

ПОЛОЖЕНИЕ **об организации обработки и защите персональных данных**

1. Общие положения

1.1. Настоящее Положение является основным внутренним документом S.A. „IUGINTERTRANS” в области обработки и защиты персональных данных и обязательно для директора, работников головного офиса, всех подразделений, практикантов и иных лиц, допущенных к персональным данным предприятия.

1.2. Оператором персональных данных является Societatea pe Acțiuni „IUGINTERTRANS”, фискальный код 1003610000214, место нахождения: MD-7401, Республика Молдова, г. Тараклия, ул. Вокзальная, 28, телефон 029421010.

1.3. Положение распространяется на обработку на бумажных носителях и в электронной форме, включая личные дела и архив, программу «1С», рабочие компьютеры и телефоны, корпоративную электронную почту, центральный сервер, локальные серверы видеонаблюдения, спутниковый контроль служебных автомобилей, цифровые тахографы, журналы посетителей и корпоративные документы.

1.4. Положение действует в головном офисе и во всех производственных, складских и транспортных подразделениях предприятия в городах Тараклия, Комрат, Анений Ной, Дрокия и Яловень.

1.5. Для целей настоящего Положения персональные данные означают любые сведения о прямо или косвенно определённом либо определяемом физическом лице; обработка означает любое действие или совокупность действий с такими сведениями, включая получение, запись, систематизацию, хранение, изменение, просмотр, использование, передачу, ограничение, удаление и уничтожение.

1.6. Медицинские сведения относятся к специальным категориям персональных данных и обрабатываются только при наличии предусмотренного законом основания и усиленных мер защиты. Сведения о судимости и правонарушениях обрабатываются только в случаях и пределах, прямо допускаемых законом.

1.7. Если специальный внутренний документ предприятия устанавливает более строгие правила для отдельного процесса, применяются такие более строгие правила.

2. Принципы обработки

2.1. Каждая операция с персональными данными должна иметь конкретную законную цель и правовое основание, быть добросовестной и понятной физическому лицу.

2.2. Запрещается собирать персональные данные на случай возможной будущей необходимости либо использовать их для цели, несовместимой с первоначально объявленной целью.

2.3. Состав данных ограничивается сведениями, объективно необходимыми для соответствующей цели. Получение копии документа допускается только тогда, когда закон либо документированная служебная необходимость требуют сохранения копии, а одной визуальной проверки или записи необходимых реквизитов недостаточно.

2.4. Работники, ведущие соответствующий учёт, принимают разумные меры для исправления неточных и обновления устаревших данных.

2.5. Данные хранятся не дольше срока, установленного законом, номенклатурой дел, договором либо документированным решением предприятия исходя из цели и риска. По истечении срока данные уничтожаются, удаляются или необратимо обезличиваются.

2.6. Предприятие обеспечивает конфиденциальность, целостность и доступность данных, защиту от неправомерного доступа, изменения, разглашения, утраты, уничтожения и повреждения.

2.7. Соблюдение настоящих принципов должно подтверждаться документами: реестром операций, уведомлениями, перечнями доступа, договорами, журналами, оценками рисков, актами уничтожения, материалами обучения и проверки.

3. Правовые основания обработки

3.1. До начала новой операции ответственное за процесс лицо определяет и отражает в реестре операций цель, категории данных, круг физических лиц, правовое основание, получателей, срок хранения и меры защиты.

3.2. Предприятие обрабатывает данные, когда это необходимо для заключения или исполнения договора с физическим лицом, выполнения предусмотренной законом обязанности, защиты жизненно важных интересов, исполнения задачи в общественном интересе либо осуществления документированного законного интереса предприятия или другого лица, если права и свободы физического лица не имеют преимущественной силы.

3.3. Согласие используется только тогда, когда отсутствует более подходящее правовое основание. Согласие должно быть добровольным, конкретным, осознанным и однозначным, подтверждаться активным действием и допускать отзыв столь же простым способом, каким оно было предоставлено.

3.4. В трудовых отношениях согласие работника не используется как формальное универсальное основание для обработки, необходимой работодателю по закону или трудовому договору. Отказ от необязательной обработки не должен влечь неблагоприятных последствий для работника.

