АРТЕМ ДМИТРИЕВ,
руководитель практики по защите данных, PwC Legal

Культ согласий

Культ?.. Да, именно культ. Актуальное регулирование и практика его применения есть не что иное как культ согласий работника на обработку его персональных данных (далее — ПД). Роскомнадзор с каждым годом требует все больше согласий, чтобы «даровать бизнесу свою добродетель», а бизнес, как служитель этого культа, вынужден приносить в жертву сотни человеко-часов своих работников. От этого страдают сотрудники HR, рядовые работники, legal-, compliance- и DPO-функции. Все они подходят к исполнению этого требования с разным контекстом, но с одинаковой головной болью.

Причем согласия никак не защищают права и интересы работников, публичные интересы и уж тем более интересы работодателей и бизнеса. Более того, как поступить работодателю, если работник отказывается дать согласие на обработку его ПД: отказаться от хостинга своих систем на арендуемых мощностях, вести КДП и бухгалтерский учет своими силами, расторгнув договоры с внешними провайдерами? А если работник сперва даст согласие, а затем его отзовет? Эти вопросы до сих пор остаются риторическими.

Не зря на территории Евросоюза согласия работников в большинстве случаев не могут использоваться как основание для обработки ПД. Собираемые работодателем согласия не являются свободными и добровольными, а значит, не могут служить валидным основанием для обработки ПД работников.

Требование по поводу сбора согласий сегодня максимально отстранено от реальных потребностей участников оборота данных и действительных рисков приватности. У работодателя фактически нет возможности использовать иные основания для обработки ПД работников (например, исполнение договора с работником или свой законный интерес). Об этом регулярно напоминает Роскомнадзор, позиция регулятора непреклонна. Им нужны ваши (наши) согласия: чем больше — тем лучше!

Вернуться в содержание

Откуда взялся этот культ?

Увы, он прямо предусмотрен отечественным законодательством. Несколько случаев, когда необходимо получить письменное согласие работника на обработку ПД, закреплено в Законе о персональных данных: включение в общедоступные источники ПД (например, корпоративные адресные книги и справочники), обработка специальных категорий ПД (например, сведений о здоровье и национальности) или биометрии, наконец, передача данных (в том числе предоставление удаленного доступа к ним) компаниям в странах, не обеспечивающих адекватного уровня защиты прав субъектов ПД, таких как Индия, США, Китай и др.).

Есть и куда более драматичные нормы отечественного законодательства. Так, комбинация ст. 88 Трудового кодекса РФ и ст. 9 Закона о персональных данных обрекает бизнес на истинные страдания. Согласно Трудовому кодексу практически любая передача ПД работника третьим лицам требует его предварительного согласия, а в соответствии с Законом о персональных данных письменное согласие дается на обработку ПД только для одной определенной цели по принципу «одна цель — одна подпись — одно согласие — отдельный лист» (например, для кадрового учета, обеспечения перемещений, внутригрупповых коммуникаций и использования ИТ-систем). Не стоит забывать и про раскрытие ПД контрагентам и потенциальным клиентам в рамках коммерческих предложений. Получается, что необходим целый пакет согласий.

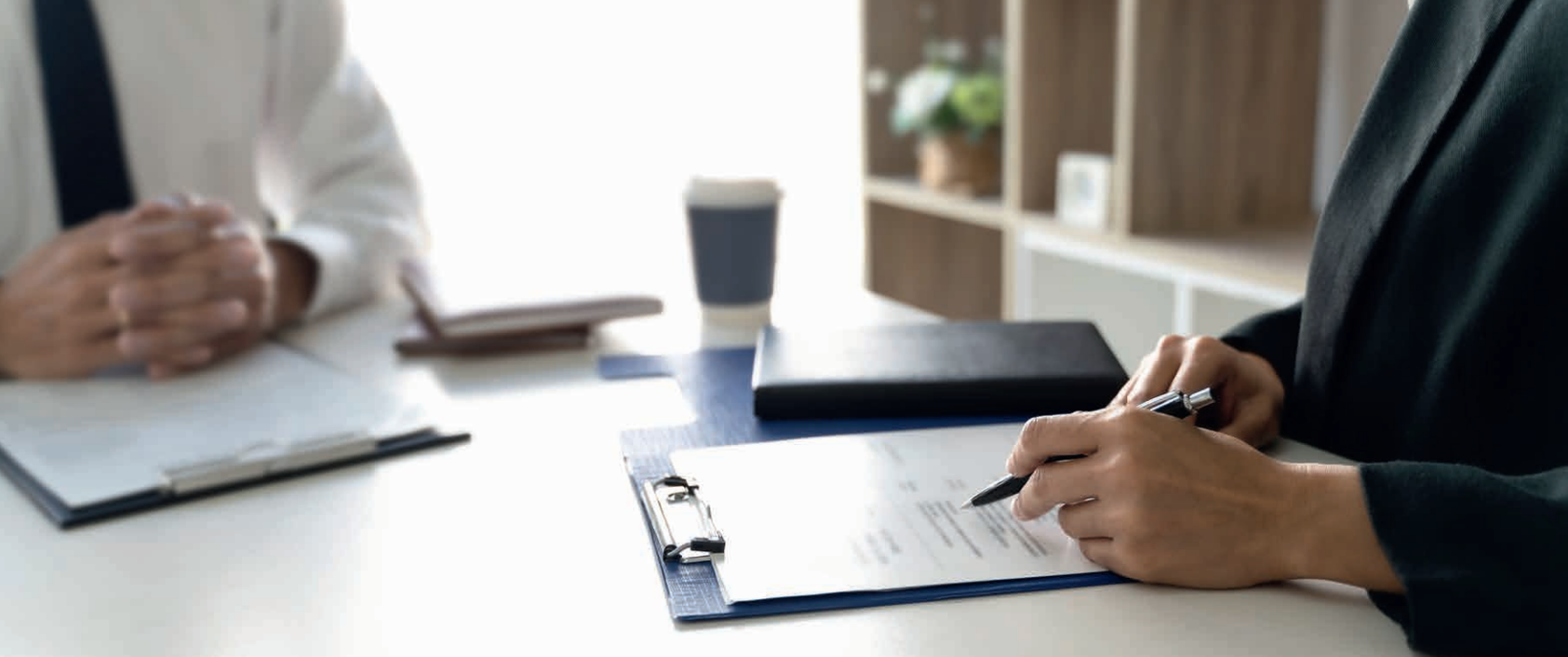
Теперь к указанным требованиям добавилась еще обязанность работодателя получать согласие

