SIA "DLV"

УСЛОВИЯ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Содержание

1. Цель условий и термины

Цель этих условий обработки и защиты Персональных данных (далее – **Условия**) установить для DLV:

- мероприятия организации и совокупность необходимых технических средств, которые обеспечивают честную и законную обработку и использование Персональных данных только в предусмотренных целях, их хранение, возобновление, вид исправления и удаления, обеспечивая защиту прав любого физического лица на свои Персональные данные;

- выполненные обязательные технические и организационные требования защиты обработки Персональных данных, обрабатывая данные физических лиц и обеспечивая безопасность Информационных ресурсов и Информационных систем DLV;

- процедуру нарушения защиты Персональных данных.

Эти Условия разработаны согласно требованиям Регулы.

В этом документе используются следующие термины:

Термин (сокращение)	**Определение**
Угроза	Причины, которые не позволяют поддерживать безопасность Информационной системы в соответствии с установленными требованиями Конфиденциальности, Доступности и Целостности Информационных ресурсов. Угроза безопасности Информационной системы это намеренные (специальные) или из-за неосторожности осуществленные действия или происшествие, которые могут вызвать повреждение, уничтожение или поступление системы в распоряжение таких лиц, которые являются не уполномоченными, или из-за которых доступ к Информационным ресурсам системы может быть нарушен или невозможен. Возможность угрозы устанавливает Уязвимость системы.
Записи аудита	Записи с памяти Информационной системы, которые созданы на разных стадиях процесса обработки информации, чтобы эти записи можно было позднее в определенном порядке пересмотреть и проследить ход осматриваемого процесса.
Высоко ценная информация	Информация, используя которую не на месте, не санкционированно меняя, испортив или сделав ее недоступной уполномоченным лицам на какой-то период времени, могут возникнуть существенные и продолжительные потери, пострадать репутация DLV и может быть совершено нарушение защиты Персональных данных.
Аутентичность	Особенность, которая удостоверяет, что идентичность предмета или ресурса является такой, как заявлено.
Биометрические данные	Персональные данные, которые относятся к физическим чертам и чертам поведения, которые позволяют уникально идентифицировать это лицо, например, снимки лица или данные отпечатков пальцев.
Core HR Data	Имя, фамилия, персональный код, дата рождения, пол, фотография (изготовление пропуска), место жительства, телефон, адрес электронной почты, номер расчетного счета, персональное дело (включая информацию рабочего заявления (CV; удостоверение государственного языка, данные документов об образовании; отзывы), трудовой договор, карта Обязательной проверки здоровья, оценка рисков рабочей среды на рабочем месте Сотрудника, функция, обучения, оценка деятельности, повышения в должности, данные поведения и дисциплины), единицы департаментов /

	нанимательской деятельности, данные рабочего места, информация о заработной плате, информация о данных болезней и персонализированных данных (СГД), налоговые данные и данные социального страхования, детали номерного знака транспортного средства, данные о возрасте детей Сотрудника (Номер свидетельства о рождении детей Сотрудника и дата выдачи для предоставления дополнительного отпуска), данные об инвалидности (для предоставления дополнительного отпуска), в отдельных случаях Персональные данные для оформления рабочего пропуска (копия разрешения на пребывание, данные паспорта Сотрудника третьей страны) или визы, резервации гостиницы, данные регистрации свидетельств решений/ о браке (в случае смены фамилии)
Сотрудник	Существующие (~400), бывшие сотрудники DLV и претенденты на работу
Анализ Данных	Данные используются в том виде, который анализирует поведения и модели, и позволяет сделать выводы в каждом случае, чтобы улучшить продуктивность, конкурентоспособность и / или прибыль.
Обрабатывающий Данные	Термин “Обрабатывающий Данные” соответствует установленному в 8 пункте 4 статьи Регулы определению. Общество, которое обрабатывает Персональные данные от имени Заведующего Данных. Если общество хранит или обрабатывает Персональные данные, но не заведует (не контролирует) Персональными данными и обрабатывает Персональные данные, которые основываются согласно указаниям Заведующего Данных, тогда это общество является "Обрабатывающим Данные". В процесс обработки данных могут входить представители услуг (например, поставщик услуг расчета заработной платы, представитель IT услуг).
Заведующий Данных	Термин “Заведующий Данных” соответствует установленному в 7 пункте 4 статьи Регулы определению. Общество, которое принимает решение, почему и в каком виде (т.е., устанавливает цели и средства, с помощью которых) обрабатываются Персональные данные. Принимая решение, кто заведует Персональными данными, необходимо ответить на следующие вопросы: - кто принимает решение, какая информация будет храниться? - кто принимает решение об использовании информации и целях? - кто принимает решение о средствах обработки Персональных данных? Если общество заведует и несет ответственность за Персональные данные, находящиеся в его распоряжении), оно является Заведующим Данных.
DLV	SIA “DLV” – юридическое лицо с единым регистрационным номером Nr.40003227719, юридический адрес: Krīdenera dambis 9, Rīga, LV-1019 (DLV принадлежащая интернет страница: www.dlvbet.lv; игровые залы DLV: “Zilais Dimants”, “Dimats Z” и “Dimanta Bingo”), которое действует в статусе Заведующего Персональными данными. Список, в котором перечисляются места предоставления услуг DLV, доступен на сайте www.dlvbet.lv.
Угрозы	Любое событие, из-за которого DLV может понести потери. Угрозы могут быть различные – различные катастрофы, терроризм, убыток финансирования бюджета, повреждения коммуникаций, повреждения данных, ошибки, противозаконная или вредоносная деятельность сотрудников (также бездеятельность) и прочее.
Физическая защита	Защита Информационных ресурсов от Угроз, возникающих из-за физического воздействия на информационные носители (например кража, падение напряжения, повреждения аппаратуры и др.).

Информация ограниченного доступа	Информация внутреннего оборота, для которой заведующий Информационных ресурсов установил круг допустимых лиц.
Влияние	Результат Инцидента безопасности Информации.
Уязвимость	Несовершенство Информационной системы, что допускает осуществление какой-либо установленной Угрозы и влияние на безопасность системы.
Инцидент	Случай, при котором Угрозы Информационной системы негативно повлияли на деятельность Информационной системы, используя ее недостатки.
Информационные ресурсы, информация	Файлы данных, базы данных, архивы и др. информация (независимо от вида носителя данных).
Заведующий Информационных ресурсов	Лицо, которое несет ответственность за Информационные ресурсы (их Доступность, Целостность, Конфиденциальность, использование последствия использования) и обязанности которого установлены в нормативах DLV.
Информационная система/-ы	Ввод, хранение и обработка данных в компьютеризированной системе, которые предусматривают доступ Пользователя к хранящимся в ней данным или информации, или в какой-либо форме фиксированная структурированная совокупность Персональных данных, которая доступна, учитывая соответствующие идентифицирующие лицо критерии.
Администратор Информационной системы	Лицо, которое планирует, управляет и заведует использованием системы и которое несет ответственность за ее функционирование.
Целостность	Характеризует, в какой степени информация хранится и/или передается полной, точной, правдивой и актуальной.
Особые категории Персональных данных	В 9 статье Регулы установленные виды Персональных данных, которые раскрывают какое-либо из далее указанных сведений о лице: расу или этническое происхождение, политические взгляды, религиозные или философские взгляды или участие в профсоюзе. Особые категории Персональных данных относятся также к генетическим данным, биометрическим данным (например, отпечатки пальцев или снимки лица), данным о здоровье, данным о сексуальной жизни или сексуальной ориентации, а также любым Персональным данным, которые относятся к осудительным приговорам или уголовным преступлениям.
Классифицирование	Присвоение уровня Конфиденциальности, Доступности и Ценности.
Клиент	a) любое физическое лицо, которое использует, использовало, или выразило желание используя любые предоставляемые услуги DLV или в каком-либо другом виде связано с ними (в том числе Клиенты в игровых залах, Клиенты интерактивных интернет азартных игр, посетители); b) любое физическое лицо, которое действует от имени юридического лица, поставщика или другого бизнес партнера DLV и представляет такое юридическое лицо.
Конфиденциальность	Свойство, при котором информация не доступна или не раскрывается неуполномоченным индивидуумам, системам или процессам.
Легитимные интересы	Возникают, если обработка Персональных данных необходима в целях Легитимных интересах Заведующего Данных или Третьих лиц, исключая

