Я, принимаю решение о предоставлении моих персональных данных и даю согласие на их обработку следующему субъекту информационных отношений:

ООО «Вайз Технолоджиз», 220005 РБ, г. Минск, ул. Тимирязева, 65Б, 7 этаж, офис 711, УНП 691468858.

Кроме указанных персональных данных я также выражаю свое согласие на обработку субъектом информационных отношений следующей информации:

Время/дата начала работы и ее окончания; время/дата фотографий; статус датчиков GPS; статус настройки определения местоположения устройства по сети; статус соединения с сетью «Интернет»; список установленного на устройстве субъекта персональных данных ПО для проверки на наличие ПО для изменения геолокации и получения прав супер пользователя; получение сведений о получении устройства в течение осуществления работы в wiserep; информация о настройках времени и часовых поясов; логирование действий в WiseRep и состояния батареи.

Срок, в течение которого действует настоящее согласие – 5 лет

На основании моего письменного обращения с требованием о прекращении обработки персональных данных субъект информационных отношений прекратит обработку таких персональных данных в течение 3 (трех) рабочих дней, о чем мне будет направлено письменное уведомление в течение 10 (десяти) рабочих дней. Обработка персональных данных прекращается в случае ликвидации или реорганизации субъекта информационных отношений. Я согласен с тем, что по моему письменному требованию уведомление об уничтожении персональных данных будет вручаться мне (моему представителю) по месту нахождения обособленного подразделения субъекта информационных отношений.

I, user name, make a decision on provision of my personal data and express my will consent to their processing to this informational relations subject:

Wise Technologies LLC, 220005 Republic of Belarus, Minsk, 65Б Timiryazeva str., 7 floor. Office 711, Taxpayer Identification Number 69146885.

Besides the specified personal data, I also express my consent for the processing by informational relations subject of the following information:

Work start and completion time/date; time/date of photos; status of GPS sensors; status of configuration of location sensing via network; status of the Internet connection; the list of the software installed on the PD subject's device for the verification of availability of the software for the geolocation variation and access to the super-user rights; information on receipt of a device within the period of work performance in wiserep; information of time and time-zones settings; logging of actions in WiseRep and of battery status.

The period of validity of this consent of the personal data subject is 5 years:

The informational relations subject shall terminate the personal data processing within three (3) business days upon my written application with the request for the termination of processing of its personal data; notice hereof I shall be notified in writing about it within ten (10) business days. The personal data processing shall be terminated in case of liquidation or reorganization of the informational relations subject. I agree that upon my written request the notice of the personal data destruction shall be handed in to me (my representative) at the offices of the informational relations subject's separate subdivision.

Wise Technologies
SIMPLE OUTSIDE, WISE INSIDE

"УТВЕРЖДЕНО"
Директор Волчкевич О.А.
(должность) (личная подпись) (расшифровка подписи)
Приказ №1-17 от 12.02.2016

Положение об обработке и защите персональных данных

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с законодательством Российской Федерации о персональных данных (далее по тексту - ПДн) и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в информационных системах ПДн (далее — ИСПДн).

1.2. В целях настоящего Положения используются следующие термины:

персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники;

распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц;

предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц;

блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн);

уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и /или в результате которых уничтожаются материальные носители ПДн;

обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3. Настоящее Положение определяет порядок и условия обработки ПДн в ООО «Вайз Технолоджиз» (далее по тексту - Оператор), включая порядок передачи ПДн третьим лицам, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн, систему защиту ПДн, порядок организации внутреннего контроля и ответственность за нарушения при обработке ПДн, иные вопросы.

1.4. Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передачу), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.5. Настоящее Положение вступает в силу с момента его утверждения Руководителем Оператора и действует бессрочно, до замены его новым Положением.

1.6. Все изменения в Положение вносятся приказом.

1.7. Ответственные лица Оператора должны быть ознакомлены с настоящим Положением.

2. Цели и задачи обработки ПДн

2.1. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

2.2. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

2.3. Обработке подлежат только ПДн, которые отвечают целям их обработки.

2.4. Содержание и объем, обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

2.5. Обработка ПДн сотрудников Оператора может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Оператора.

