 58.2 GDPR

По разбирательствам	По устранению недостатков
• Запрос информации от контролера и обработчика • Аудиторские проверки защиты данных • Обзор сертификаций • Уведомление о нарушениях • Запрос доступа к ПДн • Запрос доступа к оборудованию, средствам обработки и в помещения	• Предупреждение • Выговор • Предписание соблюдать запросы субъектов • Предписание выполнить требования GDPR • Предписание об уведомлении об утечках • **Ограничение обработки ПДн (втч и запрет)** • Предписание об устранении нарушений • Отзыв сертификатов • **Наложение административных штрафов** • Предписание о приостановке передачи данных в третьи страны

ПОЧЕМУ GDPR?

- Реальный фокус на права субъектов ПДн с учетом современных ИТ
- Реальные штрафы и полномочия SA
- Защита ПДн с учетом экономической целесообразности
- Очень много разъяснений и примеров
- Упрощенные требования для SME (до 250 человек): без DPO, без записей об обработке ПДн, без уведомления об утечках

Согласно Закону Кыргызской Республики «Об информации персонального характера» Персональные данные – это любая информация, используя которую человека можно прямо или косвенно узнать (идентифицировать).

Например:

ФИО;

персональный идентификационный номер (ПИН/ИНН);

биометрические данные;

семейное положение;

онлайн-идентификатор (имя пользователя в социальных сетях, IP-адрес);

кадры камеры видеонаблюдения, позволяющие идентифицировать физическое лицо;

другая информация.

Примерами **специальной категории («чувствительных») персональных данных** являются биометрические данные граждан, медицинские записи больных, банковские реквизиты. Обработка и передача такой информации требует дополнительных мер контроля безопасности

Согласно Закону Республики Казахстан персональные данные - сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.

Персональные данные по своей доступности подразделяются на общедоступные и ограниченного доступа.

Общедоступными персональными данными являются персональные данные или сведения, на которые в соответствии с законодательством Республики Казахстан не распространяются требования соблюдения конфиденциальности, доступ к которым является свободным с согласия субъекта (информация из СМИ, телефонных справочников и т.п.).

Персональными данными ограниченного доступа являются персональные данные, доступ к которым ограничен законодательством Республики Казахстан. К ним относятся установочные данные лица (фамилия, имя, отчества, год, дата рождения, национальность), сведения о месте жительства (место регистрации), индивидуальном идентификационном номере (ИИН), документах, удостоверяющих личность (номер) и другие сведения.

Согласно Закон **«О персональных данных»**

Персональные данные - зафиксированная на электронном, бумажном и ином материальном носителе информация, относящаяся к определенному физическому лицу или дающая возможность его идентификации.

Конкретного перечня в законе нет, что оставляет некоторый простор для толкования, но, как правило, персональные данные включают такую информацию, как ФИО, пол, дата и место рождения, место жительства, образование, семейное положение, занимаемая должность и другое.

К персональным данным во всем мире также относятся заработная плата и другая информация, которая не подлежит разглашению. Это может быть не только в виде текста, но и фотографии, и видео.

Информация о расе, религии, мировоззрении, политических убеждениях, частной жизни, судимости и состояния здоровья считается специальными персональными данными. Их обработка запрещается кроме некоторых случаев (например, если человек сам опубликовал их в общедоступных источниках).

Модельный закон «О персональных данных» для стран СНГ

- *Персональные данные* - информация (зафиксированная на материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним. К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие.

Принят на сорок восьмом пленарном заседании Межпарламентской Ассамблеи государств - участников СНГ
(Постановление от 29 ноября 2018 года №48-9)

Причины утечек

- Любая организация, которая в своей деятельности обрабатывает персональные данные, обязана предпринять комплекс организационных и технических мер, направленных на их защиту. Перечень этих мер и способов регламентируется для каждой группы данных. При разработке системы таких технических и административных решений используется модель угроз, в которой учитываются риски двух типов:

1. внешние;
2. инсайдерские.

Внутренние реализуются наиболее часто. Гражданин предоставляет сведения о себе во множестве случаев в медицинском учреждении, в туристическом агентстве, в котором для оформлении визы он практически полностью раскрывает сведения о своем финансовом статусе. Согласие на обработку персональных данных зачастую не подписывается. Таким образом, паспортные данные, сведения о недвижимости, доходах, операциях по банковской карте оказываются в незащищенном виде в компьютере, на котором может не быть даже антивирусной защиты. В этом случае доступ к ним становится возможным

Внешние - представляющих собой неправомерное проникновение в защищенный информационный периметр организации-оператора, – хакерские атаки, которые в странах СНГ редко становятся серьезными угрозами для жизни и здоровья граждан. Многие базы информационные системы защищены серьезно, а утечка массива сведений, защищенных средствами криптографической защиты, без возможности персонификации, не несет серьезных рисков. Сократилось и количество внешних атак на сайты банков.