	случаи, когда интересы Субъекта данных или основные права и свободы являются более важными чем такие Легитимные интересы. Примеры Легитимных интересов это обработка Персональных данных в исследовательских целях или для устранения уголовных преступлений.
Пользователь	Юридическое или физическое лицо, которое заключило договор с DLV об использовании данных (в т.ч. Сотрудники) или которое на основании запроса получает данные от DLV или в указанном в нормативных актах порядке.
Логическая защита	Защита Данных или Информационных ресурсов, которую реализовывают с помощью средств программного обеспечения, например, идентифицируя Пользователя Информационной системы, проверяя соответствие его полномочий для соответствующих действий IS, защищая информацию от намеренного или случайного изменения или удаления.
Стороны, заключающие договор	Физические лица (т.е., не общества), которые предоставляют / предоставляли DLV услуги, но не согласно трудовому договору.
Несовершенство	Характеризует степень Уязвимости системы, при реализации конкретной Угрозы, например, слабая административная система, не точно установлены обязанности, ответственность, не проводится контроль доступа или не полный контроль (как физический, так и логический доступ), нет условий безопасности Информационной системы и др.
Персональные данные	Термин “Персональные данные” соответствует установленному в 1 пункте 4 статьи Регулы определению. Любая информация о живом физическом лице, которая прямо или косвенно позволяет идентифицировать это лицо. Персональные данные могут включать имя, фамилию, персональный код, онлайн-идентификатор, информацию о месте нахождения лица или любую другую информацию, которая характерна для этого лица, и, которая позволяет идентифицировать лицо, или делает лицо идентифицируемым. Регула относится как к автоматизированным Персональным данным, так и мануальным системам регистрации данных, в которых Персональные данные доступны согласно конкретным критериям. Они могут включать хронологически расположенные списки мануальных записей, которые содержат Персональные данные. Персональные данные, которые являются псевдонимами - напр. С помощью пароля кодированные данные – могут входить в область деятельности Регулы в зависимости от того, насколько сложно присвоить псевдоним конкретному лицу.
Обработка Персональных данных	Термин “Обработка Персональных данных” соответствует установленному в 2 пункте 4 статьи Регулы определению. Любая деятельность или совокупность действий, которая проводится с Персональными данными, например, любого вида сбор Персональных данных, использование, регистрирование, организация, преобразование, распространение, уничтожение, хранение или любое другое действие, делающее Персональные данные доступными. Обработку можно производить или же мануально, или же используя автоматизированные системы, например, системы информационных технологий (соответственно интерпретируя "обрабатывать" и "обработка").
Нарушение защиты Персональных данных (далее – Нарушение)	Термин “Нарушение защиты Персональных данных” соответствует установленному в 12 пункте 4 статьи Регулы определению. Нарушение безопасности, в результате которого происходит случайное или незаконное уничтожение, потеря, преобразование, запрещенное раскрытие или доступ отосланных, хранящихся или другим образом обработанных

	Персональных данных.
Доступность	Характеризует, в каком объеме уполномоченные лица могут получать доступ к необходимой информации не позднее чем в указанное время после момента запроса Информации.
Профилирование	Термин “Профилирование” соответствует установленному в 4 пункте 4 статьи Регулы определению. Автоматизированная обработка Персональных данных, чтобы оценить конкретные персональные аспекты связанные с физическим лицом, чтобы анализировать или предусмотреть производительность, решения, желания, отношение и / или поведение лица (и соответственно интерпретируется "Профиль").
Регула	Регула 27 апреля 2016 года Европейского Парламента и Совета (ЕС) 2016/679 о защите физических лиц в отношении обработки Персональных данных и свободном обороте таких данных, и в связи с которой отменяется Директива 95/46/ЕК (Общая регула защиты данных)
Риск (риск)	Вероятная неспособность DLV в полном объеме и качественно осуществить выполнение каких-либо своих обязательств или функций. В контексте безопасности информации рассматриваются только те риски, которые связанные с функционированием Информационной системы.
Технологические ресурсы	Программное обеспечение (выполнимый программный код и файлы конфигураций, которые обеспечивают функционирование Информационной системы), компьютеры, аппаратура компьютерных сетей, линии коммуникаций и др. технические средства, которые используют для обработки, распространения и хранения информации.
Заведующий Технологических ресурсов	Лицо, которое несет ответственность за обслуживание и безопасность Технологических ресурсов.
Третье лицо	Любое лицо или общество, агентура или другая организация (которая не является субъектом данных, Заведующий Данных или Обрабатывающий Данные), кто в прямом подчинении Заведующего Данных или Обрабатывающего Данные является уполномоченным обрабатывать Персональные данные.
Ценность	Важность Информационного ресурса DLV, которую устанавливают, оценив возможные убытки, из-за которых могут возникнуть потеря, порча или попадание в руки посторонних лиц Информации.
Информация средней ценности	Информация, неуместно используя которую, не санкционированно изменяя, повреждая или делая ее недоступной уполномоченным лицам на какой-то промежуток времени, DLV может понести ощутимые потери, может пострадать репутация DLV и может быть совершено нарушение защиты персональных данных.
Общедоступная информация	Информация, которая свободно доступна Сотрудникам DLV и любому другому лицу, которое запросило эту информацию.
Информация низкого риска	Информация, неуместно используя которую, не санкционированно изменяя, повреждая или делая ее недоступной уполномоченным лицам на какой-то промежуток времени, DLV не несет значительные потери или не возникает значительное нарушение деятельности.

2. Общая информация

Субъекты данных, категории обработки Персональных данных (также Особые категории Персональных данных) и виды, цели обработки Персональных данных, источники, правовая основа, Профилирование, распространение Персональных данных, хранение Персональных данных, географическая территория обработки Персональных данных, период хранения.

Субъекты данных:	**Сотрудники**	**Стороны, заключающие договор**	**Клиенты**
Категории обрабатываемых Персональных данных, также Особые категории Персональных данных, и виды	- В отношении существующих Сотрудников Core HR Data, переписке электронной почты, снимка (видеонаблюдения), В отношении Сотрудников администраторов – данные о судимости. - В отношении бывших Сотрудников Core HR Data (бывшие Сотрудники могут запросить справки, характеристики и т.п.), переписка электронной почты, снимок (видеонаблюдение) в меньшем объеме, не храня информацию о данных болезни и данные о выходе на пенсию (СГД). - В отношении рабочих претендентов: имя, фамилия, адрес, номер телефона, CV, отзывы от предыдущих работодателей и заметки интервьюирования рабочих претендентов. **Особые категории Персональных данных:** - **Данные о здоровье** (Обязательные проверки здоровья, а также, чтобы провести расследования	Имя, фамилия, персональный код, адрес, номер телефона, адрес электронной почты, номер НДС, договор, если Сторона, заключающая договор, действует в месте, где DLV ведет видеонаблюдение, также снимок Стороны, заключающей договор **Особые категории Персональных данных**: не обрабатываются	**Данные идентификации**, например: имя, фамилия, персональный код, дата рождения, пол, фотография, данные документа удостоверяющего личность (например: данные паспорта, данные ID карты). **Контактная информация**, например: декларированный и фактический адрес места жительства, номер телефона, адрес электронной почты. **Финансовые данные**, например: информация банковской кредитной карты Клиента, чтобы выплатить денежную сумму для произведения ставки; Номер счета Клиента, на который в случае выигрыша выплачивается выигрыш. **Данные, которые получены и/или созданы, выполняя предусмотренные нормативными актами обязанности**, например: данные, которые исходят из запросов информации, которые

	несчастного рабочего случая (из медицинского учреждения запрашивают такую справку о степени тяжести здоровья пострадавшего (Сотрудника))); - информация о нарушениях правил дорожного движения; - участие в профсоюзных организациях/прерывание профсоюзного договора сотрудника (в случае прерывания трудового договора). В отношении рабочих претендентов Персональные данные Особой категории не обрабатываются.		получены из розыскных учреждений, присяжных нотариусов, административных налоговых учреждений, судов и присяжных судебных исполнителей. **Данные связей**, которые собираются, когда Клиент посещает игровые залы и домашние страницы DLV, где DLV предоставляет услуги, или связывается с DLV по телефону, в переписке по электронной почте, оповещения и другие средства связи, например: социальные медиа, данные, которые получены, при посещении Клиентом домашней страницы DLV или связываясь с DLV с помощью других каналов, а также **визуальные записи и/или аудиозаписи** (снимок Клиента, ведя видеонаблюдение). **С услугами связанные данные**, например: полученные услуги, выплаченные выигрыши, поданные заявления, запросы и жалобы.
Цели обработки	В налоговых целях и целях платежей; для выполнения функций управления (стратегия бизнеса, цели маркетинга и рекламы); для предотвращения преступной деятельности или для раскрытия в связи с защитой собственности	В налоговых целях и целях платежей; для выполнения функций управления (стратегия бизнеса, цели маркетинга и рекламы); для предотвращения преступной деятельности или для раскрытия в связи с	**Для выполнения юридических обязательств и проверки идентичности Клиента:** для выполнения применяемых законов и нормативных актов (в том числе, но не единственной