Актуальное регулирование и практика его применения есть не что иное как культ согласий работника на обработку его персональных данных

работников на распространение их ПД (например, для публикации контактов на сайте, лэндинговых страницах мероприятий, в СМИ и т. д.). Любопытно, что отдельное согласие на распространение ПД необходимо получать, даже если эти данные публикуются по требованию закона (например, в случае обязательного раскрытия информации). И ведь это совершенно точно соответствует культу: больше, еще больше согласий!

Культ возник с принятием Закона о персональных данных и Трудового кодекса РФ?

Положения законодательства десятилетиями существуют в неизменном виде, однако культ согласий за последние годы эволюционировал. Если разобраться в том, как он менялся, станет жутко от того, как без изменения законодательства может драматично меняться практика его применения. Итак, ретроспектива 20 лет. В течение долгого времени требования были, но на практике согласия



Культ потребовал выполнения сложного ритуала «одна цель — одна подпись — одно согласие — отдельный лист». Сегодня от каждого работника требуется получить по 5–8 согласий в зависимости от бизнес-процессов компании

не собирали, регуляторы этого и не требовали. Потом стали требовать наличия согласий, но весьма простых в смысле наполнения и формы — так называемых one pager. Позже потребовали детализировать информацию в разбивке по категориям ПД, третьим лицам и целям. Стали появляться согласия в форме сложных таблиц с разбивкой по целям. И уже вскоре в этих таблицах пришлось отдельно собирать подписи на каждую указанную в согласии цель, то есть появилась таблица с подписями в каждой строке (одна цель — одна подпись). А однажды и этого оказалось мало. Культ потребовал выполнения сложного ритуала «одна цель — одна подпись — одно согласие — отдельный лист». Сегодня от каждого работника требуется получить по 5–8 согласий в зависимости от бизнес-процессов компании. Каждое такое согласие должно быть на отдельном листе. И это, наверняка, наиболее беспощадный и алогичный privacy-ритуал за все время становления регулирования ПД в России.

Чего же ждать дальше?

Роскомнадзор уже прямо высказался по поводу широко обсуждаемой практики замены согласий работников на обработку ПД положениями в трудовых договорах и локальных нормативных актах работодателя. Так вот, согласия нельзя заменить полностью или частично другими документами, даже если работник их подписывает или знакомится с ними под роспись.

Есть несколько законодательных инициатив по изменению формулировки ст. 9 Закона о персональных данных. Их ключевая задача — поменять «цель» на «целИ», чтобы письменное согласие могло распространяться сразу на несколько целей. Пока эти инициативы далеки до логического завершения, зато начиная с июля зафиксированное нарушение в порядке сбора письменных согласий означает присвоение компании повышенной группы риска, что, в свою очередь, влечет за собой усиленное внимание регулятора и, в частности, возможность проведения плановых проверок раз в два года. В связи с этим говорить об ослаблении культа согласий преждевременно. Пока наблюдается как раз-таки обратный тренд.

Что это означает для бизнеса на практике?

