ЧАСТНОЕ УЧРЕЖДЕНИЕ СТОЛИЧНЫЙ ЦЕНТР ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «РУНО»

(ЧУ СЦ ДПО «РУНО»)

ИНН 7709471098

ПРИКАЗ

«03» ноября 2026 г. № УМ_11_26/8

г. Москва

Об утверждении внутренних процедур

В целях исполнения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и организации обработки персональных данных в ЧУ СЦ ДПО «РУНО»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Регламент реагирования на инциденты в области персональных данных и Регламент хранения, прекращения обработки, уничтожения данных и управления доступом. Утвердить формы учета, приведенные во вкладке «Проверки и формы учета».

2. Назначить ответственным за организацию обработки персональных данных: контент-менеджер по производству образовательного продукта – Хлюпову Анастасию Александровну. Директор обеспечивает организационные условия исполнения обязанностей; ответственный подчиняется непосредственно исполнительному органу учреждения и действует в пределах статьи 22.1 Закона № 152-ФЗ.

3. Назначить Хлюпову А.А. ответственной за реагирование на инциденты в области персональных данных и техническим координатором. Возложить на нее регистрацию инцидентов, организацию ограничения последствий, взаимодействие с провайдерами, сбор материалов расследования, подготовку уведомлений Роскомнадзору и контроль сроков их направления. При её отсутствии замещающее лицо назначается отдельным распорядительным актом; до назначения координацию обеспечивает директор.

4. Подписание уведомлений Роскомнадзору осуществляет директор Шегай Л.В. либо лицо, действующее на основании надлежащим образом оформленных полномочий. Хлюпова А.А. обеспечивает подготовку и организацию направления уведомлений в установленные сроки; самостоятельное подписание и подача от имени учреждения допускаются при наличии необходимых полномочий. Обеспечить резервный способ направления на случай отсутствия основного исполнителя.

5. Руководителям подразделений определить владельцев процессов: заявки и CRM; обучение и личный кабинет; выдача документов и архив; бухгалтерский учет; кадровая обработка; реклама и рассылки. Для каждого процесса заполнить реестр обработки, определить права доступа и сроки по видам документов.

6. В течение 5 рабочих дней после подписания приказа заполнить служебные контакты и схему замещения, организовать ознакомление работников под подпись и ограниченный канал сообщений об инцидентах. Этот срок установлен учреждением, а не законом.

7. В течение 10 рабочих дней после подписания приказа провести проверку из вкладки «Проверки и формы учёта», представить директору результаты, перечень расхождений и план исправлений с исполнителями и датами. Этот срок является внутренним.

8. До завершения проверки не утверждать как проверенные факты соответствие настроек систем публичным документам, наличие всех рекламных согласий, локализацию всех баз и отсутствие трансграничной передачи. Публичные документы приводить в соответствие с подтвержденными процессами и применимыми требованиями.

9. Доступ подрядчиков к персональным данным предоставлять после проверки основания и договорных условий, в пределах согласованных задач; поручение обработки оформлять по части 3 статьи 6 Закона № 152-ФЗ.

10. Контроль исполнения настоящего приказа оставляю за собой.

Директор ЧУ СЦ ДПО «РУНО» Л.В. Шегай

С приказом и приложениями ознакомлены:

Должность: Контент-менеджер по производству образовательного продукта

ФИО: Хлюпова Анастасия Александровна

Подпись: _____

Дата: «03» ноября 2026 г.

ПРИЛОЖЕНИЕ
к приказу ЧУ СЦ ДПО «РУНО»
от «03» ноября 2026 г. № УМ_11_26/8

РЕГЛАМЕНТ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Область применения и основания

1.1. Регламент применяется к работникам и к взаимодействию с подрядчиками при обработке данных в Битрикс24, на сайте, в личном кабинете и учебной платформе, на инфраструктуре Selectel, в электронной почте, сервисах рассылок, формах, аналитике, бумажных документах и резервных копиях.

1.2. Основания: статьи 18.1, 19, 21 и 22.1 Закона № 152-ФЗ; порядок взаимодействия с РКН в рамках реестра инцидентов, утверждённый приказом Роскомнадзора от 14.11.2022 № 187; иные применимые обязательные акты. Оценка дополнительных обязанностей по взаимодействию с ГосСОПКА проводится отдельно по части 12 статьи 19 Закона № 152-ФЗ и применимому порядку ФСБ.

1.3. Сигналом считается подозрение на раскрытие данных, ошибочное письмо или доступ, потерю носителя, компрометацию учётной записи, публичную ссылку, выгрузку базы или сообщение провайдера. Сигнал регистрируется и проверяется даже без подтвержденной утечки.