2.6. Основной целью обработки ПДн является исполнение договорных обязательств.

3. Персональные данные, обрабатываемые в ИСПДн

3.1. В ИСПДн обрабатываются ПДн следующих субъектов ПДн:

3.1.1. сотрудники Оператора;

3.1.2. клиенты (потребители услуг Оператора);

3.1.3. контрагенты Оператора

3.1.4. сотрудники правообладателя (разработчика) программного обеспечения Оператора, осуществляющие эксплуатационную и сервисную поддержку;

3.2. Данный перечень может пересматриваться по мере необходимости.

3.3. Персональные данные субъектов ПДн включают: фамилию, имя, отчество, контактный телефон, а также адрес электронной почты.

3.4. Кроме указанных персональных данных оператор также вправе обрабатывать следующую информацию, получаемую от субъекта персональных данных посредством ПО оператора: Время/дата начала работы и ее окончания; время/дата фотографий; статус датчиков GPS; статус настройки определения местоположения устройства по сети; статус соединения с сетью «Интернет»; список установленного на устройстве субъекта персональных данных ПО для проверки на наличие ПО для изменения геолокации и получения прав супер пользователя; получение сведений о получении устройства в течение осуществления работы в wiserep; информация о настройках времени и часовых поясов; логирование действий в WiseRep и состояния батареи.

4. Доступ к ПДн

4.1. Сотрудники Оператора, которые в силу выполняемых служебных обязанностей постоянно работают с ПДн, получают допуск к ПДн на срок выполнения ими соответствующих должностных обязанностей.

4.2. Оператором установлен разрешительный порядок доступа к ПДн. Сотрудникам Оператора предоставляется доступ к работе с ПДн исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

4.3. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником Оператора по согласованию Руководителя.

4.4. Доступ к ПДн третьих лиц, не являющихся сотрудниками Оператора без согласия субъекта ПДн, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется с ведома Руководителя Оператора.

4.5. Доступ сотрудника Оператора к ПДн прекращается с даты, прекращения трудовых отношений, либо даты изменения должностных обязанностей сотрудника и/или исключения сотрудника из списка лиц, имеющих право доступа к ПДн. В случае увольнения все носители, содержащие ПДн, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы, должны быть переданы соответствующему должностному лицу.

5. Основные требования по защите ПДн

5.1. При обработке ПДн в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и/или передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к ПДн;

в) недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль над обеспечением уровня защищенности ПДн.

5.2. Оператор обязан принимать необходимые правовые, организационные, технические и другие меры для обеспечения безопасности ПДн.

5.3. Оператором используется технические средства и программное оборудование для обработки и защиты ПДн.

5.4. Все лица, допущенные к работе с ПДн, а также связанные с эксплуатацией и техническим сопровождением ИСПДн должны быть ознакомлены с требованиями настоящего Положения.

5.5. Сотрудники обязаны незамедлительно сообщать соответствующему должностному лицу Оператора об утрате или недостаче носителей информации, составляющей ПДн, а также о причинах и условиях возможной утечки ПДн. В случае попытки посторонних лиц получить от сотрудника ПДн, обрабатываемых Оператором незамедлительно известить об этом соответствующее должностное лицо Оператора.

6. Согласие на обработку ПДн

6.1. Субъект ПДн принимает решение о предоставлении своих ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством РФ.

6.2. Получение письменного согласия на обработку ПДн осуществляется сотрудником Оператора либо по поручению Оператора контрагентом Оператора.

7. Порядок обработки и защиты ПДн

7.1. Обеспечение конфиденциальности ПДн, обрабатывающихся Оператором, является обязательным требованием для всех лиц, которым ПДн стали известны.

7.2. Сотрудники Оператора, осуществляющие оформление документов, обязаны получать в установленных случаях согласие субъектов ПДн на обработку.

7.3. В случае нарушения установленного порядка обработки ПДн сотрудники Оператора несут ответственность в соответствии с разделом 8 настоящего Положения.

