



# ПОЛИТИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ BILDERLINGS

## Содержание

1. Описание политики .....	2
2. Определения.....	3
4. Принципы защиты персональных данных .....	6
5. Согласованная и законная обработка .....	6
6. Обработка для ограниченного круга целей .....	7
8. Надлежащая, соответствующая и достаточная обработка .....	8
9. Точность данных.....	9
10. Хранение данных не дольше, чем необходимо для соответствующей цели.....	9
11. Оценка воздействия на защиту данных.....	10
12. Отчеты по мероприятиям Обработки.....	10
13. Обработка в соответствии с правами Субъекта данных .....	11
14. Безопасность данных.....	12
15. Передача персональных данных в страну за пределами ЕЭЗ.....	13
16. Разглашение и распространение персональных данных.....	14
17. Запросы о наличии информации о Субъекте данных.....	15
18. Уведомление об утечке данных.....	16
19. Контроль документации .....	18
Приложение А: Контроль безопасности со стороны Обработчика данных .....	19



## 1. Описание политики

1.1 Типы персональных данных, которые **компания группы Bilderlings<sup>1</sup>** («Bilderlings», «мы», «нам», «наш») могут потребовать для обработки, являются следующими: информация о действующих, бывших и потенциальных поставщиках, заказчиках, подрядчиках и любых других пользователях каких-либо услуг нашей компании (например, о пользователях веб-сайта) и других лицах, с которыми мы взаимодействуем для реализации целей в рамках нашей деятельности. Персональные данные, которые могут храниться в бумажном или электронном виде или на иных носителях, подлежат определенным процедурам правовой защиты, включая процедуры, указанные в Общем регламенте по защите данных, Регламенте (ЕС) 2016/679 («ОРЗД»), Законе Латвийской Республики «О защите данных физических лиц», Законе «О защите данных» Великобритании (2018) и других нормативных актах.

1.2 Данная политика и любые другие документы, указанные здесь, определяют основные принципы, в соответствии с которыми будут обрабатываться любые Персональные данные, которые мы собираем у Субъектов персональных данных или которые предоставляются Субъектами персональных данных или из других источников. Пользователи данных обязаны соблюдать данную политику при Обработке личных данных от нашего имени. Любое нарушение данной политики может привести к применению дисциплинарных мер и ответственности согласно законодательству. Данная политика сфокусирована на наших обязательствах в роли Контролера персональных данных, и на нас могут быть возложены различные или дополнительные обязательства в отношении любой Обработки, которую мы выполняем в качестве Обработчика персональных данных.

1.3 Настоящий документ является действующей редакцией Политики. Он подлежит пересмотру не реже одного раза в год и периодически обновляется должностным лицом по защите данных для отражения каких-либо изменений в законодательстве или в наших методах и практиках. Ознакомиться с текущей версией Политики можно на веб-сайте Bilderlingspay.com или обратившись к нашему должностному лицу по защите данных.

---

<sup>1</sup>

В группу компаний Bilderlings входят следующие предприятия: Bilderlings Pay Limited, компания, зарегистрированная в Великобритании, номер компании: 09908958, юридический адрес: Прескот-стрит, 66, Лондон, Великобритания, E1 8NN, Регистрационный номер в Управлении по финансовому регулированию и надзору: 900637, и Bilderlings Pay SIA, компания, зарегистрированная в Латвийской Республике, регистрационный номер 40103869042, юридический адрес: улица Пилс 8/10, Рига, LV-1050.



## 2. Определения

**2.1 Субъекты данных** – это все живые идентифицируемые лица, Персональными данными которых мы располагаем. Субъект персональных данных не обязательно должен быть резидентом или гражданином ЕС. Все Субъекты персональных данных имеют законные права в отношении своей персональной информации.

**2.2 Персональные данные** – это данные, касающиеся живого человека, который может быть идентифицирован прямо или опосредовано на основании этих данных (или исходя из этих данных и другой информации, находящейся в нашем распоряжении). Персональные данные могут быть фактическими (например, имя, адрес или дата рождения) или могут быть представлены в виде мнения и описания об этом человеке, его действиях и поведении.

**2.3 Контролеры данных** – это лица или организации, которые устанавливают цели и порядок, в рамках которых выполняется обработка любых Персональных данных. Они несут ответственность за установление практик и политик в соответствии с ОРЗД. **Пользователи данных** – наши сотрудники, агенты, партнеры и подрядчики, которые занимаются Обработкой персональных данных. Пользователи персональных данных должны всегда обеспечивать защиту данных, которые они обрабатывают, в соответствии с настоящей политикой защиты данных и любыми применимыми процедурами обеспечения безопасности данных.

**2.4 Обработчики данных** – это лица или организации, которые выполняют Обработку персональных данных от нашего имени и в соответствии с нашими инструкциями. Сотрудники Контролеров данных не входят в данное определение, но в него могут входить поставщики, которые выполняют Обработку персональных данных от нашего имени.

**2.5 Веб-сайт** – это наш веб-сайт <https://www.bilderlingspay.com/>.

**2.6 Обработка** – это любое действие или ряд действий, которые выполняются с Персональными данными или пакетом Персональных данных при помощи автоматизированных или неавтоматизированных средств. К обработке относится получение, запись или хранение данных или выполнение любой операции или ряда операций с данными, включая организацию, изменение, извлечение, использование, разглашение, удаление или уничтожение. Обработка также включает передачу Персональных данных третьим лицам.