3.5. При обработке на основании законного интереса до начала операции составляется письменная оценка, в которой определяются интерес предприятия, необходимость обработки, возможное воздействие на физическое лицо, его разумные ожидания и защитные меры. Это правило применяется, в частности, к видеонаблюдению и контролю местоположения транспорта.

3.6. Медицинские сведения работников обрабатываются в объёме, необходимом для исполнения обязанностей в сфере трудовых отношений, охраны здоровья и безопасности труда, социального страхования, оценки пригодности к работе и установления либо защиты правовых требований.

4. Физические лица, данные которых обрабатываются

4. Предприятие обрабатывает персональные данные следующих основных категорий физических лиц:

4.1. работники, бывшие работники, кандидаты на трудоустройство, практиканты и учащиеся;

4.2. акционеры, члены совета общества, ревизионной комиссии, директор и представители органов управления;

4.3. посетители, водители и иные лица, находящиеся на территории объектов или попадающие в поле видеокамер;

4.4. индивидуальные предприниматели, руководители, учредители, представители и контактные работники покупателей, поставщиков, перевозчиков и других контрагентов;

4.5. лица, участвующие в претензионных, судебных, исполнительных, страховых, дисциплинарных и иных производствах;

4.6. иные физические лица, данные которых законно поступают предприятию при осуществлении производства, торговли, перевозок, ремонта транспорта, корпоративного управления и исполнения обязательных требований.

5. Основные процессы и цели обработки

5.1. Подбор работников, заключение, исполнение, изменение и прекращение трудовых договоров; ведение личных дел, учёт рабочего времени, отпусков, отсутствий, квалификации, дисциплины, материальной ответственности, охраны здоровья и безопасности труда.

- 5.2. Начисление и выплата заработной платы, премий, надбавок, пособий и компенсаций; налоговый, бухгалтерский и социальный учёт; банковские перечисления; удержания по исполнительным документам; командировки, займы и материальная помощь.
- 5.3. Обязательные медицинские осмотры, подтверждение пригодности к работе, учёт временной нетрудоспособности, несчастных случаев и профессиональных заболеваний.
- 5.4. Организация производства хлебобулочной продукции и замороженных полуфабрикатов, складского хранения, пропускного режима, охраны имущества, безопасности работников и расследования конкретных происшествий.
- 5.5. Организация автомобильных перевозок, планирование маршрутов, контроль эксплуатации, пробега и расхода топлива, соблюдение режима управления и отдыха водителей, оформление перевозочных, таможенных, страховых и разрешительных документов.
- 5.6. Заключение и исполнение договоров, доставка продукции, расчёты, бухгалтерский и налоговый учёт, претензионная работа, взыскание задолженности, участие в судебных и исполнительных производствах.
- 5.7. Корпоративное управление, взаимодействие с организацией, ведущей реестр акционеров, проведение общих собраний, учёт доверенностей, голосования и выплаты дивидендов.
- 5.8. Эксплуатация рабочих компьютеров, служебных телефонов, корпоративной электронной почты, программы «1С», сайта, серверов и иных средств, необходимых для деятельности предприятия.
- 5.9. Исполнение официальных запросов судов, полиции, прокуратуры, государственных органов, Инспекции труда, судебных исполнителей и иных уполномоченных законом получателей.

6. Получение данных и информирование физических лиц

- 6.1. Персональные данные, как правило, получают непосредственно у физического лица. Получение из другого источника допускается при наличии правового основания и фиксируется в реестре операций либо материалах соответствующего дела.
- 6.2. До получения данных или в иной установленный законом срок физическому лицу предоставляется понятное уведомление, содержащее сведения о предприятии, целях, основаниях, категориях данных, получателях, международной передаче, сроках хранения, правах и способах обращения.
- 6.3. Уведомление предоставляется отдельно от трудового договора, заявления, анкеты или согласия либо выделяется в них таким образом, чтобы его можно было легко заметить и прочитать.
- 6.4. При изменении цели, состава получателей, срока хранения или других существенных условий обработки уведомление обновляется до начала изменённой обработки.
- 6.5. Специалист по кадрам организует ознакомление работников и кандидатов; менеджеры подразделений обеспечивают доступ к уведомлениям о видеонаблюдении и контроле транспорта; работники, заключающие договоры, обеспечивают информирование соответствующих представителей контрагентов.