7.4. ПДн субъектов на бумажных носителях, обрабатываемые Оператором, хранятся в отделах (у сотрудников), имеющих допуск к обработке соответствующих ПДн. Право допуска сотрудников к неавтоматизированной ИСПДн определяется приказом Руководителя. Носители ПДн не должны оставаться без присмотра. При покидании рабочего места, сотрудники, осуществляющие обработку

ПДн должны, убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче ПДн осуществляется по возможности их восстановление.

7.5. Места хранения документов, содержащих ПДн:

7.5.1. ПДн клиентов Оператора (договоры, акты, соглашения, анкеты, копии паспортов, иные подобные документы, содержащие ПДн клиентов Оператора, носители информации (флеш-карты, диски, и т.п.) хранятся в основном и запасном офисах Оператора, размещаются на полках и запираются на ключ. Ответственное лицо, осуществляющее контроль определяется приказом Руководителя.

7.5.2. ПДн сотрудников Оператора — документы, носители информации (флеш-карты, диски и т.п.) хранятся в сейфе компании и запираются на ключ. Ответственное лицо, осуществляющее контроль — Руководитель Оператора.

7.6. Выдача документов для ознакомления осуществляется лицам, допущенным к соответствующей информации в целях исполнения должностных обязанностей, на срок, не более одного рабочего дня.

7.7. При работе с программными средствами автоматизированной системы Оператора, реализующей функции просмотра и редактирования ПДн, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

7.8. При получении ПДн сотрудником Оператора, который в соответствии с должностными обязанностями получает ПДн от клиента, сотрудника иного лица в обязательном порядке проводится проверка достоверности ПДн. Ввод ПДн, полученных Оператором, в информационную систему осуществляется сотрудниками имеющими доступ к соответствующим ПДн. Сотрудники, осуществляющие ввод информации, несут ответственность за достоверность и полноту введенной информации.

7.9. Особенности обработки ПДн, содержащихся на бумажных носителях, без использования средств автоматизации (при составлении документов не используется ПЭВМ) установлены в соответствии с Постановлением Правительства РФ от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

7.10. При неавтоматизированной обработке ПДн на бумажных носителях:

7.10.1. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы;

7.10.2. ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

7.11. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее — типовые формы), должны соблюдаться следующие условия:

7.11.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн;

7.11.2. Типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, — при необходимости получения письменного согласия на обработку ПДн;

7.11.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

7.11.4. Типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

7.12. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

7.13. Случаи уничтожения, блокирования и уточнения ПДн:

7.14. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

7.15. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя — путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

7.16. Уничтожение носителей, содержащих ПДн, осуществляется в следующем порядке:

7.16.1. ПДн на бумажных носителях уничтожаются путем использования шредеры (уничтожители документов), установленного в офисе Оператора.

7.16.2. ПДн, размещенные в памяти ПЭВМ уничтожаются путем удаления её из памяти ПЭВМ.

7.16.3. ПДн, размещенные на флеш-карте, диске, ином носителе информации уничтожаются путем удаления файла с носителя, при необходимости путем нарушения работоспособности флеш-карты или CD-диска.

7.17. Офис, помещения Оператора, по окончании рабочего дня и отсутствия сотрудников в офисе помещениях, должны запираться, окна должны быть закрыты, должна быть включена сигнализация (при наличии).

7.18. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

7.19. Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИСПДн.

7.20. В обязанности администраторов ИСПДн входит управление учетными записями пользователей ИСПДн, поддержание штатной работы ИСПДн, обеспечение резервного копирования данных, а также установка и конфигурирование аппаратного и программного обеспечения ИСПДн, не связанного с обеспечением безопасности ПДн в ИСПДн. Также, в

обязанности администраторов ИСПДн входит обеспечение соответствия порядка обработки и обеспечения безопасности ПДн в ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемых к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленных федеральным законодательством.

7.21. В обязанности администраторов ИСПДн также входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации ИСПДн, учет и хранение машинных носителей ПДн, периодический аудит журналов безопасности и анализ защищенности ИСПДн, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

7.22. В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения, критичных для безопасности ПДн, полномочий у одного лица не рекомендуется совмещать роли пользователя ИСПДн и администратора ИСПДн в лице одного сотрудника.

7.23. Квалификационные требования и детальный перечень прав и обязанностей администраторов ИСПДн закрепляются в соответствующих должностных инструкциях.