**2.7 Создание профиля** – это любая форма автоматизированной Обработки персональных данных, состоящая в использовании Персональных данных для оценки определенных аспектов личного характера, связанных с физическим лицом, в частности, для анализа или прогнозирования вопросов, касающихся результатов деятельности данного физического лица на работе, его экономического положения, здоровья, личных предпочтений, интересов, надежности, поведения, местоположения или перемещений.

**2.8 Политика обработки персональных данных** – это самая последняя редакция нашей политики, доступная на веб-сайте, касающаяся сбора, хранения и использования Персональных данных (в действующей редакции).

**2.9 Псевдонимизация** – это Обработка персональных данных таким образом, чтобы их больше невозможно было отнести к конкретному Субъекту данных без использования дополнительной информации при условии, что такая дополнительная информация хранится отдельно и подлежит выполнению технических и организационных мероприятий для гарантии того, чтобы Персональные данные не могли быть отнесены к идентифицированному или идентифицируемому физическому лицу. Следует учесть, что данные, подвергнутые псевдонимизации, по-прежнему являются Персональными данными.

**2.10 Конфиденциальные персональные данные** включают информацию о расовом или этническом происхождении человека, его политических взглядах, религиозных или философских убеждениях, членстве в профсоюзах, физическом или психическом здоровье или состоянии, половой жизни, а также о совершении или разбирательстве в отношении любого совершенного или предположительно совершенного преступления данным человеком, урегулировании в рамках такого разбирательства или приговоре какого-либо суда в ходе такого разбирательства. В ОРЗД включены биометрические и генетические данные в качестве Конфиденциальных персональных данных. Конфиденциальные персональные данные могут обрабатываться только при соблюдении строгих условий, включая условие, требующее официального разрешения соответствующего лица, если иначе не предусмотрено действующим законодательством.

**2.11 Услуги** предполагают: (i) доступ к соответствующим решениям Bilderlings, предоставляемый через ссылку аутентификации Клиента на сайте Bilderlings, или ином установленном веб-сайте или IP-адресе; и/или (ii) вспомогательные продукты и услуги, в сети или вне сети, которые Bilderlings предоставляет или на которые выдает лицензию Клиенту.



2.12 **Регистр** – регистр обработки и учёта персональных данных в системах компании Bilderlings и который соответствует требованиям 30 статьи Регламента (ЕС) 2016/679 («ОРЗД»).

### **3. Подотчетность**

3.1 Принцип подотчетности ОРЗД требует от организаций способность подтвердить соответствие требованиям к защите данных. Необходимо гарантировать, чтобы соответствие защиты данных являлось частью любых новых мероприятий по планированию технологии или новых мероприятий по Обработке.

3.2 Должностное лицо по защите данных отвечает за соблюдение настоящей политики и ОРЗД. Адрес электронной почты уполномоченного должностного лица по защите данных в Bilderlings – [DPO@bilderlings.eu](mailto:DPO@bilderlings.eu). По любым вопросам относительно функционирования данной политики или любым предполагаемым случаям нарушения данной политики следует в первую очередь обращаться к должностному лицу по защите данных.

3.3 Должностное лицо по защите данных является независимым должностным лицом, назначенным для выполнения следующих задач от имени Bilderlings:

- Информирование и консультирование нас или наших Обработчиков данных, которые осуществляют мероприятия по Обработке, об обязанностях в соответствии с ОРЗД или положениями по защите данных в конкретных юрисдикциях.
- Мониторинг нашего соответствия ОРЗД или действующему законодательству по защите данных, которые могут относиться к нам, и мониторинг нашего соответствия требованиям нашей политики или политики Обработчика данных.
- Предоставление по запросу рекомендаций в отношении оценки воздействия на защиту персональных данных и контроль ее эффективности.
- Взаимодействие с контролирующим органом и выполнение функций контактного лица для контролирующего органа по вопросам, связанным с Обработкой.

3.4 Субъекты данных могут связываться с должностным лицом по защите данных по всем вопросам, связанным с обработкой их персональных данных, и в отношении их прав в рамках ОРЗД.

3.5 Все сотрудники Bilderlings несут ответственность за соблюдение ОРЗД и должны пройти соответствующую подготовку для обеспечения соблюдения требований данной политики.



Для гарантии того, что должностному лицу по защите данных будет оказана необходимая поддержка при выполнении его обязанностей, такое должностное лицо подчиняется высшему руководству Bilderlings.

## **4. Принципы защиты персональных данных**

Любой, кто выполняет Обработку персональных данных, должен соблюдать принципы надлежащей практики. В отношении персональных данных принципы предусматривают следующее:

- **Согласованная, законная обработка данных физических лиц на условиях прозрачности.**
- **Данные собираются для определенных, явных и законных целей и не обрабатываются в дальнейшем способом, который несовместим с данными целями.**
- **Надлежащие, соответствующие данные, ограниченные аспектами, которые необходимы в рамках цели, для которой выполняется обработка.**
- **Точные и при необходимости актуализированные данные. Если персональные данные являются неточными в отношении цели, для которой они обрабатываются, необходимо предпринять соответствующие шаги для их немедленного удаления или исправления.**
- **Исключение хранения Персональных данных дольше, чем необходимо в рамках целей их обработки.**
- **Обработка с учетом прав Субъектов данных.**
- **Обработка способом, который обеспечивает надлежащую защиту Субъекта данных, включая защиту от несанкционированной Обработки и случайной утраты, уничтожения или повреждения.**
- **Исключение передачи данных лицам или организациям, находящимся в странах, где отсутствует надлежащая защита, без обеспечения соответствующих защитных мер.**

## **5. Согласованная и законная обработка**

5.1 Целью ОРЗД является не предотвращение Обработки персональных данных, а гарантирование того, что обработка будет выполняться согласовано, прозрачно и не окажет негативного воздействия на права Субъекта данных. Конкретные цели, для которых



обрабатываются Персональные данные, должны быть четко и законно сообщены Субъекту данных и установлены в ходе сбора Персональных данных.