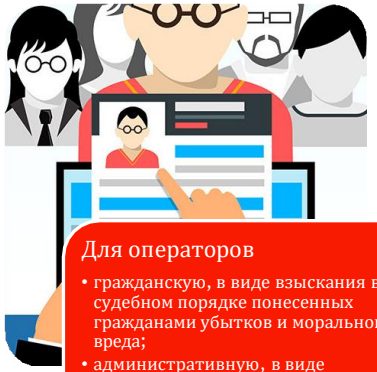
Последствия утечек

Для граждан

- от разглашения любой информации, имеющей отношение к личности;
- от шантажа;
- от неправомерного списания средств с банковской карты;
- от вмешательства в личную жизнь;
- от угроз детям, например, в случае публикации в СМИ данных о школах, где они учатся.

Для бизнеса

- Внутренние коммуникации: заметки, электронные письма и документы с подробным описанием операций компании.
- Метрики: статистика эффективности, прогнозы и другие собранные данные о компании.
- Стратегия: детали рекламных сообщений, дорожные карты, адресные картотеки и другая важная бизнес-информация.
- **Коммерческие тайны**
- **Аналитика**



Для операторов

- гражданскую, в виде взыскания в судебном порядке понесенных гражданами убытков и морального вреда;
- административную, в виде наложения штрафа, приостановления или запрета деятельности, связанной с обработкой персональных данных;
- уголовную, в случае неправомерного распространения ПДн, причинившего существенный ущерб и передаче информации в правоохранительные органы.