7. Доступ работников предприятия

- 7.1. Доступ предоставляется только конкретному работнику, которому он необходим для выполнения должностных обязанностей, в объёме, соответствующем его задачам. Доступ по должности не означает право свободно просматривать, копировать или использовать все доступные сведения.
- 7.2. Перечень разрешённых категорий данных и действий утверждается отдельным документом. Передача сведений внутри предприятия по устному запросу допускается только после проверки служебной необходимости и личности запрашивающего работника.

7.3. Каждый пользователь электронной системы использует личную учётную запись и пароль. Передача пароля, совместное использование учётной записи и оставление открытой рабочей сессии без присмотра запрещены.

7.4. Специалист, обслуживающий компьютеры, вправе получать технический доступ только в объёме, необходимом для обслуживания, устранения неисправности, обеспечения безопасности или восстановления данных. Доступ к содержанию документов и переписки допускается при объективной технической необходимости, с разрешения директора и документальной фиксацией.

7.5. Специалист, обслуживающий камеры видеонаблюдения получает физический доступ к центральному серверу и локальным серверам видеонаблюдения и выполняет копирование либо извлечение записей только с разрешения директора и с регистрацией совершённого действия.

7.6. Охранники при регистрации посетителя только визуально проверяют удостоверение личности, не записывают его серию и номер, не снимают копию и не удерживают документ.

7.7. При переводе, изменении обязанностей, длительном отсутствии или прекращении трудовых отношений руководитель немедленно сообщает специалисту, обслуживающему компьютеры, и владельцу соответствующего бумажного учёта о необходимости изменить или прекратить доступ.

7.8. Все работники, допущенные к персональным данным, подписывают обязательство о конфиденциальности и проходят первоначальное, а затем периодическое обучение.

8. Хранение бумажных и электронных данных

8.1. Личные дела работников ведутся централизованно специалистом по кадрам на бумажном носителе. Они хранятся в запираемом кабинете; дела уволенных работников передаются в отдельное архивное помещение, ключ от которого находится у специалиста по кадрам.

8.2. На компьютере специалиста по кадрам допускается хранить только те электронные сведения и документы, которые необходимы для кадрового учёта. Доступ к ним предоставляется индивидуально и защищается паролем.

8.3. Медицинские книжки и графики осмотров могут храниться у менеджеров подразделений в запираемых местах. Обычный доступ имеют менеджер соответствующего подразделения и специалист по кадрам в пределах служебной необходимости.

8.4. Документы о несчастных случаях хранятся отдельно от обычных личных дел; их параллельное хранение у специалиста по кадрам и менеджера подразделения допускается только в необходимом составе.

8.5. Юрисконсульт хранит материалы договорных, претензионных, судебных и исполнительных дел в запираемом кабинете, на защищённом рабочем компьютере и в корпоративной электронной почте. Доступ других работников предоставляется только по конкретной служебной необходимости.

8.6. Корпоративные документы акционеров и органов общества хранятся в запираемом кабинете; доступ имеет секретарь совета общества, являющийся специалистом по кадрам, а также директор в пределах полномочий.

8.7. Хранение рабочих документов на личных компьютерах, личных телефонах, личной электронной почте и неразрешённых переносных накопителях запрещается.

8.8. Электронные данные защищаются антивирусными программами, обновлениями, индивидуальными учётными записями, разграничением доступа и резервным копированием. Возможность восстановления резервных копий проверяется периодически.

8.9. Перед ремонтом, передачей, продажей или списанием компьютера либо накопителя сведения безопасно удаляются. Если устройство передаётся внешнему ремонтнику без возможности предварительного удаления, носитель извлекается либо заключается письменное условие о конфиденциальности и запрете доступа.

9. Передача внутри предприятия и внешним получателям

9.1. До передачи проверяются личность и полномочия получателя, правовое основание, цель, необходимый объём, безопасный канал и необходимость регистрации передачи.

9.2. Предприятие может передавать данные обслуживающим банкам, Государственной налоговой службе, Национальной кассе социального страхования, Национальной компании медицинского страхования, судебным исполнителям, судам, полиции, прокуратуре, Инспекции труда, медицинским учреждениям, страховым и аудиторским организациям и иным лицам при наличии законного основания.

9.3. Ответ на официальный запрос готовится только в пределах компетенции запрашивающего органа и предмета запроса. Если запрос чрезмерен либо его основание неясно, юрисконсульт запрашивает уточнение или предлагает предоставить меньший объём.