	и собственности, находящейся в распоряжении, DLV и, чтобы защитить жизненно важные интересы Сотрудника как субъекта данных, в том числе жизнь и здоровье; для соблюдения Легитимных интересов DLV (в целях контроля и совершенствования качества предоставляемого обслуживания и/или обслуживания Клиентов; для оценки, стимулирования продуктивности; для обеспечения доказательств для требований о несоответствии услуг и/или выполнении обязательств договора, а также для обеспечения доказательств для возможного требования, которые исходят из деликта); для связанных с домашней страницей DLV целей (например, указывая контактную информацию Сотрудника); для обеспечения выполнения обязанностей DLV и выполнение применяемых нормативных правовых актов, установленных в законе, DLV как Заведующего Данных; чтобы санкционировать и контролировать доступ к дигитальным каналам и их деятельности, устранять несанкционированный доступ и его недобросовестное использование, и,	защитой собственности или использованием защиты существующего имущества, чтобы защитить жизненно важные интересы Стороны, заключающей договор, как субъекта данных, в том числе жизнь и здоровье; для обеспечения выполнения обязательств, установленных в законе, DLV как Заведующего Данных и выполнение требований применяемых нормативных правовых актов; для санкционирования и контроля доступа к дигитальным каналам и их деятельности, устранения несанкционированного доступа и их недобросовестное ииспользование, и для обеспечения безопасности информации, на основании выполнения договора, или для выполнения юридических обязательств или согласно с согласием Стороны, заключающей договор, или в легитимных интересах DLV контролировать авторизацию дигитальных услуг DLV, доступ и деятельность; для совершенствования технических систем, IT инфраструктуры, приспосабливать оборудование	обязанностью DLV является обязанность убедится в возрасте посетителей казино, игровых залов и бинго залов, не допускать участие несовершеннолетних лиц в интерактивных азартных играх или интерактивных розыгрышах и отстранять зависимых от интерактивных азартных игр игроков от дальнейшего участия в азартных играх (согласно заявлению лица, чтобы его не впускали в игровые залы), также обязанностью DLV является в установленном в нормативных актах порядке и размере заплатить за выигрыши подоходный налог с населения (ПНН); также обязанностью DLV является в установленном в нормативных актах порядке (третья часть 36 статьи Закона об азартных играх и розыгрышах) выплатить игроку выигрыш; также обязанностью DLV является в установленном в нормативных актах порядке проводить исследования Клиентов, чтобы предоставлять информацию компетентным учреждениям, чтобы устранить, раскрыть, расследовать и оповестить о возможной легализации незаконно полученных средств, финансировании

	чтобы обеспечить безопасность информации, на основании выполнения договора или, чтобы выполнить юридическую обязанность или в связи с согласием Сотрудника или легитимными интересами DLV контролировать авторизацию дигитальных услуг DLV, доступ и деятельность; чтобы совершенствовать технические системы, IT инфраструктуру, приспосабливать отображение услуги в оборудовании и развивать услуги DLV, например: тестируя и совершенствуя технические системы и IT инфраструктуру, на основании легитимных интересов DLV совершенствовать технические системы и IT инфраструктуру; для установления, осуществления и отстаивания прав требования: чтобы установить, осуществить, отстоять и цедировать права требования, или, чтобы выполнить юридическое обязательство, или осуществить права требования в легитимных интересах DLV.	отображения услуги и развития услуг DLV, например: тестируя и совершенствуя технические системы и IT инфраструктуру, на основании легитимных интересов DLV совершенствовать технические системы и IT инфраструктуру; для установления , осуществления и отстаивания прав требования: чтобы установить, осуществить, отстоять и цедировать права требования, или, чтобы выполнить юридическое обязательство, или осуществить права требования в легитимных интересах DLV.	терроризма, если Клиент подчиняется финансовым санкциям или является политически важным лицом), или, чтобы легитимные интересы DLV обеспечили обдуманное управление рисками и управление предприятием. **Для общего управления отношения Клиентов и обеспечения услуг доступа и администрирования:** для предоставления услуги, для обеспечения актуальности данных и их правильности, проверяя и дополняя данные, используя внешние и внутренние источники, на основании выполнения услуги или для выполнения юридических обязанностей. **Для защиты интересов Клиента и/или DLV:** для защиты интересов Клиента и/или DLV и обслуживания качества предоставляемых услуг DLV и, чтобы предоставлять доказательства, на основании осуществления услуги или, чтобы выполнить юридические обязательства, или согласие Клиента, или в легитимных интересах DLV устранить, ограничить и расследовать DLV недобросовестное или противозаконное использование продуктов и услуг или

			создания помех в них, для внутренних обучения или обеспечения качественных услуг. Для гарантии безопасности DLV и/или Клиента, защиты жизни и здоровья Клиента и других прав DLV и Клиента, на основании легитимных интересов DLV защищать своих Клиентов, и активы Клиентов и DLV. **Для устранения недобросовестного использования услуг и обеспечения соответствия услуг**: для санкционирования и контроля доступа к дигитальным каналам и их деятельности, устранения несанкционированного доступа и их недобросовестного использования, и для обеспечения безопасности информации, на основании выполнения договора или, для выполнения юридических обязанностей или согласно согласию Клиента или в легитимных интересах DLV контролировать авторизацию, доступ и деятельность дигитальных услуг DLV. Для совершенствования технической системы, IT инфраструктуры, приспосабливания оборудования отображения услуги и развития услуг DLV, например: тестируя и совершенствуя

			технические системы и IT инфраструктуру, на основании легитимных интересов DLV совершенствовать технические системы и IT инфраструктуру. **Для установления, осуществления и отстаивания прав требования:** для установления, осуществления, отстаивания и цедирования прав требования, или, для выполнения юридических обязательств, или в легитимных интересах DLV осуществлять права требования.
Источники	Персональные данные Сотрудника могут собираться именно с Сотрудника, из отношений трудового договора, а также из внешних источников, например, агентур занятости, предприятий по набору сотрудников, порталов рабочих заявлений, СГД, публичных регистров и публично доступной информации.	Персональные данные Стороны, заключающей договор, могут собираться именно с Стороны, заключающей договор, из отношений трудового договора, а также из внешних источников, например, публичных регистров и публично доступной информации.	Персональные данные Клиента могут собираться именно с Клиента, из внешних источников и источников использования Клиента, например, публичных регистров и публично доступной информации.
Правовая основа	- Для заключения и выполнения трудового договора; - Для выполнения юридических обязанностей DLV в соответствии с требованиями нормативных актов, которые устанавливают обязанности работодателя в связи с Сотрудниками (Трудовой закон, правила Кабинета министров 25 августа 2009 года Nr.950 “Расследование	- Для выполнения договора; - Для выполнения юридических обязанностей DLV в соответствии с требованиями нормативных актов, (законы, которые устанавливают упорядочение бухгалтерии и др.); - Для обеспечения Легитимных интересов DLV;	- Для выполнения договора (услуги); - Для выполнения юридических обязанностей DLV в соответствии с нормативными актами Азартных игр и розыгрышей (Закон об азартных играх и розыгрышах и правила Кабинета министров Nr. 715 “Порядок проверки регистрации и идентичности игроков

	несчастных случаев на работе и порядок учета", законы, которые устанавливают государственное социальное страхование, упорядочение бухгалтерии и др.); - Для обеспечения Легитимных интересов DLV; - согласно с согласием Сотрудника.	- согласно с согласием Стороны, заключающей договор.	Интерактивных азартных игр и интерактивных розыгрышей"), Закона защиты прав потребителей, Предотвращения легализации незаконно полученных средств и финансирования терроризма, закону "О бухгалтерии", закону "О подоходном налоге с населения", закону "О налогах и пошлинах", закону "О пошлинах и налогах с розыгрышей и азартных игр", Закону об архиве и другим нормативных правовым актам Латвийской Республики; - Для обеспечения Легитимных интересов DLV; - согласно с согласием Клиента.
Профилирование, персонализированные предложения и автоматизированное принятие решений	Не проводится	Не проводится	Чтобы оценить установленные персональные черты Клиента, для анализа Данных Клиента и консультирования, в целях прямого маркетинга, для автоматизированного принятия решений, например: для управления рисками, для обеспечения предоставления удаленных услуг, в т.ч. для надзора услуг, чтобы предотвратить мошенничество, и это основывается на легитимных интересах DLV, выполнении юридических обязательств, выполнении услуг (договора) или согласие Клиента.