5.2 Для законности Обработки персональных данных она должна базироваться на одном из правовых оснований, изложенных в ОРЗД. К ним относятся, среди прочего, согласие Субъекта данных на Обработку или на то, что Обработка необходима для выполнения условий договора с Субъектом данных, с целью соответствия обязательству, предусмотренному законом, которое возлагается на Контролера данных, или в рамках законных интересов Контролера данных или стороны, которой раскрываются данные. При обработке Конфиденциальных персональных данных необходимо выполнить дополнительные условия. При Обработке персональных данных в рамках своей деятельности в качестве Контролеров данных мы обеспечим выполнение данных требований.

## **6. Обработка для ограниченного круга целей**

6.1 В рамках нашей деятельности мы можем осуществлять сбор и Обработку персональных данных. К таким персональным данным могут относиться данные, которые мы получаем непосредственно от Субъекта данных (например, посредством заполнения бланков или ведения переписки с нами по почте, по телефону, электронной почте или иным образом), и данные, которые мы получаем из других источников (включая, например, деловых партнеров, подрядчиков в рамках оказания услуг технического характера, платежей и поставок, агентств оценки кредитного риска и т.д.).

Мы будем обрабатывать персональные данные только для конкретных целей, изложенных в нашей Политике обработки персональных данных, или для любых других целей, особо разрешенных ОРЗД. При первом сборе данных мы уведомим о данных целях Субъекта данных. Мы будем постоянно пересматривать наши уведомления, чтобы в них содержалась точная информация о наших процессах Обработки, и если Обработка данных осуществляется для новой цели, которая не была указана в первоначальном уведомлении, мы отправим новое уведомление с указанием данной информации.

## **7. Категории Субъектов персональных данных**

7.1 Bilderlings осуществляет сбор и обработку различной информации о вас. К такой информации относятся:



- Ваше имя, фамилия, адрес (фактический/декларированный), персональный код и/или дата рождения, пол;
- контактные данные, включая адрес электронной почты и номер телефона;
- копия документа, удостоверяющий вашу личность, его номер, дату выдачи и годности, учреждение, выдавшее данный документ;
- Сведения о вашем гражданстве (также документы об оплате коммунальных услуг), банковский счет, место работы;
- Другая информация и данные о вас, в зависимости от наших взаимоотношений и любые другие персональные данные, обрабатываемые Bilderlings в соответствии с законом, иными местными или международными законодательными нормами;

7.2 Bilderlings осуществляет сбор этой информации различными способами. Например, сбор данных выполняется посредством бланков заявлений, CV или резюме; из паспорта или удостоверения личности; из бланков, заполненных вами в начале или в ходе работы (например, из бланков на получение пособия или льгот); из переписки с вами; путем проведения собеседований, совещаний или других оценок.

7.3 В некоторых случаях Bilderlings может осуществлять сбор персональных данных о вас от третьих лиц, например, рекомендации, предоставленные бывшими работодателями, информация от организаций, занимающихся проверкой данных о сотрудниках, информация от агентств оценки кредитного риска и информация на основании проверок сведений о судимости, разрешенных законом и другая обоснованная информация от других учреждений.

## **8. Надлежащая, соответствующая и достаточная обработка**

8.1 При сборе Персональных данных непосредственно у Субъектов данных их следует исключительно:

- Использовать в рамках цели или целей, предусмотренных в Политике обработки персональных данных, или как разрешено ОРЗД;
- Обрабатывать в соответствии с Политикой обработки персональных данных или как разрешено ОРЗД; и





- Разглашать третьим лицам в соответствии с Политикой обработки персональных данных или как разрешено ОРЗД.

8.2 При получении Персональных данных о Субъекте данных из других источников мы предоставим Субъекту данных эту информацию в кратчайшие сроки.

8.3 Bilderlings необходимо осуществить обработку данных для внесения их в договор с клиентом, заключенный с вами, и для выполнения обязательств в соответствии с договором клиента.

8.4 В некоторых случаях Bilderlings необходимо осуществить обработку данных с целью гарантии соблюдения своих обязательств, предусмотренных законом, например, законодательством о контроле за отмыванием денег.

8.5 В других случаях Bilderlings имеет законное право осуществлять обработку персональных данных до, во время и после окончания взаимоотношений в рамках трудового соглашения/договора с клиентом.

## **9. Точность данных**

Мы гарантируем, что Персональные данные, которыми мы располагаем, являются точными и актуальными. Мы будем выполнять проверку точности любых Персональных данных в момент сбора и через определенные промежутки времени впоследствии. Мы предпримем все соответствующие меры для уничтожения или изменения неточных или устаревших данных.