9.4. Передача через государственные электронные системы и банковские системы осуществляется с использованием предоставленных средств защиты. Персональные данные по электронной почте направляются только с корпоративного адреса, после проверки адресата и вложений.

9.5. Лицам, которые обрабатывают данные по поручению предприятия, доступ предоставляется только после заключения письменного договора или дополнения, отвечающего статье 28 Закона № 195/2024. Не каждый самостоятельный получатель данных является лицом, действующим по поручению предприятия; его статус определяется по фактической роли.

9.6. Юрисконсульт совместно с работником, ответственным за договор, проверяет гарантии лица, обслуживающего программу «1С», спутниковый контроль, корпоративную почту и сайт, медицинские осмотры, аудит, консультирование и ремонт компьютеров.

9.7. Передача видеозаписи, кадрового документа, медицинского сведения или копии удостоверения личности регистрируется, если иное документирование однозначно не обеспечено государственной системой или материалами дела.

10. Международные передачи

10.1. Передача данных водителей иностранным заказчикам, получателям грузов, транспортным посредникам, таможенным представителям, портам, пограничным органам и страховым организациям допускается только в объёме, необходимом для перевозки, исполнения договора, таможенных и пограничных процедур, страхования и выполнения требований закона.

10.2. До регулярной передачи в другое государство юрисконсульт определяет применимое основание и гарантию в соответствии со статьями 44–50 Закона № 195/2024 .

10.3. Передача фамилии и имени водителя, сведений водительского удостоверения и регистрационных данных автомобиля по корпоративной электронной почте в государства Европы и стран Европейского союза и Турцию производится только подтверждённому получателю; документ целиком не направляется, если достаточно отдельных сведений.

10.4. Если сервис программы «1С», спутникового контроля, корпоративной почты или сайта хранит данные за пределами Республики Молдова, такая операция рассматривается как международная передача и допускается после её правовой оценки и документирования.

11. Видеонаблюдение

11.1. Видеонаблюдение применяется для безопасности людей, защиты имущества, контроля доступа, предотвращения и расследования конкретных происшествий и не используется для постоянной оценки производительности работников.

11.2. Камеры могут охватывать входы, производственные цеха, склады, коридоры, офисные зоны, кассы, места погрузки, стоянки, ремонтную базу, автозаправочную станцию и внешнюю территорию. Установка в раздевалках, комнатах отдыха, столовых, санитарных и иных бытовых помещениях запрещается.

11.3. Записывается только изображение без звука. У каждого входа в контролируемую зону размещается предупреждающая табличка и обеспечивается доступ к подробному уведомлению.

11.4. Директор имеет доступ ко всем камерам; менеджер подразделения — только к изображению и записям своего подразделения. Обычный срок хранения составляет не более 30 календарных дней.

11.5. Дальнейшее хранение выбранной записи допускается только для документированной цели, в частности расследования происшествия, защиты прав предприятия либо исполнения законного требования, с ограничением доступа и последующим уничтожением.

11.6. Подробные правила, карта зон, журнал копирования и оценка воздействия утверждаются отдельными документами.

12. Спутниковый контроль транспорта и цифровые тахографы

12.1. Сведения о местоположении, маршрутах, остановках, скорости, пробеге и расходе топлива используются для организации перевозок, безопасности, контроля эксплуатации транспорта, выполнения договоров и защиты имущества.

12.2. Сведения цифровых тахографов используются для соблюдения требований о времени управления, перерывах и отдыхе водителей, организации перевозок и подтверждения исполнения обязанностей предприятия.

12.3. Доступ к текущему местоположению и истории поездок, а также сведениям тахографов имеют менеджер транспортного отдела, мастер-механик и логисты в пределах своих задач. Использование сведений в личных целях и непрерывное наблюдение без служебной необходимости запрещаются.

12.4. Водитель до начала использования автомобиля получает отдельное уведомление о составе данных, целях, основаниях, доступе, получателях, сроке хранения и правах.

12.5. Срок хранения определяется отдельным положением после документированной оценки необходимости, требований транспортного законодательства, сроков предъявления требований и технических возможностей системы. Бессрочное хранение запрещается.