			Для улучшения опыта использования дигитальных услуг Клиента, например, приспосабливая изображение услуги в используемом устройстве и, чтобы подготовить Клиенту подходящие предложения. Если только Клиент не ограничил прямой маркетинг в отношении себя, DLV может производить обработку Персональных данных для подготовки общих и персонализированных предложений DLV. Такой маркетинг может быть основан на услугах, используемых клиентом, и то как Клиент использует услуги и то, как Клиент действует в дигитальных каналах DLV. Профилирование, основанное на персонализированных предложениях и маркетинге, которое проводиться в связи с легитимными интересами DLV, DLV обеспечивает, что Клиенты могут сделать выбор использовать удобный инструмент для управления своими настройками приватности. DLV может также собирать статистические денные о Клиенте, в т.ч. о характерном поведении и образе жизни, на основании демографических сельскохозяйственных данных.

			Статистические данные для образования сегмента/профиля могут быть получены также из внешних источников и могут быть объединены с внутренними данными DLV.
Раскрытие личных данных	Персональные данные Сотрудника раскрываются: - серверным провайдерам; - любому аудитору, финансовому консультанту, собирателю долгов, юристконсульту, присяжному адвокату, присяжному нотариусу и/или присяжному судебному исполнителю или другому DLV утвержденному обрабатывающему Персональные Данные по выбору DLV; - компетентному специалисту для оценки Рисков рабочей среды, поскольку необходимо оценить каждое рабочее место Сотрудника; - представителям услуг об обучениях Сотрудников (в сфере пожарной безопасности и т.п.); - Инспекции по надзору розыгрышей и азартных игр, Службе государственных доходов и другим учреждениям (например, правоохранительные органы и учреждения финансовых расследований, суды, внесудебные учреждения по решению споров,	Личные данные Заключающего договор раскрываются: - серверным провайдерам и другим третьим лицам, которые связанны с DLV в предоставлении предоставляемых услуг; - любому аудитору, финансовому консультанту, собирателю долгов, юристконсульту, присяжному адвокату, присяжному нотариусу и/или присяжному судебному исполнителю или другому DLV утвержденному обрабатывающему Персональные Данные по выбору DLV; - Инспекции по надзору розыгрышей и азартных игр, Службе государственных доходов и другим учреждениям (например, правоохранительные органы и учреждения финансовых расследований, суды, внесудебные учреждения по решению споров, администраторы по процессу банкротства	Персональные Данные клиента раскрываются: - серверным провайдерам и другим третьим лицам, которые связанны с DLV в предоставлении предоставляемых услуг; - любому аудитору, финансовому консультанту, собирателю долгов, юристконсульту, присяжному адвокату, присяжному нотариусу и/или присяжному судебному исполнителю или другому DLV утвержденному обрабатывающему Персональные Данные по выбору DLV; - Инспекции по надзору розыгрышей и азартных игр, Службе государственных доходов и другим учреждениям (например, правоохранительные органы и учреждения финансовых расследований, суды, внесудебные учреждения по решению споров, администраторы по процессу банкротства и

	администраторы по процессу банкротства и неплатежеспособности); - другим лицам, которые связанны с предоставляемыми DLV услугами, в т.ч. представители услуг архивирования, почты и т.п.	и неплатежеспособности); - другим лицам, которые связанны с предоставляемыми DLV услугами, в т.ч. представители услуг архивирования, почты и т.п.	неплатежеспособности); - признанным компаниям по изучению рынка и общественной мысли (в рамках ЕС) – проведение опросов и исследований связанных с предлагаемыми услугами DLV; - другим лицам, которые связанны с предоставлением услуг DLV, в т.ч. представители услуг архивирования , почты и т.п.
Хранение персональных данных	Трудовые договора, описания труда, условия трудового порядка, инструкции, другие документы (удостоверение владения государственным языком, вид на жительство) хранятся в бумажном виде в офисе, карты, в закрытом шкафу. Трудовые договора оформленные в электронном виде хранятся в компьютере и на сервере в отдельной папке “Юридический отдел”. Журналы учета трудовых договоров за предыдущие года доступны как в электронном (в компьютере и на сервере), так и в бумажном виде (в офисе, папках, закрытом шкафу). Карточки обязательных проверок здоровья сотрудников хранятся в офисе – в папке, в закрытом шкафу. Копии трудовых договоров хранятся на	Договора, заключенные сторонами, хранятся в бумажном виде в офисе в закрытом шкафу.	Договора Клиента, заполненные анкеты (заявление Программы лояльности) в физическом виде хранятся в папках (в структурных единицах), находятся в шкафу. Информация Клиента хранится в Системе управления клиентами.

	объектах (в папках, в закрытом шкафу) – для немедленного предоставления Государственной инспекции труда во время проведения проверок (проверки в отношении незаконного трудоустройства). Распоряжения о движении Сотрудников – как в электронном (в компьютере на сервере), так и в бумажном виде (в офисе, в закрытом шкафу), составляет отдел кадров, передаются на обработку в бухгалтерию. В бухгалтерию в бумажном виде подаются расчетные счета Сотрудников для выплаты заработной платы. Бухгалтерские распоряжения хранятся в бухгалтерии (в папках, в закрытом шкафу). С персональными данными Сотрудников (претендентов на работу) может ознакомиться управление DLV или их уполномоченный Сотрудник (в т.ч. представитель аутсорсинга бухгалтерского учета и т.п.) в необходимых целях. Имена и фамилии Сотрудников могут быть раскрыты другим Сотрудникам и Клиентам DLV, но остальные персональные данные DLV может раскрывать только, если получено согласие соответствующего Сотрудника или претендента.		
Географическая	Персональные данные обрабатываются в зоне Европейского		

область обработки	Союза/Европейской Экономической зоне (ЕС/ЕЭЗ).
Период хранения	Период хранения обработанных Персональных данных может быть обоснован договором, легитимными интересами DLV или применяемыми нормативными актами (например: законами о бухгалтерии, архивах, легализации преступно полученных средств, ограничениях, гражданских правах и т.п.). DLV хранит Персональные данные в соответствии целям и намерениям Персональных данных, как и в соответствии с требованиями Регул и нормативных актов, в т.ч., для соблюдения Легитимных интересов DLV (для обеспечения доказательств на требования о несоответствии услуг и/или невыполнении обязательств договора, а также для обеспечения доказательств на возможные требования, исходящие из деликта), DLV хранит Персональные данные десять лет со дня выполнения услуги или договора. После окончания периода хранения DLV стирает файлы, которые содержат Персональные данные.

3. ИНФОРМАЦИОННЫЕ РЕСУРСЫ, ТЕХНИЧЕСКИЕ РЕСУРСЫ И ЛИЦА ОТВЕТСТВЕННЫЕ ЗА ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИХ ПРАВА И ОБЯЗАННОСТИ

Управление информационными ресурсами и техническими ресурсами:

За защиту, безопасность информации и процесс оптимизации Персональных данных в целом отвечает правление DLV, которое само или с помощью назначенного лица контролирует надежность Системы обработки Персональных данных.

Правление назначает специалиста/-ов обработки Персональных данных и/или поддерживающего/-их Информационные ресурсы и технические ресурсы, или же сам берет на себя обязанность осуществлять соответствующие задания.

Правление или специалист обработки Персональных данных или поддерживающий Информационных ресурсов и технических ресурсов назначает лица, которые находятся в подчинении специалиста обработки Персональных данных или поддерживающего Информационных ресурсов и технических ресурсов, и который отвечает за безопасность Информационных систем.

Правление в рамках бюджета обеспечивает поддерживающих Информационные ресурсы и технические ресурсы средствами, которые необходимы для мероприятий безопасности Информационных систем.

Поддерживающий информационные ресурсы:

- совместно с поддерживающим технические ресурсы и (если возможно) с предоставляющим информацию производит анализ рисков связанных с Информационными ресурсами;
- обеспечивает мероприятия Логической защиты;
- обеспечивает Аудиторский учет Информационных систем, а также их сохранение и Доступность для проверки, в связи с условиями безопасности Информационных систем;
- устанавливает порядок, по которому Пользователям Информационных систем предоставляются права доступа к Информационным ресурсам и действий с ними, и организовывает контроль использования этих ресурсов;
- обеспечивает изготовление и хранение резервных копий Информационных ресурсов, а также возобновление Информационных ресурсов, если функционирование Информационных систем было прервано или невозможно из-за повреждений технических ресурсов или других причин.

Поддерживающий технические ресурсы:

- Обеспечивает мероприятия физической защиты;
- участвует в анализе рисков, устанавливает с техническими ресурсами связанные Угрозы Информационных систем и оценивает вероятность реализации этих Угроз;
- обеспечивает возобновление технических ресурсов, если таковые повреждены;
- обеспечивает возобновление технических ресурсов;

Поддерживающий Информационные ресурсы и технические ресурсы устанавливает обязанности Сотрудников в сфере безопасности Информационных систем и обеспечивает обучение Сотрудников и проверку знаний в сфере защиты Информационных ресурсов и технических ресурсов.