## **10. Хранение данных не дольше, чем необходимо для соответствующей цели**

10.1 Мы не храним Персональные данные дольше, чем это необходимо в рамках использования или предоставления Услуг, и/или для цели или целей, для которых они были собраны. Должностное лицо по защите данных будет проводить периодические проверки хранимых данных в соответствии с графиком сбора.

10.2 Персональные данные хранятся только в течение периода, оправданно необходимого для предоставления Услуг и для выполнения целей, изложенных в нашей Политике обработки персональных данных. Например, мы будем хранить Персональные данные Субъектов данных, пока они используют или способствуют предоставлению Услуг, и в



течение соответствующего периода времени впоследствии, как указано в Регистре, если по закону не требуется или не разрешен более длительный период хранения.

10.3 В течение срока действия договора Клиенты могут экспортировать копию данных Клиента, обработанных Услугами. В течение 30 дней после прекращения работы Услуги Клиенты могут: 1) запросить возврат данных Клиента, переданных Услугам; или 2) получить доступ к своей учетной записи для экспорта или загрузки данных Клиента, предоставленных Услугам.

10.4 После прекращения работы Услуги, по истечении 30 дней, предусмотренных для возврата данных Клиента, данные Клиента, представленные Услугам, хранятся в неактивном состоянии в течение срока до 90 дней, после чего данные затираются или удаляются надлежащим образом, если по закону не требуется или не разрешен более длительный период хранения.

## **11. Оценка воздействия на защиту данных**

11.1 В случае внедрения новых видов Обработки или разработки новых технологий в нашу деятельность необходимо выполнить оценку воздействия изменений операций на защиту таких Персональных данных для рассмотрения любых операций Обработки, которые представляют высокий риск в отношении прав и свобод Субъектов данных или риск несоблюдения ОРЗД.

11.2 Такая оценка будет проводиться по рекомендации должностного лица по защите данных.

## **12. Отчеты по мероприятиям Обработки**

Мы будем вести учет мероприятий Обработки (в Реестре), которые мы проводим. Будет указана следующая информация:

- имя и контактные данные Контролера данных.
- цель Обработки.
- описание категорий Субъектов данных и категорий Персональных данных.
- категории получателей, которым были или будут разглашены Персональные данные, включая получателей в третьих странах или международные организации,



и документацию о соответствующих мерах безопасности, касающихся такого разглашения.

- Временные ограничения уничтожения различных категорий данных.

## **13. Обработка в соответствии с правами Субъекта данных**

13.1 Мы будем осуществлять обработку всех Персональных данных в соответствии с правами Субъектов данных, в частности с их правом, при определенных обстоятельствах, на следующее:

- Запрос доступа к любым данным о них, хранящимся Контролером данных в общепринятом и машиночитаемом формате.
- Передача своих данных другому Контролеру данных (бесплатно), если такие Персональные данные обрабатываются на основании согласия или выполнения договора, если только данное требование не будет оказывать негативное воздействие на права или свободы других Субъектов данных или другие аспекты, например, коммерческую тайну или интеллектуальную собственность.
- Предотвращение обработки своих данных или отзыв своего согласия в любое время при определенных обстоятельствах.
- Просьба скорректировать неточные данные.
- Уничтожение Персональных данных, если они больше не требуются в рамках первоначальной цели или если Субъект данных отозвал свое согласие и никакие другие законные основания для Обработки не применимы.
- Запрет на Обработку Персональных данных при определенных обстоятельствах.
- Получение уведомления, если Персональные данные подлежат принятию решения в автоматическом режиме, то есть создание профиля, включая связанный с этим алгоритм, а также значимость и предполагаемые последствия такой обработки для Субъекта данных и непринятие такого профиля при определенных обстоятельствах.

13.2 Если мы должны предоставить копию Персональных данных, она будет предоставлена бесплатно, однако любые другие запрашиваемые копии могут предоставляться за соответствующую плату, исходя из административных расходов.

13.3 Если мы прекращаем Обработку Персональных данных или удаляем Персональные данные Субъекта данных, это может означать, что этот конкретный Субъект данных не может продолжать использовать или способствовать предоставлению некоторых наших Услуг, и об этом следует уведомить Субъект данных соответствующим образом.



13.4 Если Субъект данных просит внести исправления или удалить (за исключением данных, предусмотренных любыми правовыми обязательствами) его Персональные данные или ограничить любую Обработку таких Персональных данных, нам, возможно, будет необходимо уведомить некоторых третьих лиц, которым были разглашены такие Персональные данные в рамках такого запроса.

## **14. Безопасность данных**

14.1 В следующих правилах изложено, как в Bilderlings обрабатываются Персональные данные, и основные принципы конфиденциальности данных, которые соблюдает компания. В этом разделе основное внимание сфокусировано на роли Bilderlings в качестве контролера данных, и он не является частью дополнения к процедуре обработки данных Bilderlings.

14.2 В Bilderlings внедрены процедуры, предназначенные для гарантии обработки Данных клиента только по указанию Клиента, как описано в Приложении А («Контроль безопасности»), во всей цепочке мероприятий по обработке данных Bilderlings и ее Суб-обработчиков. Кроме того, Услуги проходят оценку безопасности со стороны собственного персонала и третьих лиц, которая предполагает оценку уязвимости инфраструктуры и оценки безопасности приложений.