Это означает сбор тысяч или десятков тысяч согласий работников. Кроме того, фактически любое изменение в списке третьих лиц, которые получают доступ к ПД или которым ПД передаются, влечет за собой необходимость получения новых согласий. Аналогично с внедрением новых процессов, привлечением внешних вендоров и т. п. Если работников 50 — особых трудностей нет, но если их 500 или тысячи, сделать это сложно или даже невозможно, а не делать — опасно. Да, Роскомнадзор проверяет за год лишь несколько десятков компаний. Риск того, что с проверкой придут именно к вам, не самый высокий, однако работники (включая бывших) могут инициировать разбирательство с компанией:

- жалоба может повлечь за собой проверку, инспекционный визит или как минимум запрос Роскомнадзора. Каждый год Роскомнадзор получает огромное количество таких жалоб;

Вернуться в содержание

- в этом году размер потенциальной ответственности существенно увеличили. Так, недостатки согласия работников могут стоить компании 500 тыс. рублей за каждый случай нарушения;
- штраф может налагаться Роскомнадзором кратно количеству заявителей. Таким образом, штрафы могут превышать пороги материальности даже самых «риск-аппетитных» компаний;
- набирает обороты обсуждение установления фиксированной компенсации субъектам ПД, чьи права нарушены. В случае внесения этих изменений, таким субъектам ПД больше не придется доказывать в суде размер моральных страданий и необходимой компенсации, а это может привести к полноценным коллективным атакам на компании.

Таким образом, согласия надо собирать и постоянно обновлять, потому что процессы постоянно меняются. Отсутствие согласий или отсутствие обновления таковых чревато высокими рисками: практическими и юридическими, финансовыми и репутационными. Есть и риск уголовной ответственности. А дальше эти риски будут только расти.

Как же быть?

Если в компании более 100 работников или многие из них работают удаленно, то единственное возможное решение — сбор согласий в электронной форме. Скан-копии согласий не подойдут. Надо использовать системы подписания документов электронной подписью (далее — ЭП). Такая система должна отвечать сразу нескольким требованиям, чтобы не возникло проблем с регуляторами и работниками.

Нужно использовать валидную ЭП. Понятно, что усиленную квалифицированную ЭП (УКЭП) использовать можно, но это очень дорого и неудобно. Можно было бы использовать простую ЭП (ПЭП), но это не защитит компанию от всех рисков. На практике регулятор предъявляет дополнительные требования к такой подписи. Представляется опасным использование ПЭП без дополнительных мер аутентификации подписанта, фиксации факта предоставления согласия, защиты неизменности подписанного документа и метки времени.

Золотая середина — усиленная неквалифицированная ЭП (УНЭП). Более того, грядущие изменения в трудовом законодательстве в части электронного документооборота и вовсе сделают применение УКЭП чрезмерно сложным и дорогим решением, в то время как УНЭП являет собой отличный баланс защиты интересов, комплаенса и сложности / стоимости внедрения.

Должны быть внедрены функциональный и legal (включая privacy) design. Это в первую очередь касается алгоритмов системы / программы для определения и отслеживания сроков хранения документов, перевода их на архивное хранение, контроля иных заданных атрибутов документов и задач в системе, а также интеграции с HR-мастер-системами и локализации ПД на территории России.

Кроме того, используемое решение должно предусматривать авторизацию через SSO или дополнительные факторы идентификации, другими словами — отвечать колоссальному количеству функциональных требований: от логирования до кастомизации под конкретные процессы компании. В нашей базе гипотез десятки пунктов к обязательной проверке. Локальные акты работодателя и договоры с работниками тоже должны соответствовать используемым ИТ-решениям: необходимо валидировать метод и процесс подписания согласий.

Использование электронного решения — единственный возможный сценарий упростить жизнь себе и своим работникам и обеспечить комплаенс. Риски будут расти, бумажными согласиями исключить их не получится. При этом нужно аккуратно выбирать решение для внедрения. Большинство известных на рынке решений, предоставляя необходимый функционал (например, кадрового электронного документооборота) из-за отсутствия legal design влечет за собой массу дополнительных рисков для компании-пользователя. Внедрение таких решений «в конце дня» способно принести компании больше минусов, чем плюсов.

Действительно, на рынке имеется множество решений, и некоторые из них предназначены для процессов управления согласиями или созданы для автоматизации кадрового документооборота. Рекомендуем обратить внимание именно на них. В большинстве случаев внедрять системы, построенные на базе классического ЭДО, изначально созданные для совсем других бизнес-процессов, сложно и дорого: они тяжеловесны и, как правило, не учитывают требований legal design и UX.

***

Напишите нам о сильных и слабых сторонах используемого вами решения для сбора согласий в электронной форме. Если вы пока только планируете внедрение такого решения, то расскажите о ваших требованиях к нему. На основании собранной информации мы подготовим аналитическую статью о рынке подобных решений и подробнее расскажем о практических аспектах требований legal design, указав, на что следует обратить внимание при внедрении / кастомизации решения и как не допустить ошибок.