4. Классификация защиты Персональных данных в соответствии со степенью ценности и конфиденциальности

Цель классификации информации идентифицировать всю важность информации в распоряжении DLV и обеспечить защиту каждой информационной группы в соответствии с ее уровнем классификации.

Поддерживающие Информационные ресурсы производят Классификацию Информационных ресурсов по степени Ценности, Конфиденциальности и Доступности. Классификацию информации производят в связи с требованием поддерживающего Информационных ресурсов, если он такие установил.

Классификация информации относится ко всей информации независимо от информационного носителя (бумага, микрофильмы, видеокассеты, магнитные ленты, кассеты, компакт-диски, жёсткие диски компьютеров, дискеты или другие носители информации).

Информацию классифицируют по Степени конфиденциальности, при оценивании Угроз ее несанкционированной утечки, следующим образом:

- Общедоступная информация;
- Информация ограниченного доступа.

Информацию классифицируют по Уровню ценности, при оценивании Угроз Целостности информации, следующим образом:

- Высоко ценная информация;
- Средне ценная информация.

Информацию по Уровню доступности, при оценивании Угроз ее Доступности. Классифицируя, устанавливают также допустимое время, при котором Информационные ресурсы могут быть не доступны. Классифицируют следующим образом:

- информация доступна постоянно;
- информация доступна только в рабочее время.

Информация, которая не классифицирована в соответствии с Принципами конфиденциальности, автоматически считается Информацией ограниченного доступа.

Если на информационном носителе хранится информация, классифицированная разными уровнями, как общим уровнем классификации информационного носителя указывают высший уровень информации имеющейся на этом носителе.

У всех информационных носителей Ограниченного доступа должен быть соответствующий знак о классификации информации.

5. Технические ресурсы, которыми обеспечивается обработка персональных данных

Обработка Персональных данных обеспечивается следующими техническими ресурсами:

- стационарные рабочие станции, портативные или персональные компьютеры;
- сервера;
- системы видеонаблюдения;
- другое оборудование и программное обеспечение по необходимости.

6. Процедура организации обработки Персональных данных

Обработка Персональных данных происходит в помещениях DLV, в помещениях, где расположены сервера DLV, и в любом месте, из которого обеспечивается удаленный доступ к Информационным ресурсам. Персональные данные обрабатываются постоянно или по необходимости, в соответствии с целями их обработки.

DLV обрабатывает Персональные данные в соответствии с установленным в нормативных актах и только тогда, если есть хотя бы одно из следующих условий:

- получено согласие субъекта Персональных данных;
- обработка Персональных данных исходит из договорных обязательств субъекта данных или, при условии запроса субъекта данных, обработка Персональных данных необходима, чтобы заключить соответствующий договор;
- обработка Персональных данных необходима DLV для осуществления обязательств установленных в законе;
- обработка Персональных данных необходима, чтобы защитить жизненно важные интересы субъекта данных, в том числе жизнь и здоровье;
- обработка Персональных данных необходима, чтобы обеспечить соблюдение интересов DLV или реализовать задачи государственной власти, для выполнения которых Персональные данные переданы DLV;
- обработка Персональных данных необходима, чтобы, соблюдая основные права и свободу субъекта данных, реализовать законные интересы DLV или Третьего лица, которому раскрыты Персональные данные.

7. ВИДЕОНАБЛЮДЕНИЕ

DLV производит видеонаблюдение для предотвращения уголовных преступлений или для раскрытия связанного с защитой имущества и жизненно важных интересов лиц, в том числе защиту жизни и здоровья, а также для выполнения обязанностей установленных в нормативных актах розыгрышей и азартных игр.

Видеонаблюдение проводится внутри и снаружи игровых залов DLV непрерывно.

Видео записываются на компьютерные носители данных, которые находятся в каждом игровом зале.

Доступ к видеозаписям есть только централизовано из офиса DLV, удаленно подключаясь к каждому компьютеру игрового зала.

Видеозаписи хранятся не менее чем 7 дней с момента произведения записи и настолько долго, насколько позволяет объем носителя данных каждой конкретной системы видеонаблюдения. При окончании объема носителя данных системы видеонаблюдения, следующие данные видеонаблюдения записываются вместо предыдущих на том же самом носителе данных.

В рамках дисциплинарного дела, административного или криминального дела DLV сохраняет соответствующую видеозапись настолько долго, пока не закончится соответствующее дело.

Не разрешено видеонаблюдение в туалете и в помещениях/зонах отдыха Сотрудников.

У каждого игрового зала в видимом всем месте необходимо размещать письменное оповещение/наклейку, которая информирует, что ведется видеонаблюдение, указав в ней цель видеонаблюдения, фирму DLV и контактную информацию.

8. ПРАВА СУБЪЕКТА ДАННЫХ (СОТРУДНИКА, СТОРОНЫ, ЗАКЛЮЧАЮЩЕЙ ДОГОВОР, КЛИЕНТА)

До обработки Персональных данных, DLV предоставляет информацию об обработке Персональных данных:

- Сотруднику, подписывая соответствующее приложение к трудовому договору об обработке Персональных данных;

- Стороне, заключающей договор, включив в договор условия об обработке Персональных данных;

- Клиенту, ознакомив Клиента с Заявлением о конфиденциальности и Политикой конфиденциальности.

У Субъекта данных есть следующие права:

1.1. запросить исправление своих Персональных данных, если они не соответствующие, не полные или не правильные;

1.2. возразить обработке своих Персональных данных, если использование Персональных данных основывается на легитимных интересах, в том числе намерениям профилирования прямого маркетинга (например, для получения предложений маркетинга или участие в опросах);

1.3. запросить удаление своих Персональных данных, например, если Персональные данные обрабатываются на основании согласия, если субъект данных отозвал свое согласие. Такие права не имеют силу, если Персональные данные, удаление которых запрошено, обрабатываются, также на основании других правовых основ, например, договора или следующих из соответствующих нормативных актов обязательств (например, Закон легализации преступно полученных средств и предотвращения финансирования терроризма) или в других случаях, установленных в Регуле;

1.4. ограничивать обработку своих Персональных данных в связи с применяемыми нормативными актами, например, во время, когда DLV оценивает, есть ли у субъекта данных права на удаление своих данных;

1.5. получать информацию, обрабатывает ли DLV его Персональные данные и, если обрабатывает, тогда получить к ним доступ и получить информацию, как они обрабатываются и кому передаются;

1.6. получать свои Персональные данные, которые он предоставил и которые обрабатываются на основании выполнения соглашения или договора в письменном виде или в каком-либо из чаще используемых электронных форматов и, если возможно, передать такие данные другим представителям услуг (переносимость данных).;

1.7. отозвать свое согласие для обработки своих Персональных данных, если Персональные данные предоставляются DLV на основании согласия субъекта данных;

1.8. в полном объеме не подлежат автоматизированному принятию решений, в том числе профилированию, если у такого принятия решений есть правовые последствия или, что подобным образом заметно влияет на субъект данных. Такие права не имеют силу, если принятие решения необходимо, чтобы заключить или выполнить договор с субъектом данных, если принятие решения разрешено согласно применяемым нормативным актам или, если субъект данных дал свое явное согласие;

1.9. подать жалобу об использовании Персональных данных в Государственную инспекцию данных (www.dvi.gov.lv), если субъект данных считает, что обработка его Персональных данных нарушает его права и интересы в связи с применяемыми нормативными актами.

Права, которые лицо <u>НЕ МОЖЕТ</u> использовать (“X” отмечены права, которые физическое лицо (субъект данных) НЕ МОЖЕТ использовать. Ячейки БЕЗ “X” это права, которые физическое лицо (субъект данных) МОЖЕТ использовать):

Основание для обработки Персональных данных:	**Права на удаление данных**	**Права на перенос данных**	**Права возражения**
Согласие			X но права отозвать согласие
Договор			X

Законная обязанность	X	X	X
Основные интересы		X	X
По заданию государственных учреждений	X	X	
Легитимные интересы		X	

9. Порядок, в котором DLV обеспечивает Субъекту данных гарантированные права и мероприятия безопасности Персональных данных

Обеспечение прав Субъекта данных.

Запросы Субъекта данных:

Если от субъекта данных получен запрос выдать или раскрыть Персональные данные субъекта данных, находящиеся в распоряжении DLV, такие запросы рассматривает член правления DLV или его назначенное лицо, и соответствующие Персональные данные можно выдать и раскрыть только член правления DLV или его назначенное лицо, если такое раскрытие или передача обоснована.