13. Служебные телефоны, электронная почта и сайт

13.1. Служебные телефоны и номера закрепляются за работниками в отдельном перечне. Получаемая от оператора связи детализация звонков используется для учёта расходов, безопасности и проверки обоснованной служебной необходимости; запись содержания разговоров не производится.

13.2. Корпоративная электронная почта предназначена для служебной переписки. Проверка её содержания допускается только при законной и документированной цели, соразмерном объёме, предварительном информировании работника и соблюдении отдельного порядка.

13.3. После прекращения трудовых отношений доступ работника к почтовому ящику и служебному телефону прекращается; служебная переписка сохраняется или передаётся назначенному работнику только в необходимом объёме, а личные сообщения, если они допустимо находились в ящике, не используются.

13.4. Рабочие группы в программах обмена сообщениями создаются только для определённой цели. Включение личного номера работника допускается после информирования; уволенный или переведённый работник незамедлительно удаляется из группы, если участие более не требуется.

13.5. Официальный сайт предприятия не должен собирать данные через формы, средства анализа действий посетителя или иные технологии до определения цели, основания, срока хранения и размещения необходимого уведомления.

14. Права физических лиц

14.1. Физическое лицо вправе получить информацию об обработке, доступ к своим данным и их копию, потребовать исправления, удаления или ограничения обработки в установленных законом случаях, получить переносимые данные, возразить против обработки и потребовать вмешательства человека при решении, основанном исключительно на автоматической обработке.

14.2. Обращение может быть подано письменно по месту нахождения предприятия, через корпоративную электронную почту, указанную в уведомлении, либо лично специалисту по кадрам или юрисконсульту. Получивший обращение работник в тот же рабочий день передаёт его юрисконсульту для регистрации.

14.3. До предоставления данных личность заявителя проверяется соразмерным способом. Запрашивается только дополнительная информация, действительно необходимая для подтверждения личности.

14.4. Ответ предоставляется без неоправданной задержки и не позднее одного месяца со дня получения обращения. При сложности или большом количестве обращений срок может быть продлён не более чем на два месяца с уведомлением заявителя в течение первого месяца и указанием причин.

14.5. Действия по обращению, как правило, бесплатны. При явно необоснованных или чрезмерных повторных обращениях предприятие вправе применить предусмотренную законом плату либо мотивированно отказать, доказав основания решения.

14.6. Отказ, частичное удовлетворение и невозможность совершить требуемое действие оформляются мотивированно с разъяснением права обратиться в Национальный центр по защите персональных данных Республики Молдова и в суд.

15. Нарушения безопасности персональных данных

15.1. Нарушением безопасности является, в частности, утрата документа или устройства, ошибочная отправка, неправомерный просмотр, разглашение, изменение, уничтожение, заражение вредоносной программой, недоступность данных либо получение доступа посторонним лицом.

15.2. Работник немедленно сообщает о предполагаемом нарушении непосредственному руководителю и юрисконсульту, сохраняет документы и электронные следы, не скрывает происшествие и не предпринимает несогласованных действий, способных уничтожить доказательства.

15.3. Юрисконсульт организует регистрацию и правовую оценку; специалист, обслуживающий компьютеры, принимает срочные технические меры; соответствующий менеджер обеспечивает сохранность документов и доступ к месту происшествия.

15.4. Каждое нарушение документируется с указанием обстоятельств, затронутых данных и лиц, последствий и принятых мер, включая случаи, когда уведомление государственного органа не требуется.

15.5. Если нарушение способно создать риск для прав и свобод физических лиц, предприятие уведомляет Национальный центр по защите персональных данных Республики Молдова без неоправданной задержки и, по возможности, не позднее семидесяти двух часов после того, как узнало о нарушении. При высоком риске затронутые лица информируются без неоправданной задержки, если закон не допускает исключение.

16. Оценка риска и защита при разработке процессов

16.1. При приобретении программы, установке камеры, изменении системы доступа, внедрении нового учёта, привлечении внешнего лица или существенном изменении существующего процесса работник-инициатор до заключения договора или запуска направляет юрисконсульту описание цели, данных, пользователей, получателей, места хранения и предполагаемых мер защиты.

16.2. По умолчанию в системе должны быть отключены ненужный сбор, избыточная видимость данных, общий доступ, бессрочное хранение и необязательная передача третьим лицам.