Утечки персональных данных в Кыргызстане

Дело Безопасного города

Дело Банка Бай Тушум

Дело сайта Жогорку Кенеша

Дело с ПЦР-тест

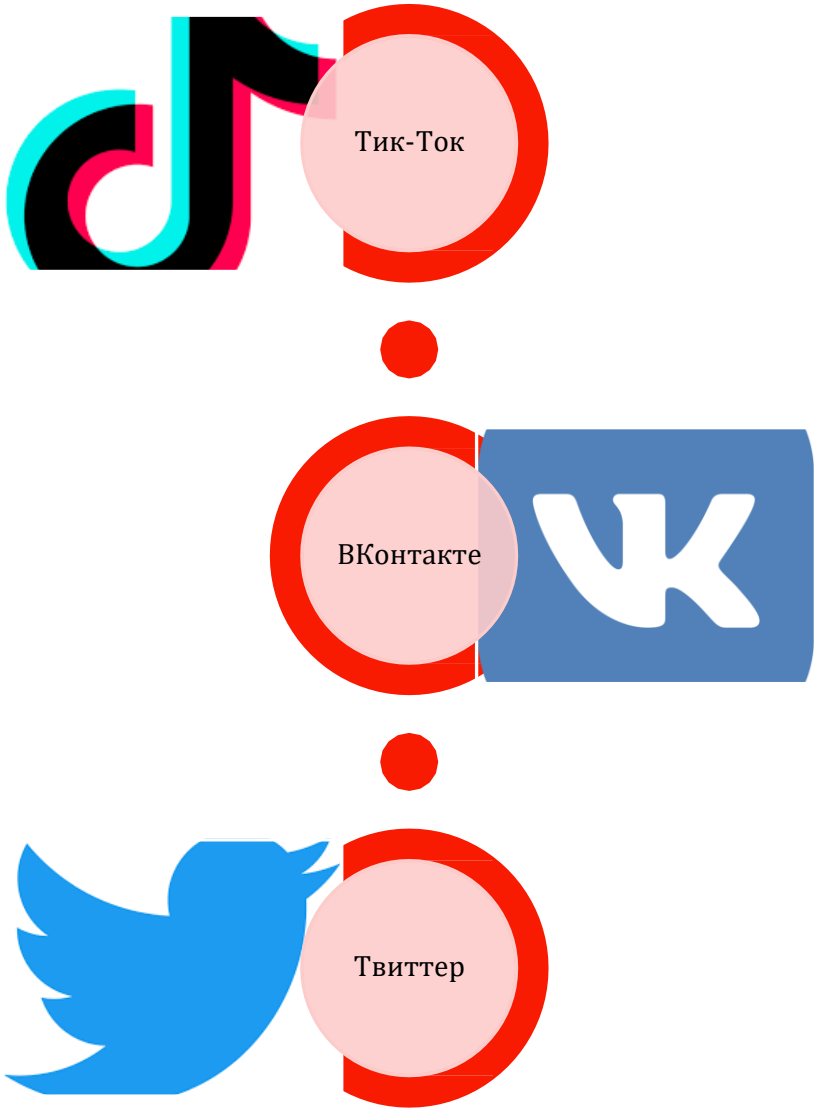
Утечки персональных данных в Казахстане

Дело Qihoo 360

Дело ЦИК

Дело Qazqom банка

Утечки персональных данных в Узбекистан



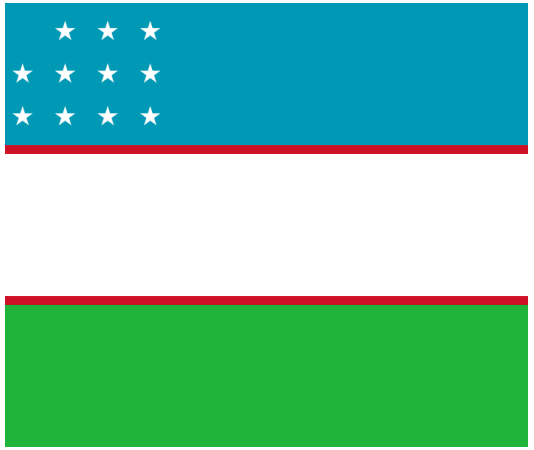
Какой орган рассматривает вопросы по персональным данным?

ГАЗПД

Государственной агенство по защите персональных данных при Кабинете Министров Кыргызской Республики

КИБ

Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики



Узкомназорат

Государственной инспекции по контролю в сфере информатизации и телекоммуникаций Республики Узбекистан

Европейский совет по защите персональных данных

Процедура обращения при утечке ПД в Казахстане

- При обнаружении фактов незаконного сбора или утечки персональных данных, а также нарушения правил использования ЭЦП граждане могут обратиться в уполномоченный орган по защите персональных данных (УО) любым удобным и доступным для него способом, позволяющем зарегистрировать обращение (в электронном виде, на бумажном носителе, посредством почты или портала «Электронного правительства», путем направления обращения на блог руководителя, электронного письма на ведомственную электронную почту и т.д.).
- о дополнительным вопросам касательно фактов незаконного сбора или утечки персональных данных, а также нарушения правил использования ЭЦП Вы можете написать на электронную почту kib@mdai.gov.kz
- ***Примечание***: требуется для онлайн платформ, собирающие ПД, обязаны иметь сервера на территории Казахстана.

Ответственность

Штрафы при утечке ПД в Казахстане

Часть 1 ст. 79 КоАП РК

Незаконные сбор и (или) обработка персональных данных, если эти деяния не содержат признаков уголовно наказуемого деяния:

Субъект-нарушитель	Размер штрафа (в МРП на 2022 год)	Размер штрафа (в тенге на 2022 год)
Физические лица (ФЛ)	10	30 630
Должностные лица, частные нотариусы, частные судебных исполнители (ЧСИ), адвокаты, субъекты малого предпринимательства, некоммерческие организации (НКО)	20	61 260
Субъекты среднего предпринимательства	30	91 890
Субъекты крупного предпринимательства	70	214 410

Часть 2 настоящей статьи КоАП РК Те же деяния, совершенные собственником, оператором или третьим лицом с использованием своего служебного положения, если эти действия не влекут установленную законом уголовную ответственность:		
ФЛ	50	153 150
Должностные лица, субъекты малого предпринимательства, НКО	75	229 725
Субъекты среднего предпринимательства	100	306 300
Субъекты крупного предпринимательства	200	612 600
Часть 3 настоящей статьи КоАП РК Несоблюдение собственником, оператором или третьим лицом мер по защите персональных данных, если это деяние не содержит признаков уголовно наказуемого деяния:		
ФЛ	50	153 150
Должностные лица, субъекты малого предпринимательства, НКО	100	306 300
Субъекты среднего предпринимательства	150	459 450
Субъекты крупного предпринимательства	200	612 600
Часть 4 настоящей статьи КоАП РК Деяние, предусмотренное частью третьей настоящей статьи, повлекшее утерю, незаконный сбор и (или) обработку персональных данных, если эти деяния не влекут установленную законом уголовную ответственность:		
ФЛ	200	612 600
Должностные лица, субъекты малого предпринимательства, НКО	500	1 531 500
Субъекты среднего предпринимательства	700	2 144 100
Субъекты крупного предпринимательства	1 000	3 063 000

Уголовная Ответственность

при утечке ПД в Казахстане

ст. 147 УК РК

Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите

Часть статьи	Наказание					
	Штраф (в МРП и в тенге)	Исправительные работы	Общественные работы	Ограничение свободы	Лишение свободы	Атимия[1]
Часть 1 Несоблюдение мер по защите персональных данных лицом, на которое возложена обязанность принятия таких мер, если это деяние причинило существенный вред правам и законным интересам лиц	3 000 МРП / 9 189 000 тенге	3 000 МРП / 9 189 000 тенге	600 часов	2 года	2 года	до 3 лет