Чтобы защитить Персональные данные от незаконного раскрытия, DLV, получив требование субъекта данных о предоставлении данных или о осуществлении других прав субъекта данных, удостоверяется в личности субъекта данных. Для этой цели DLV вправе запросить у субъекта данных указать Личные данные, сравнив, совпадают ли указанные данные субъектом данных с соответствующими Персональными данными, находящимися в распоряжении DLV. Проводя эту проверку, DLV также может выслать контрольное оповещение на указанные субъектом данных телефон или электронную почту (сообщения или в виде электронной почты), с просьбой произвести авторизацию. Если процедура проверки не удачна (напр., указанные субъектом данных данные не совпадают с Персональными данными, имеющимися в распоряжении DLV, или субъект данных не произвел авторизацию по отосланному сообщению или оповещению электронной почты), DLV будет вынуждено констатировать, что субъект данных не является субъектом запрошенных Персональных данных, и будет вынуждено отказать соответствующему поданному требованию.

Получив требование субъекта данных об осуществлении любых прав субъекта данных и успешно произведя ранее упомянутую процедуру проверки, DLV обязуется без замедлений, однако в любом случае не позднее чем в течение одного месяца с получения требования субъекта данных и окончания процедуры проверки, предоставить субъекту данных информацию о действиях, которые произвело DLV в соответствии с требованием, поданным субъектом данных. Учитывая сложность требования и количество, DLV в праве период в один месяц продлить еще на два месяца, об этом информируя субъект данных до конца первого месяца и указав причину такого продления. Если требование субъекта данных подано с помощью электронных средств, DLV дает ответ также с помощью электронных средств, за исключением случаев, когда это не будет возможно (напр., из-за большого объема данных) или тогда, если субъект данных попросил ответить в другом виде.

DLV вправе отказаться удовлетворить требование субъекта данных мотивированным ответом, если будут констатированы обстоятельства, установленные в правовых актах, или невозможно убедиться в личности субъекта данных, об этом письменно информируя субъекта данных. Если требования субъекта данных очевидно не обоснованы или чрезмерны, в частности из-за их регулярного повторения, DLV как Хранитель Данных может либо: a) запросить разумную плату, учитывая административные расходы, которые связаны с обеспечением информации или связей или проведением запрошенных действий; либо b) отказаться выполнять требование.

Требования третьих лиц:

Если от государственных или самоуправленческих учреждений или Третьих лиц, которые не являются Сотрудниками, Сторонами, заключающими договор, или Клиентами,

получен запрос предоставить или раскрыть Персональные данные, имеющиеся в распоряжении DLV, такие запросы рассматривает член правления DLV или его назначенное лицо, и соответствующие персональные данные может подать и раскрыть только член правления DLV или его назначенное лицо, если такое раскрытие или передача является обоснованной.

В любом случае, если Сотрудник DLV не знает, как действовать – можно или нельзя раскрывать какую-либо информацию – Сотруднику необходимо консультироваться с членом правления DLV или с его назначенным лицом, и Сотрудник может действовать в соответствующем случае только так, как указал член правления DLV или его назначенное лицо.

DLV, передавая Персональные данные, обеспечивает сохранение информации о:

- Времени передачи Персональных данных;
- Лице, которое передало Персональные данные;
- Лице, которое получило Персональные данные;
- Персональных данных, которые были переданы.

Мероприятия безопасности Персональных данных.

Чтобы защитить Персональные данные от несанкционированного доступа, случайной пропажи, уничтожения или повреждения, DLV использует мероприятия физической безопасности: закрытые картотеки, которые содержат Персональные данные; закрытые офисы / помещения с Персональными данными.

DLV использует средства безопасности, чтобы обеспечить защиту оборудования и / или файлов от неавторизированного доступа, случайной пропажи, уничтожения или повреждения: авторизация, архивирование, шифрование, доступ Пользователей, регламентирование действий, SSL сертификаты, брандмауэр.

DLV использует другие мероприятия безопасности, чтобы защитить Персональные данные от несанкционированного доступа, случайной пропажи, уничтожения или повреждения: права ограниченного доступа к Персональным данным (основываясь на необходимости знать); надежное уничтожение отходов документации конфиденциальной информации (как в бумажном, так и в электронном виде), обучения работников.

Обрабатывая Персональные данные в Информационной системе, обеспечивается только доступ уполномоченных лиц к Персональным данным, техническим средствам и документам.

У администратора Информационных систем в сотрудничестве с поддерживающим Технологических ресурсов есть права проводить аудиты действий Пользователей. Такие аудиты могут содержать проведение аудита действий Пользователя (в том числе посещаемых интернет ресурсов), анализ и запрос дополнительной информации о проведенных действиях.

В рамках надзора использования Информационных систем:

- Поддерживающий Технологических ресурсов обеспечивает, что записи Аудита формируются о Информационных системах, которые содержат классифицированные Информационные ресурсы, и действиях в компьютерной сети, в которой есть доступ к Информационным системам, которые содержат классифицированные Информационные ресурсы. В записи Аудита включены все даты и время удачных и не удачных случаев подключения, а также код Пользователя (в т.ч. поддерживающего Технологические ресурсы) или другие средства аутентификации;
- Поддерживающий Технологических ресурсов обеспечивает целостность записей Аудита и регулярно составляет записи резервных копий данных Аудита в соответствии с правилами этих условий;

- Поддерживающий Технологических ресурсов регулярно контролирует всю деятельность Информационных систем, но особое внимание обращает на контроль деятельности Информационных систем, которая содержит классифицированные Информационные ресурсы. Для этой цели поддерживающий Технологических ресурсов по выбору использует специальные программы контроля или компьютерные системы, устанавливающие вторжение.

Поддерживающий технологических ресурсов контролирует хотя бы следующие случаи:

- повторное неудачное подключение к Информационной системе;

- попытки подключиться к Информационным ресурсам, к которым Пользователь не уполномочен подключаться;

- использование Информационных систем в необычное время, например, вне рабочего времени;

- повторные попытки использования кодов Пользователя, которые уже были отклонены;

- присвоение и использование привилегированных кодов Пользователя;

- несанкционированное изменение конфигураций программного обеспечения и недопустимая установка программного обеспечения.

Контроль вирусов ресурсов Информационных систем:

- поддерживающий Технологических ресурсов устанавливает порядок и проводит мероприятия для предотвращения действий вирусов в компьютере Информационных систем;
- для предотвращения действий вирусов использует специально предусмотренное для этой цели программное обеспечение. Файлы, определенные как вирусные, незамедлительно возобновляет, как только разработчик предлагает файлы для возобновления;
- поддерживающий Технологических ресурсов регулярно производит контроль антивирусных программ, чтобы убедиться в их работоспособности и обнаружить новые файлы, определенные как вирусные.

Защита персональных и портативных компьютеров:

- Владелец информации устанавливает, какую информацию можно хранить на персональном и портативном компьютере (далее в тексте – **персональные компьютеры**). В портативных компьютерах, которые используются вне рабочих помещений DLV, хранят только ту информацию, которая необходима в установленное время установленному Пользователю компьютера;

- В персональном компьютере устанавливают и используют только то программное обеспечение и с такой конфигурацией, которую определил поддерживающий Технологическую информацию. Функциональность персонального компьютера ограничивают до уровня функций, необходимых для рабочих потребностей;

- Персональный компьютер, оставляя без присмотра Пользователя, отключают, используя экранную заставку с паролем, специальной функцией отключения или другим методом, который позволяет продолжать работу с персональным компьютером только тогда, если была произведена аутентификация Пользователя;

- поддерживающий Технологических ресурсов устанавливает порядок, в котором Сотрудники для рабочих потребностей используют им принадлежащие компьютеры и в котором используют компьютеры DLV вне рабочих помещений. Такой порядок нельзя уменьшить на уровне защиты установленных Информационных ресурсов.

Защита компьютерной сети:

- поддерживающий Технологических ресурсов разрабатывает и содержит схему компьютерной сети, в которой показана в компьютерной сети соединенная аппаратура и обеспечиваемые услуги;

- поток данных между локальной компьютерной сетью и внешней компьютерной сетью разрешает только те услуги, которые необходимы для выполнения функция DLV, для этой цели используют системы брандмауэра;

- поддерживающий Технологических ресурсов регулярно проверяет существование всего внешнего соединения и убеждается, что есть только те соединения, которые соответствуют рабочим требованиям DLV и что работают резервные соединения;

- подключение к Информационным системам из логически отдаленного места защищают, используя средства криптографии вместе с паролем Пользователя так, чтобы уверенно установить Аутентичность Пользователя.

DLV по необходимости проводит дополнительные мероприятия Логической защиты, в зависимости от уровня классификации ресурсов Информационной системы.

DLV проводит равноценные мероприятия Логической защиты для классифицированных Информационных ресурсов независимо от вида хранения данных (в т.ч. дискеты, бумажные документы, аудио кассеты и т.п.).

DLV в сотрудничестве с внешними представителями услуг информационных технологий:

- устанавливают требования ответственности вовлеченных лиц, присвоение временных счетов Пользователей, управление изменениями и другие требования безопасности Информационных систем;
- согласовывая с владельцами информации, присваивает права доступа к ресурсам Информационных систем внешним представителям информационных технологий только в объеме, необходимом для выполнения обязательств;
- устанавливают ограничения распространения информации.