7.24. Организация внутреннего контроля процесса обработки ПДн у Оператора осуществляется в целях изучения и оценки фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

7.25. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

7.25.1. Обеспечение соблюдения сотрудниками Оператора требований настоящего Положения и нормативно-правовых актов, регулирующих сферу ПДн.

7.25.2. Оценка компетентности персонала, задействованного в обработке ПДн.

7.25.3. Обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн.

7.25.4. Выявление нарушений установленного порядка обработки ПДн и своевременное предотвращение негативных последствий таких нарушений.

7.25.5. Принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн.

7.25.6. Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий

7.25.7. Осуществление внутреннего контроля за исполнением рекомендаций и указаний по устранению нарушений.

7.26. Результаты контрольных мероприятий оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн, по модернизации технических средств ИСПДн и средств защиты ПДн, по обучению и повышению компетентности персонала, задействованного в обработке ПДн.

8. Ответственность за нарушение настоящего положения

8.1. Сотрудники Оператора несут ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

8.2. Сотрудники Оператора несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

8.3. Сотрудник Оператора может быть привлечен к ответственности в случаях:

8.3.1. Умышленного или неосторожного раскрытия ПДн

8.3.2. Утраты материальных носителей ПДн;

8.3.3. Нарушения требований настоящего Положения и других нормативных документов Оператора в части вопросов доступа и работы с ПДн

8.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Оператору, его сотрудникам, клиентам и контрагентам материального или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Wise Technologies
SIMPLE OUTSIDE, WISE INSIDE

APPROVED BY
Director — (position)
Zolotarsky Yuri — (print full name)
(personal signature)
Order No. 17 dated 12 Aug 19

Regulation on the Processing and Protection of Personal Data

1. General Provisions

1.1. This Regulation has been developed in accordance with the personal data protection legislation of the Republic of Belarus (hereinafter referred to as PD).

1.2. For the purposes of this Regulation, the following terms shall be used:

personal data (PD) –basic and additional personal data of physical person or any data that allows determine this individual (PD subject);

information system owner – an informational relations subject who possesses ownership rights, user license and rights of dispose of software and hardware means, information resources, systems and networks within and under the procedure determined by the owner in accordance with the legislation of the Republic of Belarus (hereinafter referred to as ISO);

PD processing – any action (operation) or a number of actions (operations) performed with or without automation tools, including collection, recording, systematization, accumulation, storage, refinement (update, modification), extraction, use, transfer (dissemination, provision, access), depersonalization, blocking, deletion, destruction of PD;

automated processing of PD – processing of PD by means of computer technology;

dissemination of PD – actions aimed at disclosure of PD to an indefinite range of persons;

provision of PD – actions aimed at disclosing PD to a certain person or a certain range of persons;

blocking of PD – suspension of processing of PD (except for the cases when the processing is required for the PD refinement);

destruction of PD – actions that make it impossible to restore PD content in the PDIS and/or that result in destruction of tangible media of PD;

depersonalization of PD – actions that make it impossible to determine the attachment of PD to a certain PD subject without the use of additional information;

personal data information system (PDIS) – a set of PD contained in databases and information technologies and hardware that ensure their processing;

1.3. This Regulation determines the procedure and terms for processing of PD in Wise Technologies LLC (hereinafter referred to as the ISO), including the PD transmission procedure to third parties, special aspects of automated and non-automated processing of PD, arrangements for the access to PD, protection system of PD, arrangement procedure for the internal control system and liability for breaches during PD processing, other issues.

1.4. This Regulation shall apply all processes of collection, systematization, accumulation, storage, refinement, use, dissemination (including transfer), depersonalization, blocking, deletion of PD with or without the use of automation tools.

1.5. This Regulation shall come into effect upon approval by the Head of the ISO and shall be effective for an unlimited period of time until replacing with a new Regulation.

1.6. All amendments to this Regulation shall be made by orders.

1.7. Responsible parties of the ISO shall be familiar with this Regulation.

2. Purposes and objectives of PD processing

2.1. The processing of PD shall be limited by achievement of certain predetermined and legal purposes. The processing of PD which is incompatible with the PD collection purposes shall not be allowed.