1.4. Условие обязательного уведомления по части 3.1 статьи 21: установлен факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов. Не каждое техническое событие автоматически соответствует этому условию. Вывод и его фактическое обоснование фиксируются ответственным.

2. Обнаружение и первые действия

2.1. Любой работник немедленно сообщает об обнаруженном событии Хлюповой А.А. по закрытому рабочему каналу связи, а при ее недоступности — директору или назначенному заместителю. Используются служебные контактные данные из внутреннего справочника

учреждения; работник проверяет получение сообщения адресатом. Целевой срок внутреннего сообщения — не более 15 минут с обнаружения; этот срок установлен РУНО.

2.2. Указать время, систему, замеченные признаки, источник сообщения и свои действия. Не пересылать базу или документы в общий чат, личную почту, публичный облачный диск или внешний ИИ. Сведения об инциденте передавать только уполномоченным лицам в необходимом объёме.

2.3. Технический координатор без промедления ограничивает несанкционированный доступ: отзывает ссылки, сессии, токены и избыточные права, изолирует затронутый компонент, взаимодействует с провайдером. Выбор мер учитывает сохранность доказательств и доступность обучения; удаление всех журналов или переустановка системы без фиксации состояния не допускаются.

2.4. Сохранить исходные журналы, уведомления провайдера, параметры доступа и относящиеся к событию записи. Ограничить доступ к материалам расследования, вести учет их получения и изменений; при возможности фиксировать контрольные суммы копий.

3. Отсчет сроков и уведомления

3.1. Законные 24 и 72 часа отсчитываются с момента выявления инцидента оператором, РКН или иным заинтересованным лицом, а не с даты приказа о расследовании. Зафиксировать отдельно время события, обнаружения, получения сообщения и установления фактов. При расхождениях сохранять первичные сведения; не переносить отсчёт искусственно. Сроки исчисляются в часах, включая выходные и праздники.

3.2. В течение 24 часов направить первичное уведомление в РКН: сведения об инциденте; предполагаемые причины; предполагаемый вред правам субъектов; принятые меры; сведения об уполномоченном контактном лице. Заполнить действующую форму по приказу № 187, в том числе дату и время выявления, характеристики данных и количество записей в применимой части. Непроверенные обстоятельства обозначать как предварительные, не выдумывать значения.

3.3. В течение 72 часов с того же момента выявления направить дополнительное уведомление: результаты внутреннего расследования и сведения о лицах, действия которых стали причиной инцидента, при наличии. Включить предусмотренные формой причины, вред, дополнительные меры и реквизиты решения о расследовании. Не откладывать подачу

до завершения внешней экспертизы; неизвестные сведения обозначить, направить имеющиеся результаты и уточнения по применимому порядку.

3.4. Подача — через действующий сервис портала персональных данных РКН https://pd.rkn.gov.ru/ либо иным предусмотренным приказом № 187 способом. Уполномоченный отправитель сохраняет копию, время отправки, подтверждение приёма и реквизиты, необходимые для дополнительного уведомления. При техническом сбое фиксируется ошибка и применяется доступный законный резервный способ.

3.5. Ответственный контролирует входящие требования РКН и специальные сроки ответа по ним. Ожидание согласования внутри учреждения не приостанавливает обязательные сроки. Факт отсутствия обязанности уведомлять в конкретном случае фиксируется в журнале с обоснованием и пересматривается при новых обстоятельствах.

4. Расследование и завершение

4.1. Директор или уполномоченное лицо оформляет решение о расследовании, назначает состав и ответственного. Установить охваченные системы, категории лиц и данных, период доступа, источник, получателей, объём, возможные последствия и причины. Запросить у подрядчиков сведения и подтверждения мер по договорным каналам.

4.2. При неправомерной обработке применяются специальные сроки статьи 21: прекращение не позднее 3 рабочих дней со дня выявления; при невозможности обеспечить правомерность — уничтожение не позднее 10 рабочих дней. Эти сроки не заменяют уведомления в 24 и 72 часа.

4.3. Вопрос информирования пострадавших оценивается по обстоятельствам и применимым нормам. По предусмотренным статьей 21 обращениям и запросам сообщается об устранении нарушений или уничтожении соответствующим субъектам и РКН. Универсальную обязанность направлять всем уведомление в течение 24 часов настоящим Регламентом не устанавливать.

4.4. Итоговый акт включает факты, хронологию, оценку нарушения прав, причины, последствия, уведомления, принятые меры, подтверждение устранения и план предотвращения повторения. Закрытие фиксируется ответственным после проверки мер. Увольнение или назначение виновного не подменяет устранение причин.