Если DLV решает обслуживание Информационных систем доверить внешнему представителю услуг, оно должно обеспечить уровень безопасности Информационных систем, который не ниже чем установленный в этих условиях. DLV должен ознакомить представителя внешних услуг с установленными в этих условиях требованиями безопасности Информационных систем. Порядок обработки Персональных данных и уровни доступа устанавливает распределение ролей Пользователей Информационных систем.

10. Строение пароля, порядок его использования и доступ

Каждому Пользователю информационных ресурсов присваивается имя(на) пользователя(ей) (идентификатор(ы)) Информационной системы и пароль, а также установленные права доступа. Пользователь Информационной системы несет ответственность за использование, сохранение и не распространение присвоенного имя доступа (идентификатора) и пароля.

Права доступа подтверждает соответствующий владелец Информационных ресурсов. На основании запроса владельца Информационных ресурсов, администратор Информационных систем дает доступ Пользователю во все указанные в подтверждении Информационные системы.

Владелец Информационных ресурсов должен информировать администратора Информационных систем о тех Сотрудниках, которые прекращают рабочие отношения с DLV. Владелец Технологических ресурсов после получения этой информации незамедлительно аннулирует все права доступа соответствующего Сотрудника DLV к ресурсам Информационных систем.

Пользователь Информационной системы несет ответственность за действия, которые производятся, используя его имя пользователя (идентификатор). Аутентичность Пользователя Информационной системы устанавливают, чтобы убедиться, что пользователь имя пользователя (идентификатора) является санкционированным его владельцем. Для установления Аутентичности используются пароли. После ввода имя пользователя (идентификатора) и пароля, Пользователь Информационной системы может использовать ресурсы Информационной системы в соответствии с установленными правами доступа.

Пароль состоит из комбинации букв, цифр и знаков и его длинна не должна быть короче восьми символов. Нельзя как пароль использовать идентифицирующие лицо данные (например, Персональные данные, номер автомобиля, имена и фамилии родственников, имена, которые связанны с рабочим местом или которые часто там используются).

При вводе пароля Пользователем Информационных систем, он не должен быть видимым для прочтения на экране компьютера.

Пользователь Информационных систем должен менять пароль хотя бы раз в три месяца. Администратор Информационных систем должен обеспечить:

автоматический запрос смены пароля для Пользователя, первый раз регистрируясь в сети;

автоматический запрос смены пароля через каждые три месяца;

блокирование систем на время до 1 часа, если Пользователь пять раз подряд ввел не правильный пароль или имя пользователя.

Пользователь Информационных систем пароль должен запомнить. В письменном виде пароли разрешено хранить только в закрытом сейфе.

Если появились подозрения, что пароль узнало другое лицо, Пользователь Информационных систем незамедлительно оповещает об Инциденте владельца Информационных ресурсов, владельца технических ресурсов и администратора Информационных систем.

Запрещено пробовать узнать пароли других Пользователей, исключая случаи, когда это необходимо администратору Информационных систем для выполнения его третьих обязанностей. После завершения упомянутых работ, Пользователь Информационных систем меняет пароль.

На экране должна быть установлена экранная заставка с паролем активизации. Она должна активизироваться автоматически, если в течение пяти минут Пользователь не производил никаких действий.

11. Мероприятия, которые проводятся для защиты технических ресурсов от чрезвычайных случаев и средств, которые обеспечивают защиту технических ресурсов от намеренного повреждения и не допускают получение

DLV проводят мероприятия физической защиты Информационных систем, которые защищают их от не желаемых факторов окружающие среды (пожар, наводнения, колебания температуры и др.), технических (несоответствующая подача электроэнергии и др.) и человеческих факторов (намеренные или не намеренные повреждения, кража и др.).

Физическая защита серверов:

- DLV обеспечивает, чтобы все Информационные системы эксплуатировались с ограниченным доступом, в закрытых помещениях, Физическая защита которых обеспечивает только доступ уполномоченных лиц, или же обеспечивает физическую защиту серверов, чтобы их нельзя было выключить, переместить, повредить и не санкционированно поменять их конфигурацию. Серверные помещения размещают в помещениях здания, в которых менее вероятно осуществление Угроз;

- Посторонние лица, в т.ч. представители внешних услуг, в серверных помещениях могут находится только в сопровождении уполномоченных лиц;

- В зависимости от возможного объема потерь DLV обеспечивает достаточную защиту серверов и серверных помещений от физических Угроз (в т.ч. от несоответствующих климатических условий, пожаров, наводнений, прерывании подачи электроэнергии, намеренных повреждений), в случае необходимости оборудовав охранной и пожарной сигнализацией, автоматической системой пожаротушения, устанавливая оборудования альтернативной подачи тока и оборудование охлаждения воздуха.

Для инфраструктуры сетей (в т.ч. для аппаратуры сетей коммуникаций, кабельной сети) DLV обеспечивает достаточную физическую защиту, ее размещая так, чтобы к ней не могли не санкционированно подключиться, свободно подключиться или повредить несвязанные с DLV лица, а также, чтобы к ней не могли не санкционированно подключится, свободно подключиться и повредить, или случайно из-за неосторожности повредить Сотрудники или посетители DLV.

Физическая защита рабочих станций:

- Рабочее место владельца Технологических помещений отделяют помещения ограниченного доступа;

- Рабочие станции используют в соответствии с установленными требованиями производителя и используют оборудования непрерывной подачи электроэнергии, если оказывается, что риск нарушений подачи электроэнергии недопустимо высок.

Физическая защита портативного оборудования:

портативные компьютеры используют в соответствии с установленными производителем требованиями;

DLV производит регистрацию оборота портативного оборудования, чтобы установить, какое лицо использует соответствующее оборудование.

Физическая защита носителей данных:

- DLV проводит необходимые мероприятия безопасности для физической защиты всех носителей данных независимо от их вида (в т.ч. демонтированные дисковые оборудования, бумажные распечатки, распечатки факса, дискеты, оптические диски и т.п.);
- Носители данных, которые содержат ресурсы Информационных систем использовать и перемещать без особого временного ограничения могут только уполномоченные Сотрудники DLV, у которых есть доступ к ресурсам Информационных систем. Ресурсы Информационных систем, которые нет необходимости использовать или перемещать, хранятся в помещениях DLV, для них предусмотренных местах. Если необходимо уничтожить носители данных, их уничтожение контролирует и обеспечивает владелец Технологических ресурсов;
- В рамках защиты носителей данных DLV проводит физическую защиту входного и выходного оборудования данных, устраняя не санкционированное использование – оборудование принтеров не размещают в публично доступных помещениях, не допускают наружную деятельность носителей данных, если она не является необходимой для выполнения обязанностей Сотрудников;
- Носители данных с классифицированными Информационными ресурсами запрещено оставлять в ненадежных (например, в публично доступных) местах;
- Если носитель данных, который содержит классифицированные Информационные ресурсы, предусматривается уничтожить, тогда это выполняется в таком виде, чтобы не было возможно произвести возобновление в нем существующих данных.

В случае необходимости DLV проводит дополнительные мероприятия физической защиты в зависимости от уровня классификации ресурсов Информационной системы. Мероприятия физической защиты Информационных систем проводятся систематически, не допуская ситуацию, когда ресурсы Информационных систем находились вне помещений ограниченного доступа без контроля уполномоченных Сотрудников DLV. DLV регулярно проводит проверку мероприятий физической защиты.

Резервные копии данных изготавливаются в соответствии с процедурой, установленной членом правления DLV.

В случае любых Инцидентов, напр., кражи носителей данных, в случае пропажи, соответствующий Сотрудник незамедлительно информирует владельца Технологических и Информационных ресурсов, которые проводят все необходимые мероприятия для защиты данных.

12. Порядок хранения и уничтожения информационных носителей

В случае закрытия Информационной системы или до уничтожения информационного носителя ответственное лицо удаляет содержание информации, содержание баз данных, а также все прочие связанные файлы.

Если необходимо удалить данные из Информационной системы, DLV обеспечивает полное удаление данных из Информационной системы, чтобы их не было возможно

восстановить.

13. Права, обязанности, ограничения и ответственность пользователей Персональных данных

Пользователи Информационных систем могут использовать присвоенные ресурсы Информационных систем только для выполнения рабочих обязанностей и могут обрабатывать Персональные данные только в соответствии с целями их обработки и для выполнения рабочих обязанностей.