16.3. Если обработка способна создать высокий риск, до её начала проводится оценка воздействия. Для уже действующих систем такая оценка проводится при выявлении высокого риска, если ранее она не выполнялась.

16.4. Для видеонаблюдения во всех подразделениях и систематической обработки местоположения транспорта проводятся отдельные оценки воздействия. При неустранённом высоком остаточном риске до продолжения обработки проводится предварительная консультация с Национальным центром по защите персональных данных Республики Молдова.

17. Реестр операций и доказательства соблюдения

17.1. Предприятие ведёт единый письменный реестр операций обработки, поскольку численность работников составляет около восьмисот человек, а обработка имеет постоянный характер и включает медицинские сведения и процессы повышенного риска.

17.2. В реестре указываются сведения о предприятии; цели; категории физических лиц и данных; категории получателей; международные передачи и гарантии; предполагаемые сроки удаления; общее описание технических и организационных мер.

17.3. Работник, ответственный за конкретный процесс, уведомляет юрисконсульта об изменении процесса до изменения либо, если это невозможно, не позднее следующего рабочего дня.

17.4. Реестр проверяется не реже одного раза в год и предоставляется Национальному центру по защите персональных данных Республики Молдова по законному требованию.

18. Распределение обязанностей

18.1. Директор утверждает внутренние документы, определяет ресурсы, принимает решения по существенным рискам и контролирует исполнение.

18.2. Юрисконсульт координирует подготовку документов, реестр операций, рассмотрение обращений, договорные условия, международные передачи и правовую оценку нарушений. Такое поручение само по себе не означает назначения в смысле статьи 37 Закона № 195/2024.

18.3. Специалист по кадрам отвечает за централизованные личные дела, архив кадровых документов, уведомление работников и кандидатов, точность кадровых сведений, ограниченное внутреннее предоставление и учёт доступа к кадровым данным.

18.4. Главный бухгалтер организует права пользователей программы «1С», законность расчётных и обязательных передач, защиту расчётных документов и прекращение избыточного доступа.

18.5. Менеджеры подразделений и мастера производства отвечают за бумажные документы, медицинские книжки, графики и списки работников, уведомления о видеонаблюдении, доступ к камерам своего подразделения и своевременное сообщение о происшествиях.

18.6. Менеджер транспортного отдела, мастер-механик и логисты отвечают за соразмерное использование спутникового контроля, цифровых тахографов и документов водителей, а также за точность и минимальный объём международных передач.

18.7. Специалист, обслуживающий компьютеры, отвечает за техническое разграничение доступа, учётные записи, антивирусную защиту, обновления, резервное копирование, восстановление, безопасное удаление и техническое реагирование на нарушения.

18.8. Специалист, обслуживающий камеры видеонаблюдения обслуживает систему видеонаблюдения и получает доступ к серверам только в установленном порядке.

18.9. Каждый работник отвечает за соблюдение выданных ему указаний, конфиденциальность, безопасность документов и устройств, проверку адресата перед отправкой и немедленное сообщение о нарушении.

19. Контроль, обучение и ответственность

19.1. Работники, обрабатывающие персональные данные, проходят ознакомление до получения доступа; повторное информирование указанных работников проводится не реже одного раза в год и при существенном изменении правил или системы.

19.2. Соблюдение Положения проверяется по утверждённому плану, а также после существенного нарушения, изменения процесса либо получения требования государственного органа.

19.3. Нарушение Положения рассматривается с учётом вины, последствий и требований трудового законодательства и может повлечь дисциплинарную, материальную, гражданскую, административную или уголовную ответственность в предусмотренных законом случаях.

19.4. Сообщивший добросовестно о предполагаемом нарушении работник не может подвергаться неблагоприятным мерам только за такое сообщение.

20. Заключительные положения

20.1. Положение вступает в силу с **23 августа 2026 года**.

20.2. Положение пересматривается не реже одного раза в год, а также при изменении законодательства, структуры предприятия, целей, технологий, получателей, международных передач или выявлении недостаточности мер защиты.

20.3. Изменения утверждаются приказом директора и доводятся до затронутых работников до начала их применения.

20.4. Неотъемлемыми практическими средствами исполнения настоящего Положения являются специальные положения, уведомления, реестры, журналы, формы и оценки, утверждаемые предприятием последовательно.