4.5. Материалы хранятся с ограниченным доступом по установленной для соответствующих документов номенклатуре дел, с учетом требований регулятора, расследования и защиты прав. Конкретный срок и основание фиксируются в реестре, без автоматического бессрочного хранения всей затронутой базы.

5. Краткая схема

Сигнал → немедленное внутреннее сообщение и фиксация → ограничение доступа и сохранение доказательств → оценка условия части 3.1 статьи 21 → первичное уведомление РКН до 24 часов → дополнительное до 72 часов → устранение, акт и контроль мер.

ПРИЛОЖЕНИЕ
к приказу ЧУ СЦ ДПО «РУНО»
от «03» ноября 2026 г. № УМ_11_26/8

РЕГЛАМЕНТ ХРАНЕНИЯ, ПРЕКРАЩЕНИЯ ОБРАБОТКИ, УНИЧТОЖЕНИЯ ДАННЫХ И УПРАВЛЕНИЯ ДОСТУПОМ

1. Правила определения сроков

1.1. Срок определяется для конкретных цели, данных и документа. Основания: статьи 5, 6, 9, 15, 18.1, 19–21 Закона № 152-ФЗ, применимое образовательное, архивное, бухгалтерское и налоговое законодательство. Универсального максимального срока 90 дней для заявок или три года для рекламы настоящий Регламент не устанавливает.

1.2. Владелец процесса заполняет реестр: цель, основание, состав данных, системы и получатели, начало и окончание обработки, событие прекращения, обязательный срок документа, правовая норма, способы удаления и копии. Если точный срок документа не определен, ответственное лицо устанавливает его по применимому перечню до утверждения строки; срок не заменяется произвольным числом.

2. Заявки, реклама и личный кабинет

2.1. Заявка без покупки хранится для рассмотрения обращения и инициированного самим заявителем обсуждения курса или условий договора. Основание — соответствующее согласие либо пункт 5 части 1 статьи 6 в применимой части. Конкретное обращение закрывается при исполнении запроса, отказе заявителя либо документально установленной утрате цели дальнейшего обсуждения. Отсутствие покупки само по себе не является единственным основанием удаления.

2.2. Длительная работа с потенциальным клиентом в целях продвижения услуг требует подтвержденного предварительного согласия по статье 15 Закона № 152-ФЗ и статье 18 Закона № 38-ФЗ для рекламных контактов. Сохраняются только данные, необходимые для этой цели. Согласие на консультацию не заменяет рекламное; сохранение карточки в CRM не создает основание её использования.

2.3. Рекламная обработка осуществляется в пределах срока и условий конкретного действующего согласия, до его отзыва, требования прекратить рекламу, истечения установленного им срока либо прекращения соответствующей цели — в зависимости от того,

что наступит раньше. Если подготовленный текст рекламного согласия устанавливает конкретный срок, применяется именно он. Настоящий Регламент не продлевает ранее полученные согласия и не легализует прежние рассылки.

2.4. Не реже одного раза в квартал ответственный за CRM и рассылки проверяет актуальность целей, наличие доказательств согласия, отписки, истекшие сроки и дубли. Это внутренняя периодичность РУНО. Устаревшая база не сохраняется только потому, что клиент теоретически может купить курс.

2.5. Контакты без подтвержденного основания исключаются из рекламных заданий и выгрузок до правовой оценки. Запрос рекламного согласия сам не должен превращаться в рекламное рассылку без основания. Отказ немедленно синхронизируется между CRM, UniSender и другими фактически используемыми каналами.

2.6. После завершения обучения сохраняется бессрочный доступ к приобретенным материалам: лекциям, задачам и документам, предоставленным в ходе курса. Для исполнения этого обязательства сохраняются необходимые данные учётной записи, приобретений и права доступа. Неактивность и выпуск сами по себе не являются основанием закрытия кабинета. Паспортные копии, СНИЛС, аттестационные записи и иные данные не хранятся бессрочно только из-за существования кабинета: их сроки определяются отдельно.

2.7. Документы об обучении, договорные, бухгалтерские и кадровые документы хранятся по применимым обязательным срокам. Для бухгалтерской первички, регистров и отчетности — не менее 5 лет после отчетного года по статье 29 Закона № 402-ФЗ, если другая норма не требует дольше. Эта норма не распространяется на всю CRM-базу. Делопроизводитель и главный бухгалтер определяют конкретные статьи архивного перечня и вносят их в номенклатуру дел.

2.8. Сроки cookie, технических журналов, записей звонков при их наличии и резервных копий определяются отдельно по назначению и настройкам. Срок жизни cookie не равен сроку хранения всей аналитики. Фактические сроки и места хранения подлежат технической проверке; не утверждать непроверенные пределы.