Пользователь Информационных систем несет ответственность за действия, которые проводятся, используя его имя пользователя (идентификатор). Аутентичность Пользователя Информационных систем устанавливается, чтобы убедиться, что пользователь имени пользователя (идентификатора) является его санкционированным владельцем. Для установления Аутентичности используются пароли. После ввода имя пользователя (идентификатора) и пароля Пользователь Информационной системы может использовать ресурсы Информационной системы в соответствии с установленными правами доступа.

Пользователю Информационных систем пароль необходимо запомнить. В письменном виде пароль разрешено хранить только в закрытом сейфе.

Запрещено пробовать узнать пароли других Пользователей, за исключением случаев, когда это необходимо администратору Информационных систем для выполнения его прямых обязанностей. После завершения упомянутых работ Пользователь Информационных систем пароль меняет.

При окончании трудовых отношений Пользователя Информационных систем с DLV, все права доступа к ресурсам Информационных систем администратор Информационных систем аннулирует.

Используя ресурсы Информационных систем, обязанностью Пользователя Информационных систем является незамедлительное оповещение администратора Информационных систем в следующих случаях:

- если возникли подозрения, что пароль Пользователя узнали другие лица;
- получив сообщения электронной почты непонятного происхождения (например, незнакомые корреспонденты, особенно указанные темы писем);
- если возникли подозрения, что компьютер инфицирован вирусом, также выключить компьютер;
- если возникли подозрения в повреждении компьютерной техники, также незамедлительно выключить поврежденную технику;
- заметив отклонения деятельность компьютера или Информационной системы;
- если необходимо поменять расположение компьютерной техники;
- прочитать оповещения, отправленные администратором Информационной системы, и своевременно выполнить указанные действия;
- ознакомиться с инструкциями и рекомендациями, включёнными в каталог общего использования;
- регулярно удалять для работы не нужные письма электронной почты;
- не прерывать процесс обновления противовирусной программы;
- следить, чтобы на компьютере обязательно была активизирована экранная заставка с защитой пароля. Экранная заставка должна автоматически активизироваться, если в течение пяти минут Пользователь не производил никаких действий.

Пользователю Информационных систем запрещено:

- Использовать ресурсы Информационных систем, чтобы распространять или хранить с работой не связанную информацию (например, объявление коммерческого или личного

характера, призывы, рекламы, деструктивные программы, игры);

- проводить деятельность, которая ненужным образом нагружает ресурсы Информационных систем, учитывая другие нужды Пользователей Информационных систем (например, чрезмерно использовать интернет, печатать без необходимости больше количество копий документов, оставлять открытыми файлы имеющихся на сервере файлов, которые не являются необходимыми для работы);

- осуществлять загрузку доступных в интернете программ;

- самостоятельно инсталлировать программное обеспечение компьютера;

- не санкционированно передавать копии программного обеспечения рабочих данных третьему лицу;

- без согласования с членом правления DLV создавать для себя или предоставлять другим Пользователям удаленный доступ к своей рабочей станции, портативному компьютеру или ресурсам сервера;

- самостоятельно менять конфигурацию компьютера, перемещать стационарную технику офиса и устранять какие-либо повреждения компьютерной техники;

- к системе постоянного энергообеспечения компьютера подключать какие-либо электронные приборы, за исключение компьютеров, мониторов и приспособлений печати.

Пользователь Информационных систем несет ответственность за потери, которые возникли из-за несоблюдения установленных в этих условиях требований.

Администратор Информационных систем:

- создает, модифицирует и ликвидирует идентификаторы (счета) Пользователя Информационных систем и присваивает соответствующе права;

- если необходимо, ограничивает объем файла диска сервера или какого-либо его каталога, об этом информируя всех Пользователей этого диска или каталога по электронной почте;

- контролирует, чтобы Пользователи ресурсов Информационных систем соблюдали условия смены пароля, установленные в этих правилах.

Администратор Информационных систем в праве:

- По выходным или вне официального рабочего времени отключать ресурсы Информационных систем, чтобы проводить работы по поддержке, за 3 рабочих дня об этом предупредив Пользователей Информационных систем;

- Отключать ресурсы Информационных систем и приостанавливать работу системы также в рабочее время, если произошла авария (если возможно, заранее об этом предупреждая Пользователей по телефону и электронной почте).

14. ПРОЦЕДУРА НАРУШЕНИЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Согласно статьям 33 и 34 Регулы, DLV как Владелец Данных констатирует, регистрирует, расследует, оценивает и принимает решение об оповещении о произошедшем нарушении защиты Персональных данных Государственной инспекции данных и/или субъекту Персональных данных.

1. Общие правила.

1.1. О любом Нарушении защиты Персональных данных или ее признаках Сотрудник, который это констатировал, незамедлительно сообщает как владельцу Информационных ресурсов, так и технических ресурсов.
1.2. В случае Нарушения Сотрудник, в рамках своих возможностей и полномочий, обязан обеспечить безопасность Технических и Информационных ресурсов до момента появления соответствующего владельца ресурсов.

2. Регистрация, расследование и оценка нарушений

2.1. Получив от Сотрудника, Обрабатывающего Данные, Партнера Сотрудничества или любого Третьего лица информацию о возможном Нарушении, ответственное лицо (специалист защиты данных) (далее – **Ответственное лицо**) незамедлительно проводит проверку того, является ли информация правдивой. В случае подозрений о Нарушении, оно незамедлительно фиксируется в регистре Нарушений (приложение Nr.1).
2.2. За ведение регистра Нарушений отвечает Ответственное лицо.
2.3. После регистрации Нарушений Ответственное лицо начинает расследование и устанавливает вид Нарушения, причины возникновения и принимает решение о влиянии риска на права субъекта данных.
2.4. Существуют следующие виды Нарушений:
  2.4.1. Нарушение Доступности – (A)
  2.4.2. Нарушение Целостности – (B)
  2.4.3. Нарушение Конфиденциальности – (C)
2.5. В случае нескольких видов Нарушения, в регистре Нарушений указывают все соответствующие обозначения Нарушений.
2.6. По Влиянию на права и свободу субъекта данных существуют следующие Влияния Нарушения:
  2.6.1. Нарушение не создает риск или мало вероятно, что риск будет создан – (1)
  2.6.2. Нарушение может создать риск или создало риск – (2)
  2.6.3. Нарушение создает высокий риск – (3)
2.7. Если констатированы несколько видов Нарушений с несколькими Ценностями риска, действие в отношении оповещения о Нарушении проводится, учитывая высшую Ценность Влияния риска.
2.8. После анализа Влияния Нарушения принимается решение об оповещении о нем согласно с этими правилами.
2.9. Дополнительно с анализом Влияния Нарушения проводит устранение созданных Нарушением последствий в соответствии с Влиянием, которое создало Нарушение, в случае необходимости прервав работу Информационных систем.

3. Оповещение Государственной инспекции данных

3.1. Если маловероятно, что Нарушение может создать риск прав и свободы субъекта данных (Информация о низком риске), оповещение Государственной инспекции данных не ведут.
3.2. Если Нарушение может создать риск или высокий риск прав и свободы субъекта данных, Заведующий Данными о нарушении защиты данных сообщает Государственной инспекции данных незамедлительно, но не позднее чем в течение 72 часов с момента, когда Нарушение стало известным.
3.3. В оповещении Государственной инспекции данных Заведующих Данных указывает следующее:

3.3.1. описывает характер Нарушения, в том числе, категории и примерное количество субъекта данных;
3.3.2. контактную информацию специалиста защиты данных, или другую контактную информацию, где возможно получить дополнительную информацию;
3.3.3. возможные последствия Нарушения;
3.3.4. мероприятия, которые Заведующий Данных провел или планирует провести, чтобы устранить Нарушение и его неблагоприятные последствия.

4. Информирование субъектов данных о Нарушении защиты данных

4.1. Если Заведующий Данных констатирует, что Нарушение может создать высокий риск правам и свободе субъекта данных, Заведующий Данных незамедлительно об этом сообщает субъекту данных.
4.2. В оповещении субъекту данных указывает в пункте 3.3 указанную информацию.
4.3. Оповещение субъекту данных не производится, если:
4.3.1. Заведующий Данных осуществил соответствующие технические и организаторские мероприятия защиты, и упомянутые мероприятия применяются к Персональным данным, которые затронуло Нарушение, особенно такие мероприятия, которые Персональные данные делают непонятными лицам, у которых нет полномочия доступа к данным;
4.3.2. Заведующий Данных после Нарушения произвел технические и организаторские действия, чтобы для субъекта данных не был создан высокий риск его прав и свободе;
4.3.3. Если оповещение требует несоразмерных усилий. В этом случае может быть использовано публичное оповещение или схожая связь, которая с равной эффективностью информирует субъектов данных.
4.4. Если возникают подозрения об уголовном преступлении (кражу данных совершили Третьи лица и др.), Ответственное лицо после консультации с Заведующим принимает решение об оповещении Государственной полиции и Государственной инспекции данных.