2.2. Consolidation of data bases containing PD being processed for purposes incompatible to each other shall not be allowed.

2.3. Only the PD that meet purposes of their processing shall be subject of processing.

2.4. The content and volume of the processed PD shall meet stated purposes of processing. The processed PD shall not be excessive in relation to the stated purposes of processing.

2.5. The processing of PD of the ISO's employees can be performed only for the purposes of compliance with laws and other statutes and regulations, assistance in employment, training and career development of workers, employees' personal security support, control for the quantity and quality of performed works and for the safekeeping of property of the ISO.

2.6. The major purpose of the PD processing is the performance of contractual commitments.

3. Personal data processed in the PDIS

3.1. The PD of the following subjects of PD shall be processed in the PDIS:

3.1.1. employees of the ISO;

3.1.2. customers (ISO's service consumers);

3.1.3. contractors of the ISO;

3.1.4. employees of the right holder (developer) of the ISO's software, performing operational and service support;

3.2. This list shall be subject to review as required.

3.3. In accordance with the Law of the Republic of Belarus N 418-3 (amended 09.01.2019) dated 21.07.2008 "On Population register" (including, but non limited) the personal data of PD subjects shall include: full name; gender; digital photo.

3.4. Besides the specified personal data the ISO shall be also entitled to process the following information, received from the PD subject by means of the ISO's software: start and completion time/date; time/date of photos; status of GPS sensors; status of configuration of location sensing via network; status of the Internet connection; the list of the software installed on the PD subject's device for the verification of availability of the software for the geolocation variation and access to the super-user rights; information on receipt of a device within the period of work performance in wiserep; information of time and time-zones settings; logging of actions in WiseRep and of battery status.

4. Access to PD

4.1. Employees of the ISO constantly working with PD by virtue of the performed duties shall have an access to PD for the period of performance by them of the corresponding duties.

4.2. The ISO has established the authorization procedure for obtaining an access to PD. The ISO's employees shall be provided with an access to work with PD exclusively within the limits and the scope necessary for the performance of their official duties.

4.3. With regards to business needs upon the Head's agreement the ISO's employee can get a temporary or a one-time permit for work with PD.

4.4. The access to PD of third parties not being the ISO's employees without the subject's consent shall be prohibited, except as the access of employees of executive authorities exercised as a part of activity for control and supervision over the legislation performance, implementation of functions and powers of the corresponding government authorities. The information upon the request or demand of the government authority shall be provided with knowledge of the ISO's Head.

4.5. The access of the Operator's employee to PD shall be terminated from the date of employment termination or the change date of the employee's official duties and/or exclusion of the employee from the list of employees having access to PD. In case of dismissal all media containing PD being in the possession of a worker within his work in accordance with official duties, shall be transferred to the corresponding officer.

5. Major requirements towards the PD protection

5.1. When processing PD in the information system one shall provide:

a) measures aimed at prevention of unauthorized access to personal data and/or their transfer to the parties not authorized for an access to such information;

b) timely detection of facts of unauthorized access to PD;

c) non-admission of any impact on hardware of automated processing of PD that may result in faulty functioning;

d) possibility of an immediate restoration of PD having been modified or destroyed as a result of an unauthorized access;

e) permanent control over the PD protection level provision.

5.2. The ISO shall take all necessary legal, arrangement, technical and other measures for ensuring of the PD safety.

5.3. The ISO shall use hardware for the PD processing and protection.

5.4. All the parties having been allowed to work with PD as well as associated with the operation and technical support of the PDIS must become familiar with the requirements of this Regulation.

5.5. Employees shall immediately inform the corresponding officer of the Operator about the loss or lack of media with the information being PD, as well as about the reasons and conditions of a PD probable leakage. Should any of the third parties make attempt to receive from an employee the PD processed by the ISO, the employee shall immediately notify hereof the corresponding officer of the ISO.

6. PD processing consent

6.1. The subject of PD shall make a decision on provision of its PD and shall consent to their processing freely, in its interest and, expressing its will. Consent to the PD processing shall be in writing. Consent to the PD processing shall be given by the subject of PD in any form that allows to reliably ascertain the respective text document is signed by the PD subject with the communication tools and othet technical means, software applications, informational systems or networks.