14.3 Bilderlings серьезно относится к безопасности ваших данных. Bilderlings располагает внутренними политиками и средствами контроля, чтобы исключить потерю, случайное уничтожение, ненадлежащее использование или разглашение ваших данных, доступ к ним не предусмотрен, кроме как в рамках исполнения обязанностей сотрудника. Но помните, что не существует способа передачи данных через Интернет и метода хранения данных в электронном виде, которые обеспечат 100% безопасность и надежность, и мы не можем гарантировать абсолютную безопасность.

14.4 Если Bilderlings привлекает третьих лиц к обработке персональных данных от своего имени, они производят ее на основании письменных инструкций, в рамках обязанности сохранения конфиденциальности и должны выполнять соответствующие технические процедуры и мероприятия компании для обеспечения безопасности данных.

14.5 Мы обеспечим безопасность данных, защищая конфиденциальность, целостность и доступность Персональных данных, определяемых следующим образом:



- **Конфиденциальность** означает, что только лица, которым разрешено использовать данные, имеют к ним доступ.
- **Целостность** означает, что Персональные данные должны быть точными и соответствующими целям, для которых они обрабатываются.
- **Доступность** означает, что правомочные пользователи должны иметь доступ к данным, если они им нужны для официально утвержденных целей. Поэтому Персональные данные должны храниться в надежных хранилищах данных.

#### 14.6 Процедура обеспечения безопасности включает:

- **Контроль физической безопасности.** Средства компании Bilderlings включают механизмы контроля (например, аварийные сигналы, процесс сопровождения посетителей и значки контрольно-пропускного режима) для предотвращения несанкционированного доступа.
- **Безопасные блокируемые столы и шкафы.** Если в них хранится любого рода конфиденциальная информация, столы и шкафы должны быть заперты. (Персональные данные всегда считаются конфиденциальной информацией.)
- **Методы удаления.** Документы в бумажном виде измельчаются, а цифровые носители данных физически уничтожаются или надежно затираются, если они больше не нужны.
- **Оборудование.** Пользователи данных должны обеспечить, чтобы конфиденциальная информация на их мониторах не была видна проходящим мимо лицам, а также отключать свой ПК или блокировать сеанс, когда оставляют его без присмотра.
- **Управление инцидентами.** Компания Bilderlings обеспечивает политику и процедуры управления инцидентами в сфере безопасности. Bilderlings без необоснованной задержки уведомляет Субъекты данных, подвергнутых воздействию, о любом несанкционированном разглашении их соответствующих Персональных данных Bilderlings или ее агентами, о которых компания Bilderlings осведомлена в объеме, предусмотренном законами и нормативными документами о защите данных.
- **Технические средства защиты.** Компания Bilderlings гарантирует наличие технических и организационных мероприятий для обеспечения безопасности и минимизации данных, включая антивирус, обнаружение вторжений, службы аутентификации пользователей, псевдонимизацию и кодирование данных при необходимости.

## 15. Передача персональных данных в страну за пределами ЕЭЗ



15.1 Мы можем передавать любые Персональные данные, которые имеем в нашем распоряжении, в страну за пределами Европейской экономической зоны («ЕЭЗ») при условии применения одного из следующих условий:

- Страна (или организация), в которую выполняется передача Персональных данных, обеспечивает надлежащий уровень защиты прав и свобод Субъекта данных (например, на основании решений о достаточности, утвержденных обязательных корпоративных правил, стандартных договорных положений).
- Субъект данных предоставил свое согласие.
- Передача необходима по одной из причин, изложенных в ОРЗД, включая выполнение договора, заключенного между нами и Субъектом данных, или для защиты жизненно важных интересов Субъекта данных.
- Передача требуется согласно закону на основании важных общественных интересов или для создания, осуществления или защиты законных требований.
- Передача разрешена соответствующим органом по защите данных, если мы предприняли надлежащие меры безопасности в отношении защиты конфиденциальности Субъектов данных, их основных прав и свобод и реализации их прав.

15.2 В соответствии с требованиями, изложенными выше в пункте 15.1, Персональные данные, которыми мы располагаем, также могут обрабатываться сотрудниками, действующими за пределами ЕЭЗ, которые работают для нас или для одного из наших поставщиков. Эти сотрудники могут, среди прочего, заниматься выполнением договоров, заключенных с Объектом данных, обработкой данных по оплате и предоставлением дополнительных услуг.

## **16. Разглашение и распространение персональных данных**

16.1 В соответствии с пунктом 15 мы можем делиться Персональными данными, которыми располагаем, с любым членом нашей Группы.

16.2 Мы также можем разглашать Персональные данные, которыми располагаем, третьим лицам:

- В случае, если мы продаем или покупаем какой-либо бизнес или активы, мы можем разглашать Персональные данные, которыми располагаем, потенциальному продавцу или покупателю такого бизнеса или активов исходя из принципа служебной необходимости.



- Если мы или практически все наши активы приобретены третьей стороной, Персональные данные, которыми мы располагаем, будут одним из переданных активов.
- Если мы обязаны разглашать или делиться Персональными данными Субъекта данных в целях соблюдения любого правового обязательства или в целях обеспечения исполнения или применения любого договора с Субъектом данных или других соглашений; или в целях защиты наших прав, собственности или безопасности наших сотрудников, клиентов или других лиц. Данное требование предусматривает обмен информацией с другими компаниями и организациями в целях защиты от мошенничества и снижения уровня кредитного риска.