Уголовная Ответственность при утечке ПД в Казахстане

ст. 211 УК РК
Неправомерное распространение электронных информационных ресурсов ограниченного доступа

Часть статьи	Наказание						
	Штраф (в МРП и в тенге)	Исправительные работы	Общественные работы	Арест	Ограничение свободы	Лишение свободы	Атимия
Часть 1 Неправомерное распространение электронных информационных ресурсов, содержащих персональные данные граждан или иные сведения, доступ к которым ограничен законами Республики Казахстан или их собственником или владельцем	200 МРП / 612 600 тенге	200 МРП / 612 600 тенге	180 часов	50 суток с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового	x	x	до 3 лет

Процедура обращения при утечке ПД в Кыргызстане

- Согласно статье 7 Закона Кыргызской Республики «О порядке проведения проверок субъектов предпринимательства»
- В случае нарушения ПД, гражданин может обратиться в Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики основаниям для проверок является получение уполномоченным органом письменного заявления физического или юридического лица о нарушении субъектом проверки прав и интересов заявителя, письменного обращения руководителя органа местного самоуправления о нарушении субъектом проверки прав и интересов населения данной административно-территориальной единицы с приложением документов, материалов и иных подтверждающих сведений о нарушении субъектом предпринимательства законодательства Кыргызской Республики.
- **Срок** внеплановой проверки не может превышать 3 рабочих дней.
- **Решение** по жалобе должны быть готова течение 15 рабочих дней.
- ***Примечание***: В Кыргызской Республике не требуют для онлайн платформ иметь сервера на территории своего государства, то есть данные граждан могут храниться на территории другого государства.

Процедура обращения при утечке ПД в Узбекистане

- Согласно статье 27^1 Закона Республики Узбекистана «О персональных данных» сервера хранения ПД должны храниться на территории Узбекистана. В связи с чем был запущен реестр по Государственный центр персонализации (ГЦП) опубликовал реестр нарушителей закона о персональных данные. Выяснилось, что помимо Twitter, TikTok и «ВКонтакте», о которых сообщал «Узкомназорат», в Узбекистане ограничена работа Skype и WeChat.
- Предписание всем этим сервисам было выдано в середине июня, черед две недели они были внесены в реестр нарушителей. Компании могут выйти из него, если локализуют сервера в стране, как это сделал, к примеру, Yandex Go.
- Однако ГЦП РУз согласно статье 8 вышеуказанного закона, они не разрешают споры, либо реагируют в случае нарушения ПД. Однако из текста статьи 32 Закона, скорее всего в судебном порядке рассматривается вопрос утечки персональных данных.

Реестр нарушителей прав субъектов персональных данных

Социальная сеть «TikTok»

Наименование информационного ресурса	Социальная сеть «TikTok»
Информация о владельце и (или) операторе	Социальная сеть «TikTok»
Сведения по идентификации информационного ресурса, наименование уникальных доменных имен, адрес веб-сайтов и/или сетей, позволяющих идентифицировать в информационной сети интернет	https://www.tiktok.com
Номер и дата предписания Узкомназорат	01-20/1303 / 16-06-2021
Номер и дата представления Узкомназорат	01-20/1455 / 02-07-2021
Дата установления ограничения	02-07-2021
Статус ограничения	Есть ограничение

Ответственность в случае нарушения

Кыргызская Республика

- В Кыргызской Республике предусмотрена административная ответственность, согласно Статье 228[1].
- Кодекса о правонарушениях Нарушение требований по защите информации персонального и коммерческого характера,
- Однако, уголовной ответственности прямо не предусмотрена, однако в соответствии с главой 40 Уголовного кодекса Кыргызской Республики предусмотрены преступления против кибер-безопасности, которую возможно применить для толкования в случае утечки ПД.

Республика Казахстан

- В Республике Казахстан предусмотрена административная и уголовная ответственности за нарушение законодательства о персональных данных и их защите. Статья 79 “Нарушение законодательства Республики Казахстан о персональных данных и их защите” Кодекса об административных правонарушений Республики Казахстан предусматривает ответственность, к которым должны привлекаться лица, нарушившие Закон Республики Казахстан “О персональных данных и их защите”.
- Согласно статье 147 Уголовного кодекса Республик Казахстан, предусмотрена уголовная ответственность за персональных данных граждан.

Республика Узбекистан

- В Республике Узбекистан предусмотрена административная ответственность, так же как и уголовная ответственность, соответствующие поправки были внесены в 2021 году.
- Отличительной чертой среди этих стран является ответственность за Нарушение законодательства о накопительном пенсионном обеспечении граждан

СПАСИБО!

ВАШИ ВОПРОСЫ?

ПРОФЕССОР ЖЫЛДЫЗ ТЕГИЗБЕКОВА

ZH_TEGIZBEKOVA@KAZGUU.KZ