6.2. A written consent to the PD processing shall be received by the ISO's employee or by the ISO's contractor upon the ISO's instruction.

7. PD processing and protection procedure

7.1. The guarantee of confidentiality of PD processed by the ISO shall be an obligatory requirement for all parties having become familiar with them.

7.2. The ISO's employees performing the documents execution shall receive the PD subjects' consent to processing in prescribed cases.

7.3. The ISO's employee shall be liable in accordance with Section 8 of this Regulation in case of violation of the established PD processing order.

7.4. Personal data of the subjects in hard copies processed by the ISO shall be filed in departments (employees) having an access to processing of the corresponding PD. The right of access of employees of the non-automated PDIS shall be determined by the order of the Manager. The PD media shall not be left unattended. When leaving their workplace the employees performing the PD processing must take the media away into a safety locker, a locked filing cabinet or prevent from an unauthorized access to the media in any other way. In case of the PD loss or damage they shall be restored wherever possible.

7.5. Places of storage of documents containing PD:

7.5.1. PD of the ISOr's customers (contracts, statements, agreements, enquiry, passport copies, other similar documents containing PD of the ISO's customers, information media (flash-cards, CDs etc.) shall be kept in the main and auxiliary offices of the ISO, placed on shelves and locked. The person responsible for the control shall be determined by the Head's order.

7.5.2. PD of the ISO's employees - documents, information media (flash-cards, CDs etc.) shall be kept in a safety locker of the company and locked. The person responsible for the control is the ISO's Manager.

7.6. The documents shall be issued for acquaintance to the parties having been admitted to the corresponding information for the purpose of performance of their official duties for not more than one business day.

7.7. When working with the software of the ISO's automated system implementing functions of review and editing PD one shall be prohibited to present display forms containing such data to the parties not having the corresponding access.

7.8. In case PD are received by the ISO's employee that in accordance with its official duties receives PD from a customer, employee of another party the PD validation check shall be necessarily performed. PD received by the ISO shall be put into the information system by the employees having an access to the corresponding PD. Employees performing the input of information shall be liable for the authenticity and completeness of the put in information.

7.9. In case of the non-automatic processing of PD in hard copies:

7.9.1. documentation on a single paper medium of PD processing purposes of that are knowingly incompatible is prohibited;

7.9.2. PD shall be isolated form another information, particularly by their documentation on separate paper media, in special sections or in the margins of forms (template sheets);

7.10. The following conditions shall be met when using document templates the information character of which presupposes or allows the inclusion of PD to them (hereinafter referred to as templates):

7.10.1. The template of related to it documents (its execution instruction, cards, registers and logs) shall contain the information about the purpose of the non-automation PD processing, name and address of the ISO, full name and address of the PD subject, list of actions with PD to be performed during their processing, general description of processing methods of PD used by the ISO;

7.10.2. The template shall provide a box where the PD subject can mark its consent to a non-automated PD processing, if a written consent for the PD processing is required;

7.10.3. The template shall be drawn up so that each subject of PD contained in a document be able to familiarize with its PD contained in a document with no violation of rights and legal interests of other subjects of PD;

7.10.4. The template shall exclude the combination of boxes aimed for input of PD the processing purposes of which are knowingly incompatible.

7.11. The storage of PD shall be carried out in the form that allows to determine the PD subject, for a period not exceeding the one required by the PD processing purposes, in case the PD storage period is not set out by the federal law, contract, the party, beneficiary or guarantor of which is the PD subject.

7.12. PD deletion, blocking and refinement cases:

7.13. Deletion or depersonalization of a part of personal data, in case it is allowed by a material medium, can be carried out with a method excluding the further processing of these personal data with possibility to process other data documented on the material media (deletion, defacement).

7.14. Refinement of PD during its non-automated processing shall be carried out by updating or change of data on a material media, and in case it is not allowed by technical features of the material media - either by documentation of data about the made changes on the same material media or by production of a new material media with the refined PD.

7.15. Destruction of media containing PD shall be performed in the following order:

7.15.1. PD in paper media shall be destructed using shredding machines (document destroyers) installed in the ISO's office.