16.3 Мы также можем делиться Персональными данными, которыми располагаем, с wybranymi нами третьими лицами, включая, помимо прочего, наших деловых партнеров, поставщиков услуг и субподрядчиков для выполнения любого договора, который мы заключили с ними или Субъектом данных, если мы уведомили Субъекта данных соответствующим образом.

16.4 Разглашение/распространение Персональных данных за пределами нашей организации сопряжено с дополнительными рисками, и мы должны обеспечить наличие надлежащих организационных, технических и договорных мероприятий до передачи или предоставления доступа к Персональным данным.

## **17. Запросы о наличии информации о Субъекте данных**

17.1 В соответствии с ОРЗД Субъекты данных имеют ряд прав на доступ, внесение поправок, удаление и ограниченную обработку Персональных данных. К таким правам относятся:

- доступ и получение копии ваших данных по запросу;
- требование, чтобы компания Bilderlings внесла изменения в неправильные или неполные данные;
- требование, чтобы компания Bilderlings удалила или прекратила обработку ваших данных, например, когда данные больше не требуются для обработки;
- возражение против обработки ваших данных, если Bilderlings полагается на свои законные интересы в качестве правового основания для обработки; а также
- просьба в адрес Bilderlings прекратить обработку данных на время, если данные являются неточными или существует спор относительно соответствия ваших интересов законным основаниям Bilderlings для обработки



17.2 Субъекты данных должны подавать формальный запрос на получение информации о них, которой мы располагаем. Запрос оформляется в письменной форме. Сотрудники, получившие письменный запрос, должны немедленно отправить его должностному лицу по защите данных.

17.3 Наши сотрудники направят запрос должностному лицу по защите данных для оказания помощи в сложных ситуациях. Нельзя запугивать сотрудников в отношении разглашения Персональных данных.

17.4 Все запросы относительно доступа Субъекта данных обрабатываются в течение месяца с момента их получения, такой запрос выполняется бесплатно.

17.5 Мы не будем взимать плату за запросы относительно доступа Субъекта данных, если любые запросы, которые мы получаем, не будут слишком часто повторяться или явно будут необоснованными, мы можем взимать административный сбор за обработку подобных запросов или отказываться выполнять такие запросы.

## **18. Уведомление об утечке данных**

18.1 В случае утечки Персональных данных, если она может привести к высокому риску нарушения прав и свобод Субъекта данных, мы сообщим об утечке в Уполномоченный орган по вопросам информации, по возможности без необоснованной задержки, но не позднее 72 часов после того, как об этом стало известно.

18.2 В случае утечки Персональных данных, и если она может привести к высокому риску нарушения прав и свобод Субъекта данных, мы без необоснованной задержки сообщим о нарушении Субъекту данных. В уведомлении, предназначенном для Субъекта данных, будет описан характер утечки Персональных данных, а также рекомендации для Субъекта данных, связанные с уменьшением потенциальных неблагоприятных последствий. Такие уведомления Субъектам данных оформляются в кратчайшие соответствующие сроки и при тесном сотрудничестве с надзорным органом, при условии соблюдения указаний, предоставляемых таким органом или другими соответствующими органами, например, правоохранительными.





**BILDERLINGS PAY**



## 19. Контроль документации

### УТВЕРЖДЕНИЕ И ПРАВО СОБСТВЕННОСТИ

Подготовил	Должность	Дата	Имя
Автор Политики	Должностное лицо по защите данных	02.05.2018 г.	Сергей Кравченко
Утвердил	Должность	Дата	Имя
Куратор проекта	Член правления	03.05.2018 г.	Андрей Кузин

### ЖУРНАЛ ИЗМЕНЕНИЙ

Версия	Дата редакции	Дата пересмотра	Описание
Первая			



# Приложение А: Контроль безопасности со стороны Обработчика данных

## 1. Характер и цель Обработки

1.1 Компания Bilderlings выполняет обработку Персональных данных по мере необходимости в рамках услуг, предоставляемых компанией Bilderlings, и, как указано далее Клиентом при использовании Услуг, в качестве Контролера данных. Данная процедура предусматривает автоматическую обработку Персональных данных для оценки и анализа определенных вопросов личного характера, относящихся к Субъекту данных, в частности для анализа или прогнозирования вопросов, касающихся личных предпочтений, интересов, поведения и местоположения Субъекта данных.

## 2. Категории Субъектов данных

2.1 Клиент может предоставлять Персональные сервисам Bilderlings данные, объем которых определяется и контролируется Клиентом, по собственному усмотрению и которые могут включать, но не ограничиваются, Персональными данными, относящимися к следующим категориям Субъектов данных:

- Потенциальные клиенты, заказчики, деловые партнеры и продавцы Клиента (которые являются физическими лицами);
- Сотрудники или контактные лица потенциальных клиентов, заказчиков, деловых партнеров и поставщиков;
- Сотрудники, агенты, консультанты, внештатные сотрудники Клиента (физические лица);
- Пользователи Клиента, имеющие право пользоваться Услугами.