3. Сроки исполнения запросов и прекращения

3.1. Достижение цели или отзыв согласия: прекращение соответствующей обработки и уничтожение, как правило, не позднее 30 дней в применимых случаях частей 4–5 статьи 21,

с учетом предусмотренных ими исключений и самостоятельных оснований сохранения. Рекламу прекращать немедленно по требованию, не ожидая 30 дней.

3.2. Требование прекратить обработку по части 5.1 статьи 21: до 10 рабочих дней, с учетом законных исключений; продление до 5 рабочих дней — с мотивированным уведомлением.

3.3. Предоставление информации по надлежащему запросу: до 10 рабочих дней по статье 20; продление до 5 рабочих дней — с мотивированным уведомлением. Запрос на доступ проверяется с учетом части 3 статьи 14; проверка личности должна быть соразмерной, без требования скана паспорта по умолчанию.

3.4. Уточнение подтвержденных неточных данных — до 7 рабочих дней по части 2 статьи 21. Уничтожение подтверждено незаконно полученных или ненужных для цели данных по части 3 статьи 20 — до 7 рабочих дней со дня представления подтверждающих сведений. Блокирование на время проверки применяется в установленных статьей 21 случаях.

3.5. При выявлении неправомерной обработки: прекратить до 3 рабочих дней; при невозможности обеспечить правомерность — уничтожить до 10 рабочих дней с выявления. Если в предусмотренных частью 6 статьи 21 случаях уничтожение в срок невозможно, данные блокируются и уничтожаются не позднее 6 месяцев, если федеральный закон не устанавливает иного. Это исключение, а не обычный срок хранения.

4. Удаление и резервные копии

4.1. Ответственный выдает задание с перечнем данных, основанием, системами и предельной датой. Владельцы проверяют CRM, сайт и ЛК, почту, выгрузки, рассылки, рабочие папки, бумажные носители, интеграции и подрядчиков. Удаление карточки в интерфейсе без проверки копий не подтверждает уничтожение.

4.2. Технический координатор устанавливает места и цикл хранения резервных копий, возможность выборочного удаления и порядок исключения данных из восстановления. Копии не используются для обычной работы после прекращения основания. При восстановлении сначала применяются актуальные задания на удаление и ограничения доступа.

4.3. Невозможность немедленно удалить данные из резервной копии оценивается применительно к законным условиям блокирования и срокам статьи 21; фиксируются причина, меры исключения обработки и конечная дата уничтожения. Ссылка на обычный цикл резервирования сама по себе законный срок не продлевает.

4.4. Подтверждение уничтожения оформляется по приказу Роскомнадзора от 28.10.2022 № 179: для неавтоматизированной обработки — акт; для автоматизированной — акт и выгрузка из журнала регистрации событий; для смешанной — акт и выгрузка. Акт и выгрузка хранятся 3 года с уничтожения. Эти 3 года относятся к подтверждениям уничтожения, а не к рекламным согласиям.

4.5. Акт должен содержать наименование и адрес Оператора, сведения о лице, обрабатывающем данные по поручению, если уничтожение выполнено им, ФИО субъектов либо иную относящуюся к определенным субъектам информацию, категории уничтоженных данных, информационные системы или материальные носители, способ, причину и дату уничтожения, ФИО, должности и подписи исполнителей. Выгрузка отражает субъекта или идентификатор, категории данных, систему, причину и дату уничтожения; недостающие обязательные сведения дополняются актом по правилам приказа № 179.

5. Управление доступом

5.1. Доступ предоставляется по заявке владельца процесса с указанием задачи, систем, роли и срока. Используются индивидуальные учётные записи, минимальные права и многофакторная аутентификация там, где она доступна. Общие пароли и пересылка баз в неразрешённые каналы не допускаются.

5.2. Работник до допуска знакомится с относящимися к его работе правилами и обязанностью конфиденциальности. При смене роли права пересматриваются; при прекращении полномочий отключаются без неоправданной задержки, а при риске компрометации — немедленно. Не реже квартала проводится сверка действующих доступов; периодичность установлена РУНО.

5.3. Для ООО «МЯТА ТЕХНОЛОГИИ» отдельно фиксируются права в Б24 и Метрике, разрешённые действия, возможность экспорта, срок и лица с доступом. Поручение должно определять данные, операции, цели, конфиденциальность, безопасность, выполнение требований Закона № 152-ФЗ, подтверждение принятых мер по запросу и уведомление РУНО об инцидентах. Аналогично проверяются условия иных обработчиков; не каждого лицензиара автоматически признавать получателем всех данных.

5.4. При завершении работ подрядчика отзываются учётные записи, сессии и ключи, прекращаются интеграции, возвращаются или уничтожаются копии по применимым условиям, получаются подтверждения. Законное сохранение отдельных документов подрядчиком оценивается отдельно.