7.15.2. PD stored in the PC memory by deleting them from the PC memory.

7.15.3. PD stored on a flash-card, CD, other media shall be destroyed by deleting a file from the media, by failing of performance of the flash-card or CD if required.

7.16. The ISO's office, premises shall be locked upon the end of a business day and absence of employees there, windows shall be closed, the signaling system shall be activated (if available).

7.17. Network equipment, server machines should be placed in places not available for the third parties (in special premises, cabinets, boxes).

7.18. Indoor cleaning and the PDIS hardware maintenance shall be performed under control of the parties responsible for these premises and hardware in compliance with measures excluding the unauthorized access to PD, information media, software and hardware of processing, transfer and protection of information by the PDIS.

7.19. Official duties of the PDIS administrators involve management of the PDIS users accounts, maintenance of the PDIS normal operation, provision of data backing up, as well as installation and setup the PDIS' hardware and software not related with the provision of the PD safety in the PDIS. Official duties of the PDIS administrators also involve provision of compliance of the processing procedure and of the PD safety provision in the PDIS with the requirements of confidentiality, consistency and availability of PD, that are applicable to the specific PDIS, and with general requirements of the PD safety set out by the legislation.

7.20. Official duties of the PDIS administrators also involve installation, setup and administration the PDIS' hardware and software, accounting and storage of the PD computing media, periodic audit of security logs and analysis of the PDIS security level, as well as participation in internal investigations of violation of the set out order of the PD processing and security provision.

7.21. For the purposes of distribution of authorities, performance of mutual control and non-admission of concentration of a one-person authority, critical for the PD safety, one is not recommended the role of the PDIS users and the role of the PDIS administrator being combined by a single person.

7.22. Qualification requirements and a detailed list of rights and obligations of the PDIS administrators shall be captured in the corresponding job descriptions.

7.23. Arrangement of the internal control of the PD processing by the ISO shall be performed for the purposes of investigation and assessment of the actual safety condition of PD, timely response of the set out order of their processing, as well as for the purposes of improvement of this order and provision on compliance with it.

7.24. Measures for the internal control of the PD processing and safety provision shall be aimed for solving of the following issues:

7.24.1. Provision of compliance of the ISO's employees with the requirements of this Regulation and regulatory legal act governing the sphere of personal data.

7.24.2. Competence of a staff involved in the PD processing.

7.24.3. Provision of working capacity and efficiency of the PDIS hardware and software and the PD protection means, their compliance with the requirements of the authorized executive bodies on issues of the PD safety.

7.24.4. Detection of violations of the set out order of the PD processing and of a timely prevention of negative subsequences of such violations.

7.24.5. Taking corrective measures aimed at elimination of the detected violations both in the process of the PD processing and in the operation of the PDIS hardware and software.

7.24.6. Development of recommendations on improvement of the PD processing and safety provision order upon the results of supervisory measures

7.24.7. Internal monitoring of performance of recommendations and instructions on elimination of violations.

7.25. Results of the supervisory measures shall be documented as statements and shall serve the basis for the development of recommendations on improvement of processing of PD and safety provision order, on modernization of the PDIS hardware and of the PD means of protection, on training and competence improvement of the staff involved in the PD processing.

8. Liability for the breach of this Regulation

8.1. The ISO's employees shall be liable for the non-provision of the PD confidentiality and failure to respect the rights and freedoms of the PD subjects in relation to their PD, including the rights for their privacy, personal and family secret protection.

8.2. The Operator's employees shall be personally liable for the non-compliance with the requirements for the PD processing and safety provision established by this Regulation in accordance with the legislation of the Republic of Belarus.

8.3. The Operator's employee can be held strictly liable in cases of:

8.3.1. Intentional and negligent disclosure of PD

8.3.2. Loss of material media with PD;

8.3.3. Violation of requirements of this Regulation and of other ISO's instruments to the extent of access and operation with PD

8.4. In case of violation of the set out order of the PD processing and safety provision, unauthorized access to PD, disclosure of PD and causing material and other damage to the ISO, its employees, customers and contractor the parties in fault shall bear the public, criminal, administrative, disciplinary and other liability contemplated by the legislation of the Republic of Belarus.