## 3. Типы персональных данных

3.1 Клиент может предоставить или разрешить сбор при использовании Услуг Персональных данных, объем которых определяется и контролируется Клиентом по своему усмотрению, и которые могут включать, но не ограничиваться, следующими категориями Персональных данных:

- Имя и фамилия;
- Обращение;



- Должность;
- Работодатель;
- Контактные данные (компания, адрес электронной почты, телефон, фактический адрес предприятия);
- Идентификационные данные;
- Поведенческая информация и данные профиля;
- Индивидуальные предпочтения;
- Данные о соединении;
- Данные о месторасположении;
- Другие данные и информация в соответствии с законодательством, другими местными законодательными нормами или международными правилами.

## **4. Классификация данных**

4.1 Управление Услугами осуществляется в рамках многоуровневой структуры, которая предназначена для разделения и строгого хранения и доступа к данным Клиента исходя из потребностей предприятия. Структура обеспечивает эффективную, логическую классификацию данных для разных категорий Клиентов с помощью уникальных идентификаторов, характерных для Клиента, и позволяет использовать привилегии доступа, основанные на роли Клиента и Пользователя. Дополнительная классификация данных обеспечивается за счет предоставления отдельных сред для различных функций, особенно для проведения испытаний и производства.

## **5. Контроль безопасности**

5.1 Компания Bilderlings внедрила процедуры, разработанные для гарантии обработки данных клиента только по указанию Клиента во всей цепочке мероприятий по обработке компании Bilderlings и ее Субобработчиков данных. Кроме того, Услуги подвергаются оценке безопасности, которая проводится собственными сотрудниками и третьими лицами, процедура предусматривает выполнение оценки уязвимости инфраструктуры и оценки безопасности приложений.

5.2 Bilderlings использует ряд средств контроля безопасности, которые включают:



- Уникальные идентификаторы пользователей, позволяющие Клиентам устанавливать уникальные учетные данные для своих пользователей, а также устанавливать и осуществлять управление соответствующими разрешениями и правами;
- Средства контроля для гарантии сброса первоначального пароля при первом использовании;
- Средства контроля для ограничения повторного использования пароля;
- Требования к длине и сложности пароля;
- Клиенты имеют возможность объединить технологии однократного входа (Single Sign-On) для непосредственного контроля подлинности и сложности соответствующих данных, истечения срока действия, блокировки учетной записи, внесения в белый или черный список согласно степени защиты;
- Клиенты имеют возможность управлять приложениями своих пользователей, определять функции и применять разрешения и права в рамках внедрения Услуг;
- Пароли пользователей хранятся с использованием формата одностороннего солёного хэша и не передаются в незашифрованном виде;
- Хранилище паролей, зашифрованных с использованием 256-битного AES-шифрования;
- Сохраняются записи журнала доступа пользователей, содержащие дату, время, имя пользователя, URL-адрес или идентификатор данных, выполненную операцию (доступ, создание, редактирование, удаление);
- Если есть подозрение в ненадлежащем доступе к Услугам, Bilderlings может предоставить записи в журнале регистрации Клиентов с целью оказания помощи в проведении экспертного анализа. Данная услуга предоставляется Клиентам исходя из времени и материалов, имеющихся в наличии;
- Журналы доступа пользователей будут храниться в безопасном централизованном месте для предотвращения несанкционированного доступа;
- Журналы доступа пользователей хранятся не менее 90 дней;
- Персонал компании Bilderlings не осуществляет установку определенного пароля пользователю.



## **6. Обнаружение вторжения**

6.1 **Bilderlings** или уполномоченная независимая третья сторона осуществляет мониторинг Услуг на возможность несанкционированного доступа с использованием механизмов обнаружения вторжения на сервере.

## **7. Журналы безопасности**

7.1 Все системы **Bilderlings**, используемые при предоставлении Услуг, включая межсетевые экраны, маршрутизаторы, сетевые коммутаторы и операционные системы, выполняют регистрацию информации в соответствующем системном журнале или централизованном сервере журналов (для сетевых систем) с целью упрощения обзора и анализа безопасности.

## **8. Управление инцидентами**

8.1 **Bilderlings** в рамках безопасности обеспечивает политику и процедуры управления инцидентами. Компания **Bilderlings** без необоснованной задержки сообщает Клиенту о любом несанкционированном разглашении соответствующих данных Клиента компанией **Bilderlings** или ее агентами, о котором **Bilderlings** узнает, в той степени, в которой это предусмотрено законодательством о защите данных.

## **9. Аутентификация пользователей**

9.1 Для доступа к Услугам требуется действующая комбинация имени пользователя и пароля (или встроенного механизма однократного входа (Single Sign-On), которые шифруются посредством TLS во время передачи, а также специальные сведения об аппаратуре для проверки подлинности, как описано выше в разделе «Контроль безопасности». После успешной проверки подлинности пользователя формируется случайный идентификатор сеанса и сохраняется в браузере пользователя для хранения и отслеживания состояния сеанса.

## **10. Физическая безопасность**

10.1 Центры производственных данных используются для гарантии того, что Услуги обладают Системами контроля доступа. Данные системы позволяют иметь доступ к охраняемым зонам только уполномоченному персоналу. Данные средства рассчитаны на воздействие неблагоприятных погодных условий и другие обосновано предсказуемые



природные условия, обеспечиваются круглосуточной охраной, двухфакторным доступом, включая биометрические данные и контролируемое сопровождение, а также обеспечиваются резервными генераторами на площадке на случай сбоя подачи питания.

## **11. Надежность и резервное копирование**

11.1 Настройка всех компонентов инфраструктуры выполнена в режиме высокой доступности или режиме дублирования. Все данные Клиента, предоставленные Услугам, хранятся в инфраструктуре, которая гарантирует высокую доступность и регулярно копируется. Данные резервного копирования хранятся не менее 1 месяца. Резервные копии передаются и сохраняются в зашифрованном виде и хранятся в центре обработки вторичных данных.

## **12. Восстановление после аварий**

12.1 Производственные системы Услуг защищены посредством планов восстановления после аварий, которые обеспечивают резервное копирование важных данных и услуг. Существует общая система процессов восстановления, позволяющая системам, которые особо важны для бесперебойной деятельности, вернуться в рабочий режим в течение максимально короткого периода времени. Процессы восстановления для обеспечения безопасности баз данных, системного администрирования и настройки сети и данных обеспечивают оперативную схему для персонала с целью гарантии доступности процессов после отключения.

## **13. Вредоносные программы**

13.1 Услуги имеют средства контроля, предназначенные для предотвращения и обнаружения вредоносного ПО на соответствующих платформах обслуживания.

## **14. Кодирование данных**

14.1 Услуги используют или позволяют Клиентам использовать принятые в отрасли устройства шифрования для защиты данных Клиента и коммуникаций во время передач данных между сетью Клиента и Услугами, включая как минимум 128-битные сертификаты TLS и 2048-битные RSA-ключи общего пользования.



## **15. Возврат данных Клиента:**

15.1 В течение срока действия договора Клиенты могут экспортировать копию данных Клиента, обрабатываемых Услугами. В течение 30 дней после прекращения действия применимой Услуги могут: 1) запрашивать возврат данных Клиента, переданных на Услуги; или 2) получить доступ к своей учетной записи для экспорта или загрузки данных Клиентов, предоставленных Услугам.

## **16. Удаление данных Клиента**

16.1 По истечении 30 дней для возврата данных Клиента после прекращения действия Услуги, переданные на Услуги данные хранятся в неактивном состоянии в течение 90 дней, после чего данные надлежащим образом затираются или удаляются, если только законы, постановления или другие наши обязательства не предусматривают иных действий.

## **17. Использование и отчетность по направлениям**

17.1 Bilderlings может отслеживать и анализировать использование Услуг в целях безопасности и содействия Bilderlings в улучшении как Услуг, так и пользовательского опыта пользования Услугами. Например, мы можем использовать данную информацию для понимания и анализа тенденций или отслеживания наших функций, которые используются чаще всего, для улучшения функциональности продукта.

17.2 Bilderlings может предоставлять анонимные данные использования поставщикам услуг компании Bilderlings с целью оказания помощи Bilderlings в вопросах отслеживания, анализа и усовершенствования. Кроме того, Bilderlings может предоставлять такие анонимные данные об использовании на основании комплексного подхода в ходе ведения деятельности в обычном режиме; например, мы можем предоставлять информацию публично с целью указания направлений общего пользования нашими Услугами.

## **18. Субобработчики данных**

18.1 Компания Bilderlings и ее аффилированные лица заключили письменные соглашения с Субобработчиками данных, содержащие обязанности по обеспечению конфиденциальности, защите данных и безопасности данных, которые обеспечивают уровень защиты, соответствующий их мероприятиям по обработке.





18.2 Bilderlings пользуется услугами следующих Субобработчиков данных для обеспечения части инфраструктуры компании Bilderlings для размещения данных Клиента и предоставления Услуг:

- **Для обеспечения оплаты картой** – SIA Worldline Latvia (Пер. № 40003072814, ул. Дзирнаву, 37, Рига, LV-1010)
- **Для обеспечения оплаты картой (в качестве покупателя)** – BlueOrangeBank JSC (Пер. № 40003551060, ул. Смилшу, 37, Рига, LV-1050)
- **Для служб хранения данных и служб электронной почты MSO365** – Squalio LLC JSC (Пер. № 40003351675, ул. Кришьяня Валдемара, 21-19, Рига, LV-1010)
- **Для управления ресурсами клиента** – Salesforce.com INC. (Пер. № The Landmark, Маркет Стрит, 1, Сан-Франциско, Калифорния 94105, США)
- **Для подготовки предложений о страховании** - AAS "ERGO" (Пер. № 40003131253, ул. Сканстес, 50, Рига, LV-1013)
- **Для обеспечения платежных услуг** – SIA DEAC (Пер. № 40103255973, ул. Маскавас, 459, Рига, LV-1063)

## **19. Европейские специальные положения – Передача за границу**

19.1 ОРЗД предусматривает запрет на передачу Персональных данных в страну или на территорию за пределами Европейской экономической зоны (т. е. государства-члены ЕС, а также Исландия, Лихтенштейн и Норвегия, Великобритания – после 29 марта 2019 г.), если только эта страна, или территория, или организация не обеспечит надлежащий уровень защиты прав и свобод Субъектов данных в отношении обработки Персональных данных.

19.2 В соответствии с пунктом 3.20, если Клиент и компания Bilderlings расположены в ЕЭЗ, Bilderlings не передает Персональные данные в любую страну за пределами ЕЭЗ без предварительного письменного согласия Клиента, за исключением передачи данных в и из: (i) любой страны, которая имеет действующее соответствующее решение Европейской комиссии; или (ii) любой организации, которая гарантирует надлежащий уровень защиты в соответствии с применимыми законами и нормативными актами о защите данных.